MASTER THESIS

TOWARDS AN INTEGRATED SOCIAL MEDIA GRC METHOD

LIANNE VERSLUIS | 3359808 | BUSINESS INFORMATICS

Department of Information and Computing Sciences
Utrecht University | The Netherlands

Universiteit Utrecht

First Supervisor | Remko Helms
Second Supervisor | Ronald Batenburg

Supervisor | Maarten van Gerner

Management summary

Various researches have shown that although a lot of companies use social media or preparing to launch social media initiatives, the majority of these companies also said they were still struggling with how to best use the different channels, gauge their effectiveness, and integrate social media into their strategies. Most companies have no formalized social media strategy, or structured approach to social media in place. This leaves the company exposed to all kinds of risks related to social media and therefore, in this thesis it is argued that companies should use a structured approach to social media. For this purpose, social media should be integrated with corporate GRC processes.

The central research question in this thesis is: in which way could social media processes be integrated in corporate GRC processes, in order to make corporate social media use safer and more efficient? For answering this question, the thesis will go deeper into the appropriate governance structures and processes for social media use, the relevant risks, controls, and risk management processes, and the compliance mechanisms and processes that are relevant for social media.

Governance. The first step in the governance process is the evaluation of stakeholder needs, business opportunities, etcetera, in a cost-benefit analysis. Benefits of social media are amongst others that they provide a low-cost platform on which a company can build its personal brand, they allow organizations to engage rapidly and simultaneously with peers, employees, customers, and the broader public, they give organizations an opportunity to learn from instant information and unvarnished feedback, and that they can increase productivity, workflow efficiency, staff motivation and innovation. When asked, the companies that were interviewed for this research stated that they saw the speed of responsiveness with which a company can react on certain things on social media as the greatest benefit. They saw the distribution of incorrect, confidential or premature information, employee (mis)use and reputational damage as greatest risks of social media. The second step is setting a direction through a strategy, policy, or other social media plan. A guideline for developing strategies for monitoring, understanding, and responding to different social media activities is called the '4 Cs:' cognize, congruity, curate, and chase. These steps include understanding the social media landscape and stakeholder, performing a SWOT analysis, goals and objectives that are SMARRT, create specific social media roles, and have a clear decision-making structure in cases of emergency. The interviewed companies indicated that the main goals for social media use are promotion and image building. However, most companies did not have a specific social media strategy or crisis/emergency plan. The third step is monitoring the success of the direction taken and reporting this to stakeholders. Governance should be performed by a governing body, which can be the 'C-team' (CEO, CIO, CFO), together with the board and (IT) committees, but can also be a social media team, hub, or 'Center of Excellence.' Corporations should establish a governance structure when implementing social networking. Several structures for social media governance were found in practice are: organic, centralized, coordinated, multiple hub and spoke, and holistic. Most interviewed companies did not have a specific social media governance structure, but had the responsibility centralized in the communication department, with involvement of the marketing department for promotional purposes and the involvement of IT for supportive purposes.

Risk management. The first step of risk management is risk identification, in which possible events that can harm the achievement of the company's objectives are identified. Literature shows that there are various risks involved with social media, which mainly have reputational, operational, or legal impacts for the company. The sources of which risks originate are the organization itself (by mismanagement of social media), the employees, and external parties. The majority of the companies interviewed for this research stated that they saw the (negative) impact on the company's reputation as most threatening, and they saw employees as most common risk source. The second step is risk assessment, in which every risk is weighed on its likelihood and impact. The third step is risk mitigation, in which measures for containing the risk are taken. From literature, five risk mitigation techniques were distinguished: policies (guidelines and best practices), education (training and awareness), monitoring (filtering and blocking), access control, and crisis management. From the interviews with companies it appeared that the most implemented controls are monitoring and training, and that they are also seen as most important for controlling risk. The fourth step of risk management is monitoring and report. Risk management can be the responsibility of several persons, but common risk management roles are: senior management, chief information officer, system and information owners, business and functional managers, IT security program managers and computer security officers, IT security practitioners, and security awareness trainers.

Compliance. The first step of the compliance process is requirements analysis. Four internal requirements that companies have in place that are more 'advanced' in their social media use than other companies are: baseline governance and reinforcement, enterprise-wide response processes, on-going education program and best practice sharing, leadership from a dedicated and shared central hub. The second step is the identification and analyses of deviations. This is often done in internal and external audits, self-assessments, and security checks. An audit should focus on four aspects: strategy and governance, people, processes, and technology. The third step is deficiency management, which is the improvement of existing controls or the creation of new controls. The fourth step is monitor and report. Compliance roles are amongst others compliance manager, head of compliance, compliance officers, compliance assistants and other regulatory compliance positions. However, often compliance checks are performed by an (internal or external) audit function or team and therefore, the role that seems the most appropriate for the compliance process is the audit.

The findings of the research resulted in the social media GRC method, which is a process-deliverable diagram, showing the processes of social media GRC at the left side of the diagram, and the deliverables of those processes at the right side of the diagram. In this diagram, the three GRC processes are integrated with each other, to create an overall method.

Acknowledgements

I would like to thank the people that have supported and encouraged me during the internship period. First and foremost, my colleagues at Ernst & Young, with whom I've had a great time and from whom I learned a lot. I really appreciated the fact that everyone at the office made time for me, and showed interest in what I was doing. Even though I often stated that I was one of the many bullying victims amongst interns in the Netherlands, I always felt welcome and valued. This 'underbelly' feeling was also an important reason in my choice for EY as an internship company, and it was proven correct during the internship period. In particular, I want to thank Nora Boukadid and Maarten van Gerner, in supervising me during the internship and advising me with writing my thesis. I have to note that Maarten, besides a great supervisor is also a great driver, and would make a great professional chauffeur, may he ever consider a career change.

I also have to thank Niels, who hacked the e-mail address of someone I very much wanted to contact, and without his help, I would not have been able to do so. In addition to that, I would also like to thank Monique, Lieke and Jasper de Vries, for helping me with finding interviewees. Also I would like to thank Daniel and Maya, who both arranged an interview for me at very large, global companies, of which I at first couldn't dream of doing an interview at. And I would like to thank Sjoerd for arranging an interview for me, and giving some valuable insights about this interview afterwards. But, as said before, I should thank all my other colleagues as well, as everyone has helped me in some way: with tips, comments and advice, or with arranging interviews, accompanying me to the interviews, or helping me with writing out and summarizing the interviews.

During the internship, I experienced the working environment at EY, which I found very pleasant. Not only at the office, but also on EY events, parties and dinners. The behaviour and dancing skills of EY people at such events was always a great conversation starter. Not only the events, also going to and from those events was quite an adventure. For example the one time I got in a car with Claudia, and we almost ended up in Lelystad, while we had to be somewhere in Amsterdam! Those were exiting times...

Off course, I should not forget the support and advise that was given by my supervisors from the university. I would certainly like to thank Remko Helms, as he was always ready to give input and feedback for the thesis. I'm not sure if it was noticeable, but at some times it seemed to me like the thesis would never be finished. However, after meeting up and discussing the thesis, I always went home thinking and feeling more positively. I would also like to thank Ronald Batenburg, who agreed to be my second thesis supervisor, even in a very busy period. I am very grateful for that, and for his feedback on the thesis.

I very much enjoyed my time at the Utrecht University and after graduating, I am certainly going to miss my fellow students, as with some of them, I have become very close friends. Especially my buddies Vincent Blijleven and Joey van Angeren, who have become very good friends of me over the past years.

My thanks naturally also goes to my mother, father, brother and sister, and my boyfriend, who supported me all the way, not only through college but also now in the starting of my career. I probably would have suffered some kind of nervous breakdown by now, if it wasn't for them. With that said, I'm really looking forward to starting my career at EY, and with that, starting an exciting new period in my life.

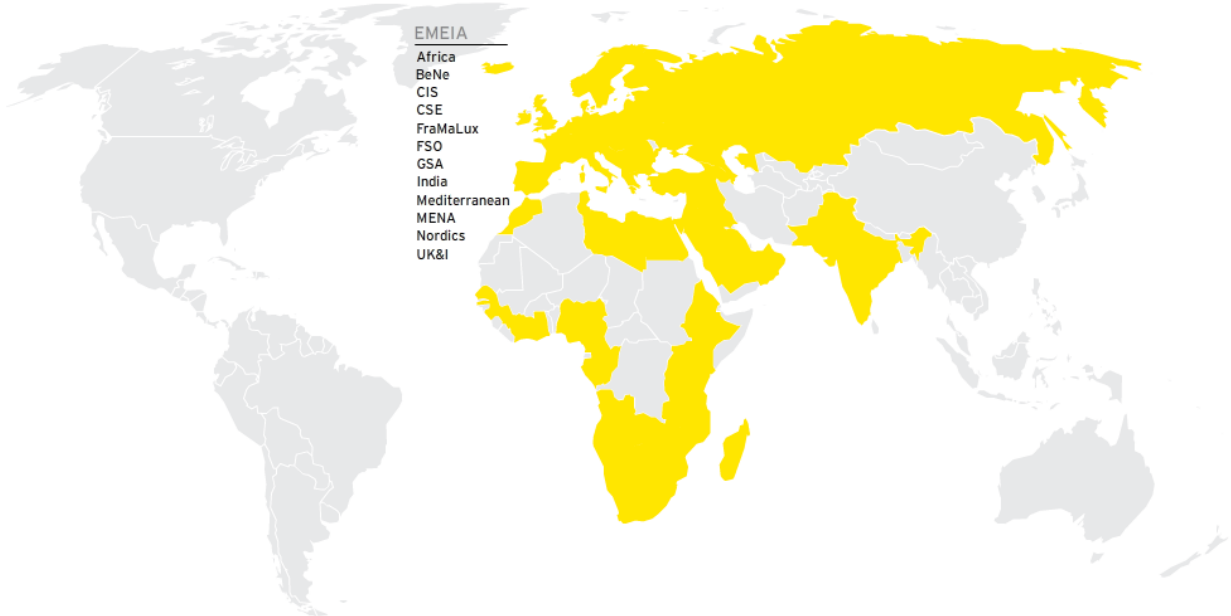
Facilitating organization

"Ernst & Young (EY) is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

We are 167,000 people based in 728 offices in 150 countries, organized into 29 Regions and four Areas. All of our people work in one of our service lines – Assurance, Advisory, Tax, Transaction Advisory Services (TAS) – or in Core Business Services (CBS) which provides internal operational support such as HR and IT services.

EY is committed to doing its part in building a better working world. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities."

The internship was conducted at the Information Technology Risk and Assurance (ITRA) department. ITRA is a specialist group that advises organizations on how to make IT more efficient and manage the risks associated with running IT operations. They focus on helping clients to optimise and secure technology so that it serves the business effectively, enhances results and reduces risk. The internship was located at the Amsterdam office of EY, which is part of the BeNe region, in the EMEIA area. The EMEIA Area comprises some 81,000 people, including 3,628 partners, working across 12 Regions and 93 countries (see below).[1]



[1] All information on this page originates from the Ernst & Young corporate website

Table of contents

List of tables and figures

1 Introduction

1.1 *Background*

Nowadays, we live in a connected world. With the emergence of Web 2.0, technologies became available that allowed the rapid mass creation and interactive exchange of user-generated content (Zerfass, Fink, & Linke, 2011). The internet became ubiquitous and dynamic, containing the wisdom of the crowds (Oreilly, 2007). New terms originated for applications that changed the web into a virtual space where users no longer passively consumed, but actively created, changed and shared information (Zerfass et al., 2011). These terms include Social Networking, E-communities, Collaborative Software, Online Communities, Virtual Communities, Social Networking Software, Social Network Services (Van Zyl, 2009), and Social media.

1.1.1 Social media

Social media is defined by Kaplan and Haenlein (2010) as internet-based applications built on the ideological and technological foundations of Web 2.0. Social media embraces a variety of platforms such as video, audio, photo, and text, and permits interactions to cross these platforms through amongst others, social sharing, email, news feeds. People spend more and more time online: according to the latest report of Nielsen and NM Incite on Social Media (2012), roughly 30 percent of total time online via a mobile device and 20 percent of total time online via a PC is spent on social networks. Additionally, the total time spent on social media in the U.S. across PCs and mobile devices increased 37 percent to 121 billion minutes in July 2012, compared to 88 billion in July 2011 (Nielsen, 2012). This is reflected by the fact that all social media platforms have grown in size and importance in recent years (Dutta, 2010), as exemplified when Facebook, that hit 655 million daily active users on average in March 2013 (Facebook, 2013).

1.1.2 Impacts

Social media drastically changed our lives. According to trend watcher Donston-Miller (2011), social media not only changes the way of communication, but will even change the entire organization in the next five years. She predicts that organizations will be less hierarchic, customers will play a more important role in the organization, customer service will be conducted more and more via social media, internal social media will replace intranets, and marketing functions will expand. These predictions are very true. Already, the customer has become much more important in the way companies do business. As Bernoff and Li (2008) put it:

> *"Empowered by online social technologies such as blogs, social networking sites like MySpace, user-generated content sites like YouTube and countless communities across the Web, customers are now connecting with and drawing power from one another. They're defining their own perspective on companies and brands, a view that's often at odds with the image a company wants to project. This groundswell of people using technologies to get the things they need from one another, rather than from companies, is now tilting the balance of power from company to customer."*

Not only the customer, but also the modern employee is using social media. The workforce of today is described by several authors as consisting of 'Generation Y' (BITS, 2011; EY, 2011) or 'Millenials' (Mittal, 2012), which is a generation that grew up with computers, ubiquitous internet access and a range of web-enabled applications, amongst which social networks and instant messaging. They are tech savvy, use smart phones and are excellent multi-taskers. For them information is to be available at their

fingertips (Mittal, 2012). They have adapted their lifestyles to each new technological invention and they won't accept that the brands they interact with, or employers they work for don't do the same (EY, 2011).

Another pressure for companies to use social media is that they also greatly can benefit from it: research showed that social applications can increase productivity, workflow efficiency, staff motivation and innovation (Van Zyl, 2009), they provide a low-cost platform on which a company can build its personal brand, they allow organizations to engage rapidly and simultaneously with peers, employees, customers, and the broader public, and they give organizations an opportunity to learn from instant information and unvarnished feedback (Dutta, 2010).

1.2 *Problem statement*

These pressures result in an increased social media use by organizations. According to a survey by the Harvard Business Review Analytic Services (HBR, 2010), more than three-quarters of the 2,100 organizations surveyed said they are either currently using social media channels or preparing to launch social media initiatives.

However, the majority of these companies also said they were still struggling with how to best use the different channels, gauge their effectiveness, and integrate social media into their strategies. Two-thirds of organizations have no formalized social media strategy in place. Sixty-one percent reported a significant learning curve before they can truly utilize social media. Many companies reported they are still searching to find the best way to demonstrate the impact of social media and the contribution to the bottom line (HBR, 2010).

Similar numbers were found in other researches. In a global survey of (EY, 2012a), it was observed that 38% of organizations do not have a coordinated approach to address social media usage within or by their organization. Zerfass et al. (2011) found 83.9% of German organizations had weak regulatory structures concerning social media. Other researchers found that 46% of US organizations had never conducted monitoring or measurement of external publics in social media, that more than 65% of Asia-Pacific organizations were without specific social media guidelines, and that only one-third of European communication professionals have organizational social media guidelines and a similar number undertake monitoring of social media channels (Verhoeven, Tench, Zerfass, Moreno, & Verčič, 2012).

1.2.1 Risks

These are surprising numbers, as there are various risks to social media. In literature, the following social media risks were found; viruses and malware, brand hijacking, reputation damage and confidentiality issues, lack of control over content, unrealistic customer expectations of "internet-speed" service, non-compliance with record management regulations, security of data and networks, legal issues such as intellectual property and copyright, employee reluctance or resistance to participate, and employee misuse and waste of time (ISACA, 2010; Owyang, 2011; Turban, Bolloju, & Liang, 2011).

According to (Merril, Latham, Santalesa, & Navetta, 2011), these risks can either have reputational, legal and operational impacts. The reputation of a company may be damaged when customers or employees post embarrassing or even incriminating things about the company online, or when they employees (un)intentionally leak sensitive or confidential information (EY, 2012b; ISACA, 2010; Molok, Chang, & Ahmad, 2010). Companies face legal risk when for example they decide not to hire an applicant based on

information they found online, or when they decide to fire employees based on their Facebook interactions with other employees in the organization (Merril et al., 2011; Nelson & Simek, 2011; Turban et al., 2011). Operational risks may involve cyber-attacks initiated through social media, mobile devices, email and other attack vectors (BITS, 2011; EY, 2012b; ISACA, 2010; Merril et al., 2011). Such attacks may consist of viruses, malware, cross-site scripting and phishing. These risks can not only lead to damage to the brand or company reputation, but also to legal issues, security and confidentiality breaches, and data theft (BITS, 2011).

1.2.2 GRC

To prevent any of the described risks from happening, companies should implement a structured approach for the use of social media. For this purpose, social media should be integrated with corporate GRC processes. According to Racz et al. (2010b), GRC is an integrated, holistic approach to organisation-wide governance, risk and compliance, ensuring that an organisation acts ethically correct and in accordance with its risk appetite, internal policies and external regulations through the alignment of strategy, processes, technology and people, thereby improving efficiency and effectiveness.

In order to understand the integration opportunities of social media in GRC processes, a closer look should be taken to governance, risk management, and compliance structures in organizations, and to what extent these processes can be used to manage social media. For defining governance, the definition of IT governance is used, as provided by the ISO (2008). In this definition, governance is seen as*: "the system by which the current and future use of IT is directed and controlled. It involves evaluating and directing the plans for the use of IT and monitors this to achieve plans and includes the policies and responsibilities for using IT within an organization (ISO, 2008)."* In the case of social media, governance can be seen as the directing and controlling of corporate social media use. For risk management, the definition of enterprise risk management is used, which according to (COSO, 2004) is: *"a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives."* Compliance is defined by EY (2010) as adherence with policies, regulations and other obligations, managed by an organization's programs, tools and other enablers.

1.3 *Research question*

As said before, companies leave themselves exposed to various risks by not having a coordinated approach to social media use. To make social media use safe and efficient, it should be integrated in the existing GRC processes of the company. The research question of this thesis therefore is:

- In which way could social media processes be integrated in corporate GRC processes, in order to make corporate social media use safer and more efficient?

Central to a safe and efficient use of social media are three processes: governance, risk management and compliance (GRC) processes. Governance processes set out rules for the risk management process, and keep oversight and control of this process. Risk management processes identify risks and mitigate these risks. Compliance processes check adherence to the rules set in the governance process. So it is necessary to include some sub questions on the topics of governance, risk management and compliance:

- Which governance structures and processes are appropriate for social media use?
- Which risks and controls are relevant for social media risk management and what are the appropriate risk management processes?
- Which compliance mechanisms and processes should be in place?

The aim of this thesis is to provide a structured way in which companies should use social media, to ensure that the usage of social media is safe and effective. In order to do this, the research provides an overview of social media uses, benefits and risks, an in-depth understanding of the three GRC topics, and gives an overview of the elements of proper social media governance, risk management, and compliance practices in organizations. To make sure that this thesis not only gives scientific insights, but also more hands-on business insights, information on the researched topics was sought both in literature and in practice.

1.4 *Scientific contribution*

Research specifically on social media GRC is still very sparse. On GRC, lots of research exists on the "G", the "R", and the "C" as separate topics, but according to Racz, Weippl, and Seufert (2010a) the potential integration moves under the radar of scientific research. Focusing on the "G," "R" and "C" in relation to social media, it appears that these topics also are not very well-documented. According to Zerfass et al. (2011), research on social media governance focuses on single aspects of Social Media Governance (e. g. guidelines, policies, definitions). They state that: *"Apart from studies that focus on guidelines, little research has been conducted on [regulatory frameworks within organizations]. Hence, little knowledge exists that might be used for guidance and examples of best practices. Similarly, resources and strategies for the use of social media are lacking in many cases."* On social media risk management and compliance, virtually no scientific literature was available. This paper aims to contribute to the body of knowledge by defining and explaining these topics.

1.5 *Related literature*

This research draws on the research of Racz et al. (2010a; Racz, Weippl, & Seufert, 2010b), who already researched the subject of GRC in a scientific manner, and the integration of the three GRC elements. They provided a clear definition of holistic GRC, which was a compilation of existing definitions of GRC, and a model to show the integration of the three elements. This model was used as basis for the social media GRC model.

1.6 *Thesis Composition*

The remainder of this thesis is as follows. In Section 2 the research method is described, explaining the choice of the research approach, and presenting amongst others the research framework, process and materials. Section 3 contains the theoretical background of this thesis, which includes social media and its impacts on the organization. Section 4 discusses the processes of GRC, and the integration of social media and GRC. Section 5 presents and analyses the results of the expert interviews. Section 6 gives the social media GRC method, together with some observations and recommendations from literature and practice. In Section 7, a discussion of the results and conclusion of the thesis are presented, containing the key findings of this thesis, limitations of the research, and an outlook for the future. The references of this thesis can be found in Section 8 and the appendices can be found in Section 9.

2 Research approach

2.1 *Design science*

As this research is aimed on providing a structured way, or method, in which social media could be used safe and effectively in the organization, it fits in the design-science paradigm. Design science creates and evaluates IT artefacts intended to solve identified organizational problems. Such artefacts are represented in a structured form that may vary from software, formal logic, and rigorous mathematics to informal natural language descriptions (Hevner, March, Park, & Ram, 2004). It seeks to create innovations that define the ideas, practices, technical capabilities, and products through which the analysis, design, implementation, management, and use of information systems can be effectively and efficiently accomplished (Hevner et al., 2004).

There are two design processes in design-science research in Information Systems (IS), namely build and evaluate. These processes can produce four design artefacts, which are constructs, models, methods, and instantiations (Hevner et al., 2004). Models use constructs to represent a real world situation the design problem and its solution space. They aid problem and solution understanding and frequently represent the connection between problem and solution components enabling exploration of the effects of design decisions and changes in the real world. Methods define processes and provide guidance on how to solve problems, that is, how to search the solution space. These can range from formal, mathematical algorithms that explicitly define the search process to informal, textual descriptions of "best practice" approaches, or some combination. Instantiations show that constructs, models, or methods can be implemented in a working system. They demonstrate feasibility, enabling concrete assessment of an artefact's suitability to its intended purpose. They also enable researchers to learn about the real world, how the artefact affects it, and how users appropriate it (Hevner et al., 2004). The artefact that is created, or built, in this thesis is a method. This method is supposed to provide a structured way in which social media GRC processes should flow, and which elements should be carefully considered to create a safe and efficient use of social media. In other words: it provides guidance to companies on how to integrate social media into GRC processes.

2.2 *Design science research methodology*

Peffers, Tuunanen, Rothenberger, and Chatterjee (2007) propose and develop a design science research methodology (DSRM) for the production and presentation of design science research in IS. They identify six activities in the development of a design science artefact: (1) problem identification and motivation, (2) define the objectives for a solution, (3) design and development, (4) demonstration, (5) evaluation, (6) communication. The DSRM activities were followed throughout this thesis. In Table 1, the different activities are shown, together with their description, resources, and the sections of the thesis in which the activity is performed.

2.2.1 Problem identification and motivation.

The problem identified in this thesis is the fact that social media is used by a growing number of companies, but not in a structured way, which leaves companies exposed to all kinds of risk. It is very important to make companies aware of those risks, and provide some guidance on how to handle those risks. In fact, it are not only the risks of social media that companies should handle in a different way, also governance and compliance structures and processes are not always (properly) in place for social media. The resources for this step is knowledge of the state of the problem, which is gathered in the literature review, which is described next.

2.2.2 Define the objectives for a solution.

As an objective for a solution, the integration of social media and GRC processes is recommended, to create a structured use of social media. To understand how companies currently (are trying to) structure their social media use, interviews were held with a number of client companies of EY. More detail on the interviewee's position in the company, and the duration of the interviews can be found in Table 2. The results of the interviews can be found in Section 5.

2.2.3 Design and development.

To model the social media GRC processes into a method, a situational method engineering approach was taken as proposed by Van de Weerd and Brinkkemper (2009). These authors proposed the modelling of so-called Process-Deliverable Diagrams (PDD) for modelling the activities and artefacts of a certain process. The PDD consists of two integrated diagrams: the process view on the left-hand side of the diagram which is based on a UML activity diagram and the deliverable view on the right-hand side of the diagram which is based on a UML class diagram. PDDs have proven to be effective means for the meta-modelling of methods, especially for the analysis and design stages herein (Van de Weerd & Brinkkemper, 2009).

Throughout the thesis, PDD's are used to visualise the processes of governance, risk management and compliance. First, the separate processes are modelled in Section 4.1.1, 4.1.2, and 4.1.3. Those processes are eventually integrated into a prototype GRC method, which can be found in Section 9.6. This prototype method was constructed based on literature entirely. The method was then further improved by adding recommendations and findings from practice. This finally resulted in 'social media GRC processes,' that were first constructed separately, as shown in the Sections 6.2, 6.3, and 6.4, and were then integrated into the social media GRC method, as shown in Section 6.5.

2.2.4 Demonstration.

As corporate social media use differs per company, and takes varying shapes and forms, there is not a 'one fits all' solution to the problem. The method created in this thesis is provided as a guideline for companies, to improve their social media processes, but is not an instant solution to the problem and could therefore not be demonstrated in the solving of a problem. However, the method was presented to various interviewees for their opinion and feedback. Following this feedback, some improvements were made.

2.2.5 Evaluation.

The method was evaluated by a social media and GRC expert of EY, This expert was given the method and was asked to provide feedback and the comments that were made during the feedback session with this expert can be found in Section 7.2.

2.2.6 Communication.

Communicating the results of this thesis, and with that the social media GRC method, is a very important, final step in the DSRM process. There are three relevant audiences for this communication process, namely: (1) the Utrecht University and the scientific world, (2) the company that facilitated the internship, Ernst & Young, and (3) the interviewees. Those parties will all be provided with a copy of the thesis.

Activity	Description	Resource	Section
Problem identification and motivation.	Define the specific research problem and justify the value of a solution.	Resources required for this activity include knowledge of the state of the problem and the importance of its solution.	Introduction, Theoretical framework (Section 1, 3)
Define the objectives for a solution.	Infer the objectives of a solution from the problem definition and knowledge of what is possible and feasible.	Resources required for this include knowledge of the state of problems and current solutions, if any, and their efficacy.	Theoretical framework, GRC, Expert interviews (Section 3, 4, 5)
Design and development.	Create the artefact.	Resources required moving from objectives to design and development include knowledge of theory that can be brought to bear in a solution.	Social media GRC method (Section 6)
Demonstration.	Demonstrate the use of the artefact to solve one or more instances of the problem.	Resources required for the demonstration include effective knowledge of how to use the artefact to solve the problem.	Discussion and conclusion (Section 7)
Evaluation.	Observe and measure how well the artefact supports a solution to the problem.	Could be budgets, the results of satisfaction surveys, client feedback, response time or empirical evidence.	Discussion and conclusion (Section 7)
Communication.	Communicate the problem, the artefact, its novelty, and its effectiveness to researchers and other relevant audiences	Communication requires knowledge of the disciplinary culture.	Discussion and conclusion (Section 7)

TABLE 1 | DESIGN SCIENCE ACTIVITIES AS DESCRIBED BY PEFFERS ET AL. (2007)

2.3 *Research framework*

The research approach is visualized by using the modelling method as proposed by Verschuren and Doorewaard (2007), and is shown in Figure 1. The rectangles represent 'research objects'. Vertical arrows represent 'confrontations' between the research objects, which then result in a new research object. In the end these research objects result in the final deliverable.

The research started with a literature review, which consisted of literature on two topics: literature on social media and literature on GRC. This literature came both from scientific papers and papers and articles from practice. The literature search on social media gained literature on social media amongst others: its definition, its benefits and risks, the various purposes which social media is used for in an organization, and tips and tricks to use corporate social media properly. The search on GRC gained literature on; the definition of GRC, how to structure governance, and which roles and responsibilities should be defined, how to manage risks, which controls should be in place, and compliance practices. The literature reviews were used to construct a theoretical framework for the thesis and to construct a prototype method for GRC. This prototype method can be found in Section 9.6. The theoretical framework was used to develop an interview guide for the expert interviews. The interviews were conducted according to this guide, and the results of the interviews, and the feedback on the prototype

method that was given in the interviews, was analysed. These results were used for constructing the final social media GRC method.

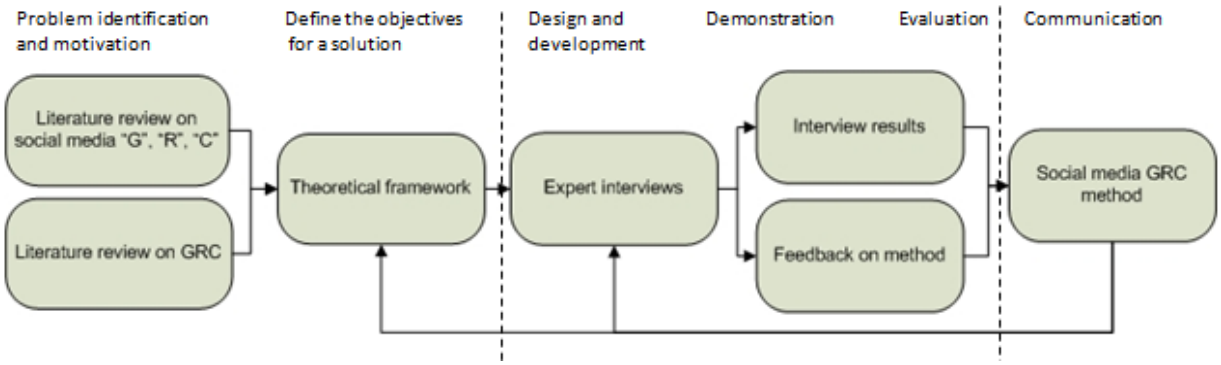


FIGURE 1| RESEARCH FRAMEWORK

2.3.1.1 Literature review

In order to develop an initial theoretical framework, a literature review was conducted by means of the structured literature approach technique proposed by Webster and Watson (2002). This is a three-step approach that covers as much literature as possible with regard to a certain field of interest. The first step is to identify a list of literature, based on a certain amount of keywords, in an online database. The articles found are reviewed based on their relevance and a list is made of relevant articles to continue in the process. The next step is to take the relevant articles, and search through their references to see whether there are more relevant articles to be found there. The last step is to take all the found literature so far, and check how often (and by whom) they have been cited. These citations are checked as well to see whether there are relevant articles to be found. Once all citations have been checked, and all relevant literature found in the last step is noted down, the final list is compiled containing literature from all three steps.

Search cycle 1. The literature review for this thesis started with three searches on Google Scholar. Keywords for these searches were: "social media governance," "social media risks," and "social media compliance" (initially, the search terms included "social media risk management," however this yielded only 8 results which were not particularly relevant to the research and therefore the search was changed to "social media risks"). Google Scholar was set to exclude patents and quotes, and only search in English. The search on social media governance gained 87 results, the search on social media risks gained 96 results, and the search on social media compliance gained 19 results. An additional search was done on GRC, with the keywords: "GRC" and "governance" and "risk" and "compliance," which had to occur in the tile of the article, which resulted in 15 articles. These searches added up to 217 results in total. However, a lot of these articles were either from fields of science that were not relevant for this research (e.g. the health industry, education/library, government), were promotional material for companies, or thesis projects. Those papers were all excluded from the final results. Then, the resulting papers were assessed on relevance by reading their title and abstract. This finally resulted in a list of 30 papers (for this list, see the References).

Search cycle 2. The next step of the literature review was to search through the references of the articles found in cycle one (only those selected for further review). Again, the goal was to find relevant sources of information, by searching through the references of the articles found in the first cycle. This resulted

in articles on two subjects: (1) social media in general; its definition, its uses in the organization, benefits and risks, and (2) standards such as the ISO, or the COSO model, or reports from organizations like the IT Governance Institute (ITGI) and the National Institute of Standards and Technology (NIST). This resulted in 12 white papers and reports (for this list, see the References).

Search cycle 3. The last step of the structured literature review focused on identifying the citations of every piece of literature taken to the last step. As far as possible, the citations were counted for every used article (how often it has been cited, and by whom) to identify their scientific value. The results of this citation count can be found in Section 9.5.

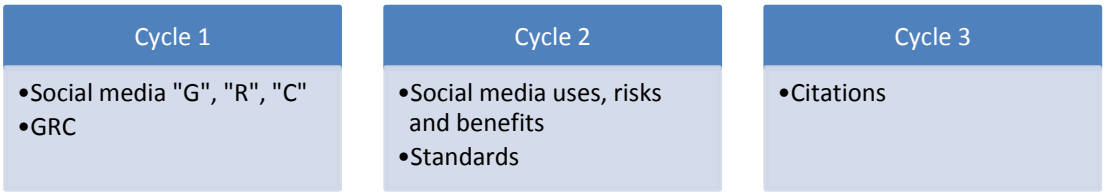


FIGURE 2 | LITERATURE SEARCH PROCESS

In addition to the scientific literature that was found in the literature review, also a document study was performed through the Ernst & Young (EY) intranet, to obtain practitioner's knowledge on social media. Several reports, white papers and presentations of different organizations were obtained through the EY intranet. These documents were read and analysed for existing rules and regulations around organizational social media use, experiences with social media, and possible recommendations or best practices for social media use and governance. This resulted in 4 white papers written by Ernst & Young.

Overall, the various literature searches resulted in 46 results, of which 30 were scientific articles, originating from scientific journals (e.g. MIS quarterly, Public communications review), and 16 were white papers and reports from organizations (e.g. Ernst & Young, Altimeter group), and from institutes (COSO, the IT governance institute).

2.3.1.2 Expert interviews

In this section, the research approach is elaborated. A qualitative research method was used for this research, which aims to examine objects or phenomena in their natural settings (Myers, 1997). The relevance of social and behavioural considerations in corporate social media use asks for a qualitative approach. Therefore, a qualitative approach is taken by using expert interviews as data source.

For data gathering, in-depth interviews were carried out with subject matter experts from 9 client companies of EY. Before every interview, additional information about the company was sought through the internet, on corporate websites and social media sites. The company website was consulted to identify the various social media channels the company used. The social media sites were consulted to see how active the companies were on their social media pages.

After information gathering on the company, the interviews with subject matter experts on social media were performed. These interviews were on the social media attitudes of the interviewee and their organization, on the governance structure in their organization, the risk mitigation techniques they used, and the techniques and mechanisms with which they checked compliance. The functions of the interviewees differed, as social media responsibility was assigned differently at the selected companies. The interviews had a duration of 15 to 90 minutes.

Company	*Function of the interviewee*	*Duration*
A	Head of EU IT compliance	20:10
B	Risk manager	45:59
C	Global audit manager	1:20:48
D	Representative	34:36
E	Communications advisor	58:48
F	Communication specialist	59:05
G	IT advisor	36:10
H	Global social media manager	15:34
I	Manager Enterprise Risk Management	32:11

TABLE 2 | OVERVIEW OF INTERVIEWEE ROLES AND INTERVIEW DURATION

The interviews were recorded with the consent of the interviewees, so that they could be transcribed later on. The transcriptions of the interviews were summarized into some key statements and quotes, and this summary was sent back to the interviewee for approval. When necessary, changes were made and the updated document was sent again for final approval.

2.4 *Validity*

A great deal of attention is applied to reliability and validity in all research methods. However, there are challenges to in attaining reliability and validity in qualitative research. Some suggested adopting new criteria for determining reliability and validity. Lincoln and Guba (1985) substituted reliability and validity with the parallel concept of "trustworthiness," containing four aspects: credibility, transferability, dependability, and confirmability.

(1) The credibility criteria involve establishing that the results of qualitative research are credible or believable from the perspective of the participant in the research. This is important because the participants are the only ones who can legitimately judge the credibility of the results (Lincoln & Guba, 1985). In order to ensure credibility, in every case the results of the interview were sent back to the interviewee for feedback and approval. (2) Transferability refers to the degree to which the results of qualitative research can be generalized or transferred to other contexts or settings. From a qualitative perspective, transferability is primarily the responsibility of the one doing the generalizing (Lincoln & Guba, 1985). To ensure transferability, multiple cases were used. (3) The idea of dependability emphasizes the changes that occur in the setting and how these changes affected the way the research approached the study (Lincoln & Guba, 1985). In other words, dependability is about showing that the findings are consistent and could be repeated. To ensure dependability in the literature review, a structured literature review approach was used and the search process for literature was accordingly documented. To ensure dependability in the interviews, and interview guide was used to ensure that the same questions were asked at every company. (4) Confirmability refers to the degree to which the results could be confirmed or corroborated by others (Lincoln & Guba, 1985), so to ensure a degree of neutrality and to eliminate any researcher bias, motivation, or interest. To keep the research as neutral as possible, the interviews conducted in the various companies were all consisting of 'open' questions, to avoid any questions that would 'push' people in a certain direction in their answer.

2.5 *List of terms and abbreviations*

- GRC - An integrated, holistic approach to organisation-wide governance, risk and compliance, ensuring that an organisation acts ethically correct and in accordance with its risk appetite, internal policies and external regulations through the alignment of strategy, processes, technology and people, thereby improving efficiency and effectiveness.
- Governance - The system by which the current and future use of IT is directed and controlled. It involves evaluating and directing the plans for the use of IT media and monitors this use to achieve plans. It includes the policies and responsibilities for using IT within an organization
- Enterprise risk management - A process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.
- Compliance - Adherence with policies, regulations and other obligations, managed by an organization's programs, tools and other enablers.
- Web 2.0 – Technologies that allow the rapid mass creation and interactive exchange of user-generated content
- Enterprise 2.0 - When social software is used within a company or between companies and their partners or customers to support collaborative work and knowledge management
- Gen X – Generation that has a strong digital affinity
- Gen Y - The digital natives, born post 1980
- Social media - Internet-based applications built on the ideological and technological foundations of Web 2.0
- Social networking sites - Web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system.
- Social engineering - A collection of techniques used to manipulate people into performing actions or divulging confidential information, namely the unauthorized acquisition of sensitive information or inappropriate access privileges by a potential threat source.

- ISO/IEC 38500:2008 - Corporate governance of information technology standard
- NIST – National Institute of Standards and Technology
- COSO - Committee of Sponsoring Organizations of the Treadway Commission
- ERM – Enterprise Risk Management
- ITGI – IT Governance Institute
- ISACA - Information Systems Audit and Control Association
- COBIT - Control Objectives for Information and related Technology
- UCF - Unified Compliance Framework

- GRC - Governance, Risk management and Compliance
- SM – Social media
- FB – Facebook
- SMARRT - Specific, Measurable, Actionable, Realistic, Results-oriented and Timely
- ORCA - Objective, Risk, Controls, Assurance

3 Theoretical background

Although it is clear that social media is very powerful, many executives are reluctant or unable to develop strategies and allocate resources to engage effectively with social media (Kietzmann, Hermkens, McCarthy, & Silvestre, 2011). Consequently, firms regularly ignore or mismanage the opportunities and threats presented by creative consumers. One reason behind this ineptitude is a lack of understanding regarding what social media are, and the various forms they can take (Kaplan & Haenlein, 2010). Therefore, the various forms of social media will be explained in this section, together with the benefits social media can bring to a company. Then the risks of social media will be elaborated on. Next, a guideline is given on how companies should implement social media.

3.1 *Social media*

Social media (SM) can be indicated by various different terms, including social networking, collaborative software, social networking software, social network services, social networking sites, social software, social media, online social networking, electronic social networking and enterprise social networking (Back & Koch, 2011; Turban et al., 2011; Van Zyl, 2009). According to Kaplan and Haenlein (2010), social media is a group of Internet-based applications that build on the ideological and technological foundations of Web 2.0, and that allow the creation and exchange of user generated content. Back and Koch (2011) state that social media can be used as a synonym for social software or to describe the communication channels opened by social software (Back & Koch, 2011). According to them, social software is the technical part (applications) in the Web 2.0; it is software or services that support, extend, or derive added value from human social behaviour.

Social media tools and applications are diversified, versatile, feature-laden and powerful (Safko & Brake, 2009). However, some common categories of social media sites, tools and applications can be identified, which are: social networking, publish, photo sharing, audio, video, micro blogging, live casting, virtual worlds, gaming, productivity applications, aggregators, search, mobile, and interpersonal (Safko & Brake, 2009). An overview of these applications, together with some example platforms is given below.

Application	**Example**
Social networking	Facebook, Friendster, LinkedIn, Xing.
Publish	TypePad, Blogger, Wikipedia and Joomla
Sharing photo, audio or video	Photo - Flickr, Picasa, Photobucket Audio - iTunes, Rhapsody and Podbean. Video - YouTube and Google Video
Microblogging	Twitxr, Twitter and Plurk
Livecasting	SHOUTcast, BlogTalkRadio, TalkShoe, and Live365.
Virtual worlds	Second Life, ViOS and Active Worlds
Gaming	World of Warcraft, Entropia Universe or Halo3.
Productivity	ReadNotify, Zoho, Zoomerang, Constant Contact and Eventful.
Aggregators	Digg, Yelp, iGoogle, Reddit, FriendFeed, My Yahoo! and Google Reader.
RSS	RSS 2.0, Atom and Pigshot
Search	MetaTube, Yahoo! Search and IceRocket.
Mobile	Jumbuck, CallWave, airG, Jott and Brightkite.
Interpersonal	WebEx, iChat, Meebo, Acrobat Connect and Skype.

TABLE 3 | SOCIAL APPLICATIONS AND EXAMPLES

In this thesis, the focus lies on the corporate use of social networking sites, such as Xing or Facebook (Back & Koch, 2011). Boyd and Ellison (2007) define social network sites as web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system.

3.1.1 Corporate social media use

The corporate use of these networking sites is termed by Turban, Bolloju, and Liang (2011) as "enterprise social networking." They argue that the main reason for firms to use social network sites are: (1) to participate in public social networks and engage in information sharing, advertising, market research, recruitment, and other activities, (2) to create internal social networks for the exclusive use of employees and alumni, (3) to create enterprise-owned social networks for customers and business partners, (4) to enhance existing application platforms, such as e-mail and customer relationship management, by including functionalities that are commonly available in social networking systems as blogs, wikis, and discussion forums, and (5) to develop tools or services that include capabilities to support social networking applications.

Firms are drawn to social media because their potential for reaching millions of users and to get their products or services discussed favourably by as much of the online population as possible (Safko & Brake, 2009). According to Dutta (2010), there are three main reasons for leaders to embrace the corporate use of social media. First, they provide a low-cost platform on which a company can build its personal brand, showcasing the company's image both within and outside the company. For example, showing commitment to a cause, profession, company, or product, and demonstrating a capacity for reflection instead of just action. Second, they allow organizations to engage rapidly and simultaneously with peers, employees, customers, and the broader public, especially younger generations, in the same transparent and direct way they expect from everyone in their lives. Third, they give organizations an opportunity to learn from instant information and unvarnished feedback.

Some companies even go as far as integrating social media throughout their entire business processes. These companies call themselves 'social businesses.' According to IBM (2011), a social business embraces networks of people to create business value. There are three underlying tenants for this: (1) Engaged, a social business connects people to expertise and enables individuals to form networks to generate new sources of innovation, foster creativity, and establish greater reach and exposure to new business opportunities. (2) Transparent, a social business strives to remove unnecessary boundaries between experts inside the company and experts in the marketplace. It embraces the tools and leadership models that support capturing knowledge and insight from many sources. (3) Nimble, a social business leverages these social networks to speed up business, gaining real-time insight to make quicker and better decisions. According to IBM (2011), a social business can reap great benefits by allowing people (both inside and outside an organization) to document and share their knowledge and ideas and others to recognize, refine and promote the value of those ideas and content.

A social business embraces networks of people to create business value. There are three underlying tenants for this definition: engaged, transparent, and nimble.

3.2 *Social media risks*

As said before, firms are reluctant or unable to develop strategies and allocate resources to engage effectively with social media, and they regularly ignore or mismanage the opportunities and threats presented in this process. This leaves the company exposed to various risks. In this section, an indication is given of where risks can originate from, and what those risks are.

3.2.1 Risk sources

There are many sources of which risks can arise. According to EY (2012b), there are three 'touch points' of social media when used in a corporate setting, which they view as risk sources. These are: (1) organizations that use social media to engage customers and other stakeholders to help shape the conversation around their products, services and brand, (2) employees that use social media either internally or externally, and (3) external stakeholders who converse publicly online about the organization, its products and services, giving the organization market insights and perspective. These three channels all pose risks to organizations (EY, 2012b). For example, organizations can cause risks by mismanagement of social media (not having clear policies and guidelines), employees can cause risks by not being compliant to or being unaware of social media policies and external parties can cause risk by posting negative comments about the company or launching attacks that affect the company.

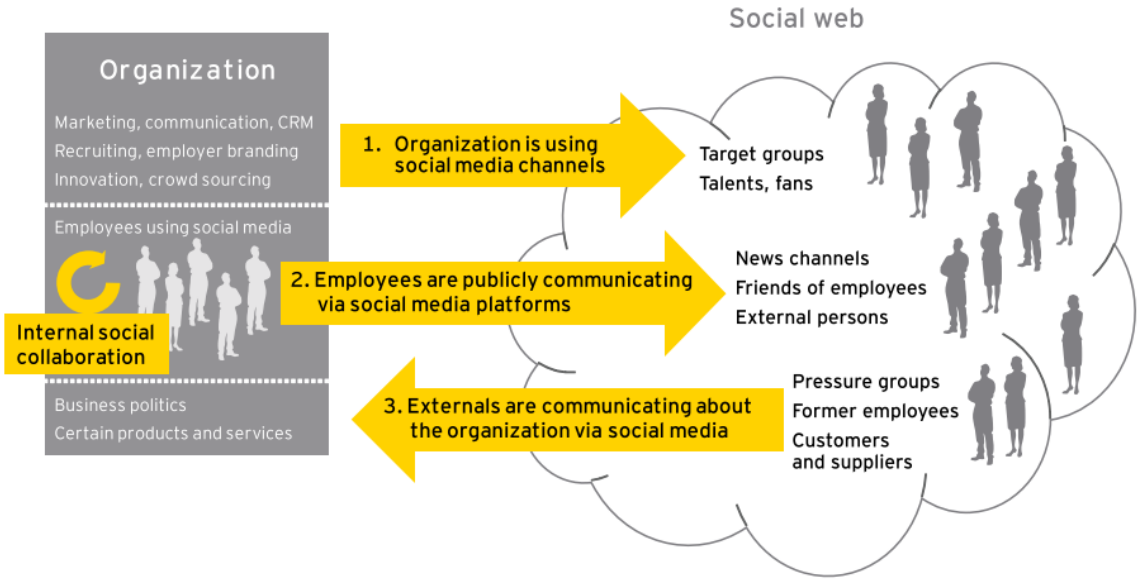


FIGURE 3 | TOUCH POINTS OF SOCIAL MEDIA (EY, 2012B)

3.2.2 Risks

Stemming from these risks sources, various risks can occur, ranging from identify theft to unprofessional employee behaviour. In order to index the risks that come along with corporate social media use, the report of the BITS (2011) was used as a starting point, as it contains a very complete overview of social media risks. The whole report was comprised into a list of social media risks and recommended mitigation techniques, which can be found in Section 9.2. The risks were then categorized into the categories legal, reputational and operational (Merril et al., 2011). The risks and risk categories are shown in Table 4, together with the authors that mentioned this risk.

Risk categories by (Merril et al., 2011)	Risks as identified by (BITS, 2011)	(Nelson & Simek, 2011)	(ISACA, 2010, 2012)	(Kaplan & Haenlein, 2010)	(Van Zyl, 2009)	(EY, 2012b)	(Dutta, 2010)	(Larson & Watson, 2011)	(Katz & McIntosh, 2013)	(Turban et al., 2011)	(Molok et al., 2010)	(Merril et al., 2011)
Operational	Identity Theft/brand hijacking		X									
	Spreading Malware		X		X							X
	Social Engineering		X			X						X
	Products lack maturity											
	Managing Access											
	Measuring success											
	Lack of centralized governance											
	Physical security risk											
	Social media content is forever											
	Lack of Associate Productivity				X	X				X	X	
Legal	No Separation of Personal/Professional communication											
	Civil Litigation											
	eDiscovery		X									
	Compliance to company policy, laws and regulations		X				X		X	X		
	Information Retention Management		X									
	Endorsement Guidelines	X										
	Labour Relations	X								X		X
	Intellectual Property/Privacy/Confidentiality issues		X			X	X		X	X	X	X
Repu-tational	Lack of monitoring	X										X
	Insufficient employee training											
	Negative brand impacts/customer dissatisfaction	X	X	X	X	X		X	X	X	X	X
	Responding to a crisis											

TABLE 4 | SOCIAL MEDIA RISKS

3.2.2.1 Operational

Operational risks have to do with security of corporate systems, and the confidentiality of company data. These are very real concerns, because when employees access social media platforms at work, even those employees who are designated as social media spokespersons for the organization, they risk endangering the organization's networked computers (Merril et al., 2011). They could be unknowingly targeted in cyber-attacks such as phishing and cross-site scripting, and acquire malware, viruses, and spyware (Merril et al., 2011).

Identity theft. Security breaches may occur through identity theft. Identity theft is when someone impersonates another person, without him knowing, or when a hacker has 'hijacked' a corporate social media account (ISACA, 2010), and posts messages as if he was an official spokesperson of the company. This obviously has become a lot easier for hackers, as people put a lot of personal information online.

Malware. Spreading malware can be done in different ways. For example, shortened URLs can be used to lead people to unsafe websites, where a virus is installed on their computer. Or 'spoofing,' which is when a company's website and social media pages are hacked or simulated by fraudsters and visitors are tricked into downloading malware or divulging information hereon. This may even allege in a lawsuit about a company's failure to monitor for malware, and spoofed sites in the social media realm (Merril et al., 2011).

Social engineering. Social engineering provides other points of entry for attackers and pose more risks for organizations (Merril et al., 2011). Social engineering is a collection of techniques used to manipulate people into performing actions or divulging confidential information (BITS, 2011). An example hereof is given in the following case, taken from practice (Goodchild, 2011):

> *"Social engineering expert Chris Hadnagy was hired as a Social Engineering (SE) auditor to gain access to the servers of a printing company which had some proprietary processes and vendors that competitors were after. After some information gathering, Hadnagy found the locations of servers, IP addresses, email addresses, phone numbers, employee names and titles, and much more. He learned that the CEO had a family member that had battled cancer, and lived. As a result, he was interested and involved in cancer fundraising and research. Through Facebook, Hadnagy was also able to get other personal details about the CEO, such as his favourite restaurant and sports team. Hadnagy called the CEO and posed as a fundraiser from a cancer charity. He informed him they were offering a prize drawing in exchange for donations—and the prizes included tickets to a game played by his favourite sports team. The CEO agreed to let Hadnagy send him a PDF with more information on the fund drive. He even managed to get the CEO to tell him which version of Adobe reader he was running because, he told the CEO "I want to make sure I'm sending you a PDF you can read." Once the CEO opened the file, it installed a shell that allowed Hadnagy to access not only his computer, but also company documents and confidential information."*

Managing access. Managing access is about restricting social media access to only those employees that have a legitimate business need to use it (BITS, 2011), to prevent unauthorized in- or outsiders to be able to post anything on corporate social media pages.

Measuring success. According to the (BITS, 2011), calculating a the return on investment (ROI) of social media presents a challenge. Institutions and marketers realize the potential and importance of communicating and connecting with consumers through social media channels, but justifying the dollar and time investment is problematic.

Lack of centralized governance. According to the (BITS, 2011) clear and well-publicized governance structure for overseeing and coordinating SM activity that enables employees to closely coordinate their activities across businesses and have a clear understanding of chain of command and accountability will ensure consistent messaging and preserve data security.

Social media lacks maturity. According to the (BITS, 2011), social media is not yet mature. This presents potentially serious consequences that can affect brand image, security reputation, and customer's personal and account information.

Physical security risk. There may also be physical security risks related to social media, when people put too much information about their whereabouts on their social media pages, making them vulnerable to physical attacks.

Social media content is forever. For many company of size, there will be a large amount of information, positive and negative, about that company posted outside official marketing channels (BITS, 2011).

Lack of Associate Productivity. Other operational risks emerge from the employees in the organization, and their (mis)use of social media. This can be loss of productivity, when employees spend too much time on social media (BITS, 2011; ISACA, 2010; Merril et al., 2011).

3.2.2.2 Legal

The legal risks associated with social media should be carefully considered prior to engaging in a social media strategy, as they may end in a courtroom. The BITS (2011) identifies the following risks: lack of separation of personal and professional communications, civil litigation, ediscovery, compliance to company policy, laws and regulations, information retention management. endorsement guidelines. labour relations, intellectual property/privacy/confidentiality issues.

Lack of Separation of Personal and Professional Communications. When employees use social media for both personal and professional purposes, there is greater risk of mistakenly using work-related accounts to express personal opinions or of accidently communicating with personal contacts through a work account (BITS, 2011).

Civil Litigation. When an employee acts as a representative of their firm or provides a direct association, their actions could potentially be used against the firm. Examples may include an employee blogging about a current court case, or an employee discussing client information or providing client sensitive data (BITS, 2011).

eDiscovery. Information on SM sites falls under the category of ESI. There are several aspects of legal discovery, including preservation, privacy and admissibility, which impacts eDiscovery and potentially leads to risks associated with the use of SM.

Compliance to company policy, laws and regulations. Companies need to understand the various laws and regulations for the countries in which they do business, for example privacy laws, but also marketing laws (BITS, 2011), and they have to be compliant to those laws. Also, companies may run into legal trouble if their social media activities violate their own privacy policies (Merril et al., 2011).

Information Retention Management. With the ability of posts, tweets and other communications to be quickly deleted and modified, what obligations are expected of firms to capture data in real-time as opposed to regular snapshots? Additionally, social media sites quickly add and remove features, including adding or removing protections for communications. In such an environment when previously private communications are exposed publicly due to a change in policies of a given social media provider, how quickly are firms expected to retain such communications (BITS, 2011)?

Endorsement Guidelines. Care must be taken when using SM conversations in the context of advertising. An employee who favourably blogs or comments on the organization or its products may be deemed an endorser under the guidelines, thereby subject to the disclosure guidelines. Failure to disclose the connection can, in some circumstances, result in the imposition of liability on the company regardless of whether the company approved (or even knew of) the post (Nelson & Simek, 2011).

Labour Relations. The use of SM by employees and employers is increasingly being impacted by issues related to employment and labour laws. Issues related to employment and labour laws include pre-employment screening and hiring practices, unfair labour practices, harassment and safety issues (BITS, 2011). Legal risks may arise from the collection of information on race, ethnicity, or medical problems from external social networks, especially if that information is used improperly or illegally when recruiting employees or used to harass colleagues (Turban et al., 2011).

Intellectual Property/Privacy/Confidentiality issues. Users of social media can share information that is considered sensitive or proprietary from a business perspective (BITS, 2011). Companies may be held directly liable for hosting material on their website or vicariously liable for employee actions on third-party sites that infringe the copyright, trademark, or other intellectual property rights of others (Merril et al., 2011; Turban et al., 2011).

3.2.2.3 Reputational

Reputational threats are activities and/or information originating from employees or external sources that may damage the image and reputation of a company (and possibly its stakeholders) (BITS, 2011). The reputational risks of social media can easily equal or exceed the reputational benefits, for one simple reason: the vast reach of social media platforms on which millions, globally, communicate every second of every day and night offer not only a vast frontier of promotional opportunity, but a vast uncharted "sinkhole" of risk (Merril et al., 2011).

Lack of monitoring. A lack of monitoring can result in an abundance of posts, tweets and comments regarding the firm that are negative, insensitive or damaging to the company image (BITS, 2011).

Insufficient employee training. When employees are not made fully aware of a company's approved policy, procedures and strategy for proactive social media use and therefore may use social media inappropriately (BITS, 2011).

Negative brand impacts. For example, through missteps in use of social media by company employees, false or inaccurate information circulating through SM, or misuse of corporate trademarks, present potentially serious, long-lasting negative impact on a company's brand and reputation.

During the first presidential debate between President Obama and Mitt Romney, Obama credited his tenacious grandmother who helped raise him and passed away three days before he was elected president. Moments later, @KitchenAidUSA, the company's official Twitter account, sent this: *"Obamas gma even knew it was going 2 b bad! She died 3 days b4 he became president."* The insensitive tweet not only went to the company's 25,000 followers, but also included a hashtag to make it a part of NBC News' social debate conversation. KitchenAid hastily deleted the tweet, but the damage was done. Even after the head of the KitchenAid brand, Cynthia Soledad, offered an apology, many still expressed outrage and announced boycotts of the brand (Dunay, 2012).

Crisis response. The last risk is about responding to a crisis, or, to be more specific: not having a response plan when a crisis occurs. According to the (BITS, 2011), a company should have a crisis communications plan that should include both defensive and proactive use of social media. So, when a customer or employee posts something that is really embarrassing to the company, and it goes viral. How should the company respond to that? Ignore it or deny it? It is very important that a company has a response plan in case something happens, in order to provide information quickly, and in an uniform fashion. A well-known example of a company that didn't have a good crisis plan in place is United Airlines, who may still feel the consequences of not adequately responding to the social media crisis they encountered.

In the spring of 2008, the guitar of Dave Carroll was damaged by baggage handlers of United Airlines when his band Sons of Maxwell landed in Chicago. The airline company refused to replace Dave Carroll's guitar. Sons of Maxwell upload a music video, aptly titled "United Breaks Guitars," and it garnered close to 9 million views on YouTube, as Dave punches out blunt lyrics such as "You broke it, you should fix it / You're liable, just admit it." He went on to make 2 more songs, the trio has been viewed well over 11 million times, and has some of the highest Like-to-Dislike ratings on the site, with waves of comments crashing against United's shores to this day—despite being uploaded over a year ago, the original video still garners multiple comments per day, the majority of which scathe the airline company for its poor service (Thomas, 2010).

3.2.3 Risk matrix

The various social media risks van be related to the risk sources that were discussed previously. For example, identity theft, which is an operational risk, is caused generally by an external party. In this sense a risk matrix has been created, taking the various social media risks as identified by the BITS (2011), and showing their main impact (operational, legal, or reputational) as identified by Merril et al. (2011) and their main source (organization, employee or external parties) as proposed by EY (2012b). As said, the general impact and source of the risk are described, so it might be that with some risks, another risk source or impact can be ascribed to it. However, to keep the table relatively simple, it was chosen to show only the main impact(s) and source(s). The social media risks, their impact (operational, legal, reputation), and their (possible) risk source (organization, employee, external source), were summarized in the table below.

Risks (BITS, 2011)	Impact of risk (Merril et al., 2011)			Risk source (EY, 2012b)		
	Operation	Legal	Reputation	Organization	Employee	External
Identity Theft/Brand hijacking	X					X
Spreading Malware	X				X	
Social Engineering	X					X
Products Lack Maturity	X			X		
Managing Access	X			X		
Measuring success	X			X		
Lack of centralized governance	X			X		
Physical security risk	X			X		
Social media content is forever	X				X	X
Lack of Associate Productivity	X				X	
Lack of Separation of Personal and Professional Communications		X		X	X	
Civil Litigation		X			X	
eDiscovery		X		X		
Compliance to company policy, (inter)national laws and regulations		X		X	X	
Information Retention Management		X		X		
Endorsement Guidelines		X		X		
Labour Relations		X		X		
Intellectual Property/Privacy/Confidentiality issues		X			X	
Lack of monitoring			X	X		
Insufficient employee training			X	X		
Negative brand impacts			X		X	X
Responding to a crisis			X	X		

TABLE 5 | SOCIAL MEDIA RISKS, IMPACTS AND SOURCES

3.3 *Implementing social media*

Kietzmann et al. (2011) present a guideline, which they call the '4 Cs,' relating to how firms should develop strategies for monitoring, understanding, and responding to different social media activities. These four 'Cs' are cognize, congruity, curate, and chase (Kietzmann et al., 2011) and are described more in-depth below.

3.3.1.1 Cognize

The firm should first recognize and understand its social media landscape (Kietzmann et al., 2011). Larson and Watson (2011) developed a model that depicts the social media landscape, through which they aim to convey the magnitude of complexity introduced into stakeholder interactions by social media technologies. Figure 4 shows a map of all stakeholders from a firm's perspective that might interact via social media, consisting of: citizen/customers, employees, suppliers and corporate customers, government, investors, and the firm itself. As depicted in the social media landscape, these groups can have inter-stakeholder communications (e.g., employee-to-firm), or intra-group communication (e.g., employee-to-employee).

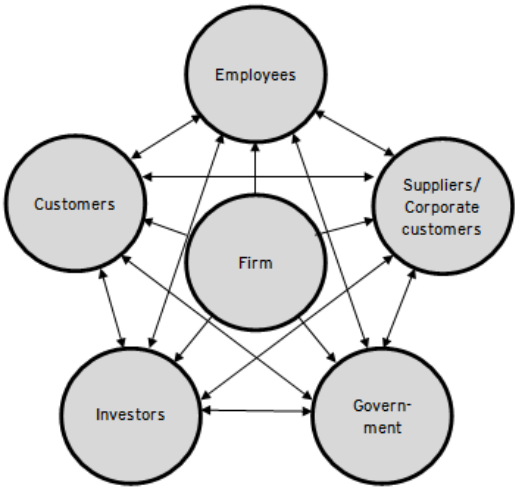


FIGURE 4 | THE SOCIAL MEDIA ECOSYSTEM

Within the firm, there are also some stakeholders that can be identified. These internal stakeholders vary per company, but can be identified from the areas that are affected by social media. This means that stakeholders could also be from different departments within the firm, such as sales, marketing, support, customer relationship management (CRM), HR and R&D (EY, 2012b), or from business leadership, risk management, and legal representation (ISACA, 2012).

3.3.1.2 Congruity

The firm needs to develop strategies that are congruent with, or suited to, different social media functionalities and the goals of the firm (Kietzmann et al., 2011). Safko and Brake (2009) recommend organizations to develop their social media strategies by using a rating scale that ranks social media options from zero to four to denote gradations from "not valuable" to "extremely valuable." Or, by using a "SWOT analysis" to evaluate "strengths and weaknesses," as well as "opportunities and threats." The strengths and weaknesses of the company should translate via social media tools. Opportunities and threats should indicate external factors that might work in favour, or against the firm (Safko & Brake, 2009).

To successfully use social media, organizations should first carefully consider which objectives they are trying to reach with it, and establish some metrics in order to determine if they are successful in their social media use. ITGI (2007) recommends these goals and objectives to be: Specific, Measurable, Actionable, Realistic, Results-oriented and Timely (SMARRT). They should be linked to the business goals and supported by suitable metrics. Some example objectives for different business functions are given by Bernoff and Li (2008). For the R&D department, the authors state that organizations should pursue "listening," by which they mean the on-going monitoring of their customers' conversations with each other, to gain insights from customers and using that input in the innovation process. The objective for marketing is "talking:" using conversations with customers to promote products or services. For the sales department, "energizing" is very important, which is the identification of enthusiastic customers and using them to influence others. According to the authors, organizations should also pursue "supporting," in the customer support department, by which they mean enabling customers to help one another solve problems. The objective for operations is "managing:" providing employees with tools so that they can assist one another in finding more effective ways of doing business.

Bernoff and Li (2008) also give some example metrics of measuring the success of social media use in the different departments, and social applications that can be used best for the different departments. In addition to that, Rozwell, Lapkin and Fletcher (2010) provide for each 'business focus' a key performance measurement example, and some internal and external initiatives that can be undertaken on social media. The recommendations of Bernoff and Li (2008) and Rozwell et al. (2010) were merged into one overview, which is shown in Table 6. For the HR, some metrics and applications were missing, and some recommendations were included in the table for filling these gaps.

3.3.1.3 Curate

The firm must act as a curator of social media interactions and content, which involves developing a clear understanding of how often and when a firm should chime into conversations on a social media platform, and who will represent the firm online (Kietzmann et al., 2011).

Various persons can be responsible for representing the firm online. Common roles involved in this were identified by Owyang (2011) and are: (1) the social strategist, who is the social media leader and program manager; (2) the community manager, who acts as liaison between the community and the brand; (3) the business unit liaison, who represents one or multiple business units; (4) the education manager, responsible for planning and organizing social media education; (5) the social media manager, who manages one or more social media projects; (6) the social analyst, who measures and reports on social media activity; (7) the web developer, who provides assistance; (8) the content strategist, responsible for the coordination of content strategies; (9) the digital strategist, who integrates social media into digital channels; and (10) agency partners, who are third party experts.

	Key performance measure (Rozwell et al., 2010)	Key success metrics (Bernoff & Li, 2008)	Internal initiatives (Rozwell et al., 2010)	External initiatives (Rozwell et al., 2010)	Social applications (Bernoff & Li, 2008)
Marketing *"Talking"*	market share	• better market awareness • online "buzz" • time spent on sites • increased sales	• sentiment analysis data review • sales training course creation • campaign knowledge sharing	• campaign concept testing • event publicity • special offers to followers	• blogs • communities, • video on user-generated sites
Customer service *"Supporting"*	customer responsiveness	• # of members participating • # of questions answered online • decreased # of support calls.	• FAQ database • best practices forum • listening post for actionable insight	• service quality feedback • anticipate customer service support trends • customer support community	• support forums • wikis
Product develop-ment "*Listening"*	time to market	• insights gained, • usable product ideas, • increased speed of development	• project team work space • employee idea management campaigns	• partner idea management campaigns • crowd-sourcing NPD ideas	• brand monitoring, • research communities, • innovation communities
HR *"Recruiting"*	recruitment efficiency	• *recommended success metric: # of employees recruited online*	• development of job descriptions • candidate interviews and evaluation	• alumni network • job posting, candidate search and background check	• *recommended social application: social networking sites*
Sales *"Ener-gizing"*	sales close rate	• community membership, • online "buzz" and increased sales.	• Q&A expertise engine • forecast/review projections • win/loss review	• social network analysis for influence assessment • lead generation	• social networking sites • brand ambassador programs • communities • embeddable widgets
Leader-ship "*Managing"*	operational effectiveness	• # of members participating, • increased operational efficiency, • decreased # of e-mail.	• collaborative decision making • employee "problem" forum	• CEO blog • social media analysis	• internal social networks • wikis

TABLE 6 | GOALS AND METRICS FOR SOCIAL MEDIA USE

Whether a firm should or should not respond to online conversations should be documented in some sort of decision flow-chart. This can be for example a response or escalation chart. These charts are termed by Grant (2010) 'social media triage charts,' which are one-page flowcharts. They define these charts as charts that are easy to share with any staff who use social media, and they are meant to help front-line staff decide what is ok for them to respond to themselves, what might require escalation for someone else internally to respond to, and what might be better for someone in the community (a member) to respond to (Grant, 2010). Below, the social media triage chart of the American Society of Civil Engineers (ASCE) was depicted, as an example of a well-thought decision flow-chart (see figure below).

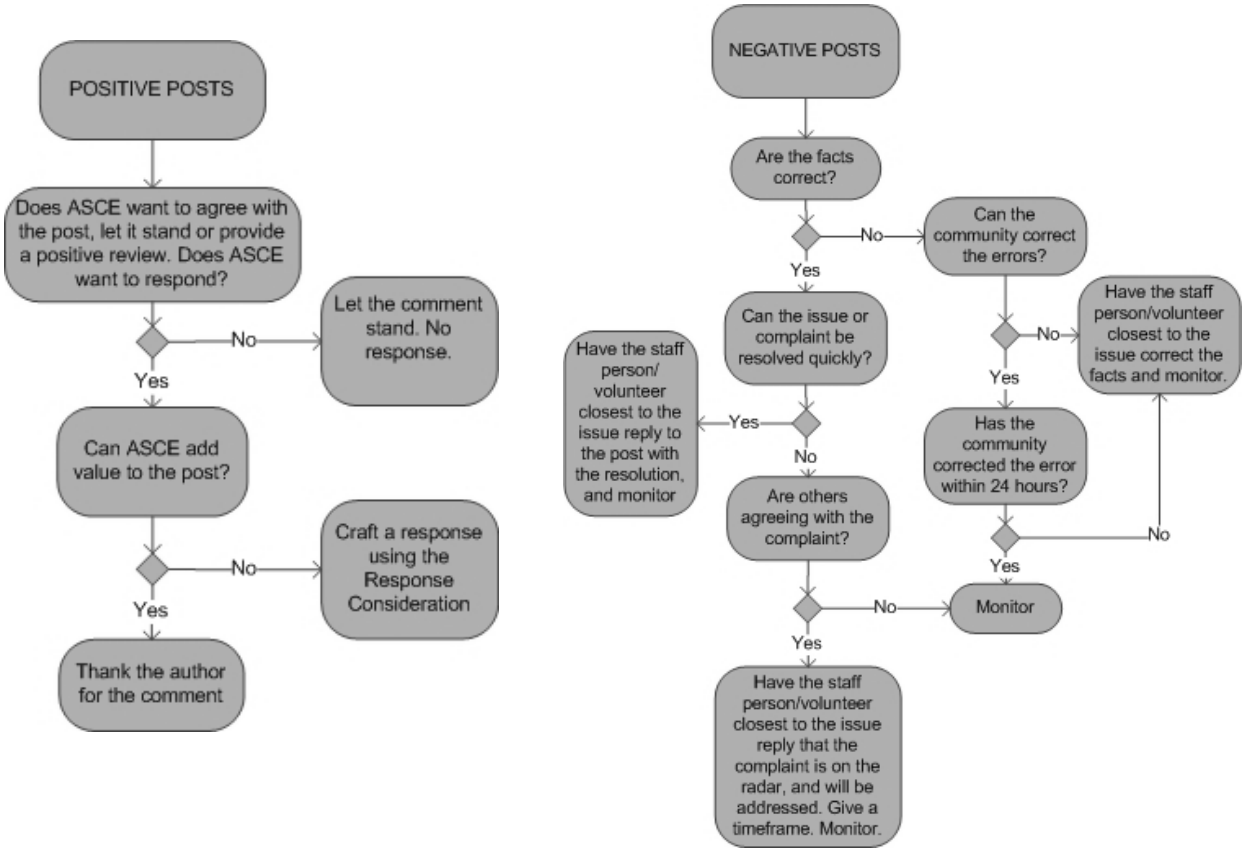


FIGURE 5 | RESPONSE DECISION FLOW-CHARTS OF ASCE (GRANT, 2010)

3.3.1.4 Chase

The firm must scan its environments in order to understand the velocity of conversations and other information flows that could affect current or future position in the market (Kietzmann et al., 2011). This can for example, be done by a PEST analysis, an analysis which is often used in strategic management and describes four macro-environmental factors: political, economic, social and technological. Furthermore, monitoring tools can be used to scan the internet and find mentions of the company name online.

4 GRC

To ensure an efficient use of social media, it should be integrated in the GRC practices of the company. In order to do this, first there has to be a clear understanding of the term GRC. According to Racz et al. (2010b), GRC is an integrated, holistic approach to organisation-wide governance, risk and compliance, ensuring that an organisation acts ethically correct and in accordance with its risk appetite, internal policies and external regulations through the alignment of strategy, processes, technology and people, thereby improving efficiency and effectiveness. In this section, first the general processes of IT GRC are described. Then these processes are applied to social media, terming it social media GRC.

4.1 *IT GRC*

4.1.1 Governance

The definition of corporate governance as provided in the standard ISO/IEC 38500:2008 (ISO, 2008), is as follows: "the system by which the current and future use of IT is directed and controlled. It involves evaluating and directing the plans for the use of IT and monitors this to achieve plans. It includes the policies and responsibilities for using IT within an organization." The ISO/IEC standard recommends three process steps to achieve this: evaluate, direct, and monitor. Ohki, Harada, Kawaguchi, Shiozaki and Kagaua (2009) recommended adding "reporting to stakeholders" as a fourth process step.

So the first step of the governance process is to evaluate stakeholder needs, conditions and options (ITGI, 2007). This can be done, for example by a cost-benefit analysis (Katz & McIntosh, 2013). Then, a direction is set through prioritisation and decision making. Then the performance, compliance and progress against agreed direction and objectives is monitored (ITGI, 2007)**.** The results of this process are reported to stakeholders of the company. These steps were visualised into a PDD, which is shown below.

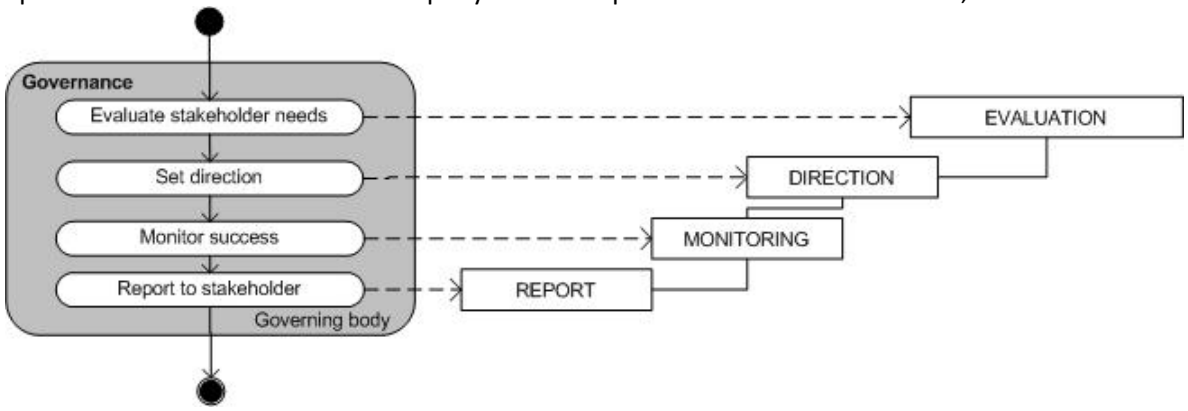


FIGURE 6 | VISUALISATION OF THE GOVERNANCE PROCESS AS DESCRIBED BY (ITGI, 2007)

The governance function keeps oversight on social media. As COBIT (ITGI, 2007) suggests, the governance function and the management function are two separate entities, with the governance function giving direction to the management. The governance function, or governing body, in IT literature is often embodied by the 'C-team' (CEO, CIO, CFO), together with the board and IT committees. Such a committee can either be at the board level (e.g. IT strategy committee), or at the management level (IT steering committee) (ITGI, 2007; Van Grembergen, De Haes, & Guldentops, 2004).

4.1.2 Risk management

According to COSO (2004), enterprise risk management is defined as: a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives. It consists of eight high-level processes (risk components) for risk management: internal environment, objective setting, event identification, risk assessment, risk response, control activities, information and communication, and monitoring.

The risk management process begins with the characterization of the internal environment of the organization. The internal environment sets the basis for how risk is viewed and addressed by an entity's people, including risk management philosophy and risk appetite, integrity and ethical values, and the environment in which they operate. The second process is to set objectives. These objectives support and align with the entity's mission and are consistent with its risk appetite. The third process is to identify internal and external events that can affect the achievement of an entity's objectives. These events may or not may turn into a risk, based on the internal environment and the objectives of the organization. The fourth process is a risk assessment: risks are assessed, based on their likelihood and impact, in order to prioritize the risk and to determine how they should be managed. The next step is to define for every risk an appropriate response: avoiding, accepting, mitigating/reducing, or sharing/transferring risk, and to develop a set of actions to align risks with the entity's risk tolerances and risk appetite. The sixth process is the establishment of control activities, to ensure the risk responses are effectively carried out. The next process is to identify, capture, and communicate relevant information that enables people to carry out their responsibilities. The final process is to monitor risks and make modifications when necessary. Monitoring is accomplished through on-going management activities, separate evaluations, or both (COSO, 2004). The steps of the risk management process were visualised in Figure 7.

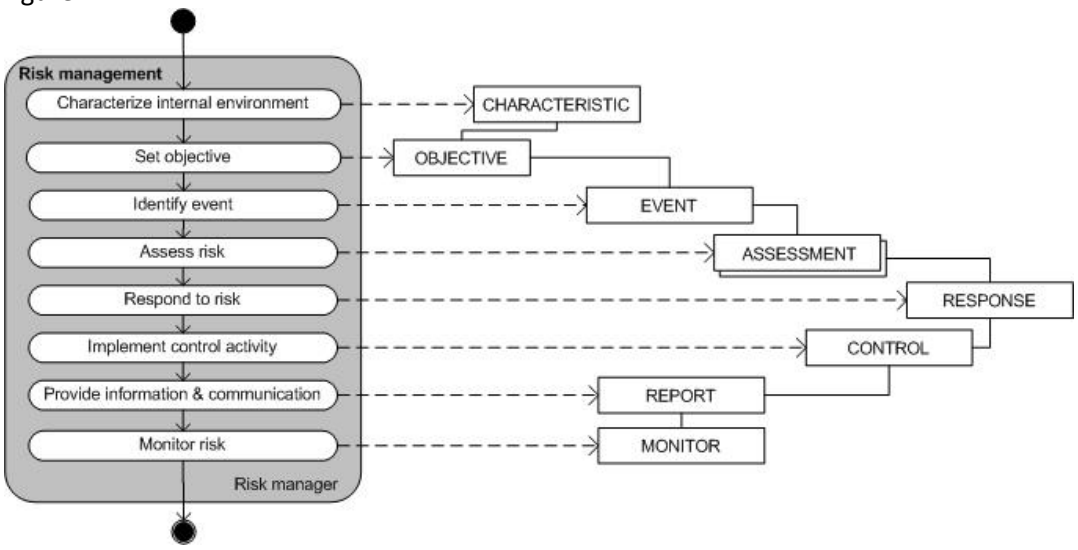


FIGURE 7 | VISUALISATION OF THE RISK MANAGEMENT PROCESS AS DESCRIBED BY COSO (2004)

Risk management can be the responsibility of several persons, but the following key roles who should support and participate in the risk management process can be identified: Senior Management, Chief Information Officer, System and Information Owners, Business and Functional Managers, IT security

program managers and computer security officers, IT Security Practitioners, Security Awareness Trainers (Stoneburner, Goguen, & Feringa, 2002).

4.1.3 Compliance

Compliance is defined by EY (2010) as adherence with policies, regulations and other obligations, managed by an organization's programs, tools and other enablers. (ISACA, 2010) states that just as enterprises must develop an appropriate strategy and controls to manage their use of social media, it is the role of assurance professionals within the enterprise to validate and monitor these controls to ensure that they are, and remain, effective and that compliance with these controls is established and measurable. For compliance the model suggested by Racz et al. (2010a) was adapted. This model divides the general process of IT compliance into four sub-processes: requirements analysis, deviation analysis, deficiency management, and reporting/documentation.

Requirements analysis comprises the identification of regulatory, legal, contractual, and other obligations that affect the organisation's IT operations. Internal policies, such as best practices for software engineering or security guidelines, can also be included. The requirements build the foundation of a company's internal control system as far as IT is concerned. Once the requirements have been identified, adherence is examined for instance through internal and external audits, self-assessments, and security checks. The frequency of these examinations depends on external requirements and on the impact of potential deviations. Whereas a yearly examination will be sufficient in many cases, continuous monitoring may be recommendable in other cases. The results of the deviation analysis define the requirements for deficiency management. At this stage existing deficiencies are eliminated through improvement of existing controls, creation of new controls, or through a makeover of parts of the control system (Racz et al., 2010a). The compliance process is shown in the figure below.

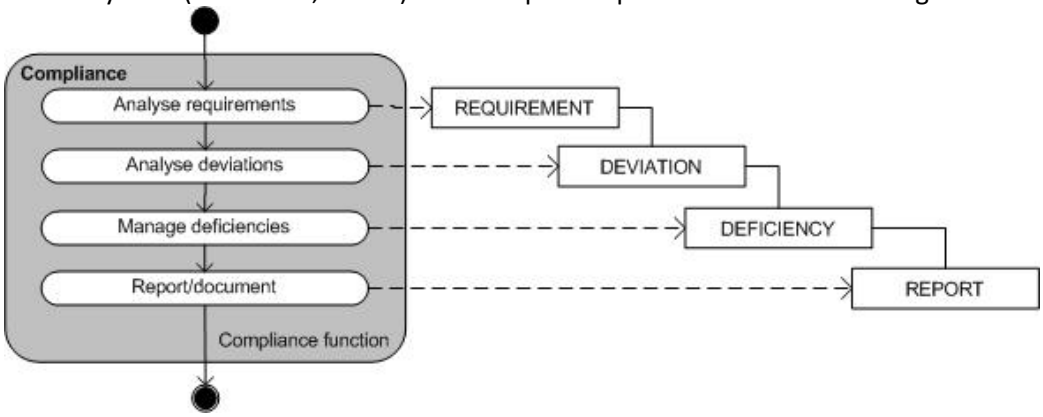


FIGURE 8 | VISUALISATION OF THE COMPLIANCE PROCESS AS DESCRIBED BY RACZ ET AL. (2010A)

Compliance roles are amongst others compliance manager, head of compliance, compliance officers, compliance assistants and other regulatory compliance positions. When audits are required, often third-party experts are involved, such as auditing companies, to perform the audit.

4.1.4 Integration of GRC processes

The three GRC processes described in this section were integrated into a prototype GRC method, which is shown in Section 9.6. This method was used as a starting point for the social media GRC method and was commented on by social media experts and extended with social media practices from both literature and practice. These practices are described in the next section.

4.2 *Social media GRC*

In this section, the GRC processes described in the previous section are applied to social media. The steps that were identified and explained in the previous section are now made more specific for social media by merging literature on social media governance, risk management and compliance, and IT GRC literature.

4.2.1 Social media governance

Before discussing the steps of social media governance, it is first important to identify the role(s) that performs the governance process. Governance is often performed by a governing body, which is a central decision-making group or team: this is the group or team that is responsible for a certain project or process. For social media, there are three important governing bodies, of which two are taken from IT governance literature, and one from literature on social media. From IT governance literature, the two important governing bodies identified were: the C-team (CEO, CIO and CFO) and the board. These governing bodies are also important for social media, as they are involved on a strategic level: the C-team and the board have to evaluate business opportunities and make strategic decisions. The governing body found in literature was found at companies that make 'advanced' use of social media in practice by Owyang (2011), and is called the social media team, hub, or 'center of excellence' (CoE). While the C-team and the board are functioning on a strategic level, the social media team or center of excellence is functioning on the management level. This team is responsible for the implementation of social media, and for making sure that social media rules are made known to employees, and to monitoring the compliance to those rules.

Next to a governing body, corporations should establish a governance structure when implementing social networking (Turban et al., 2011). Several structures for social media governance were found in practice by Owyang (2011): organic, centralized, coordinated, multiple hub and spoke, and holistic. The governance structure indicates who is responsible for social media in the organization, and which decision-making flows there are. According to Owyang (2011), the coordinated structure was the most effective structure for governance, with a social media center of excellence as central group.

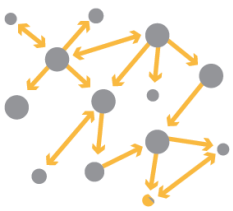
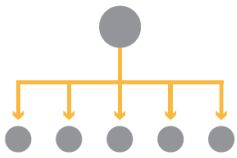
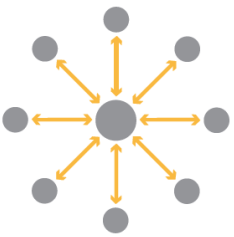
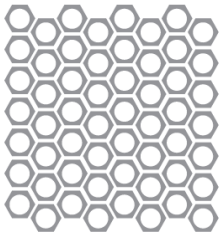
Organic	Centralized	Coordinated	Multiple hub and spoke "Dandelion"	Holistic "Honeycomb"
				
Notice that the dots (those using social tools) are inconsistent in size and one set of employees are not directly connected to others	*Notice that a central group initiates and represents business units, funnelling up the social strategy to one group*	*Notice how a central group will help to provide an equal experience to other business units*	*Notice how each business unit may have semi-autonomy with an overarching tie back to a central group*	*Notice how each individual in the organization is socially enabled, yet in a consistent, organized pattern*

FIGURE 9 | GOVERNANCE STRUCTURES AS IDENTIFIED BY OWYANG (2011)

Now the governing body and structure for social media are identified, the steps for social media governance can be further explained. The governance processes that were identified in the previous section are: evaluation, direction, monitoring and report. For social media governance, the monitor and report step are merged, as the 'reporting' step reports the results of the monitoring step.

4.2.1.1 Evaluation

The first task in the governance process is to evaluate stakeholder needs, conditions and options (ITGI, 2007). As the modern customer and workforce have become more demanding, and want organizations to be 'online,' this could well be a need for companies to start using social media. The governing body will evaluate this need for possible up- and downsides. According to Katz and Mcintosh (2013), it may be useful to conduct a cost-benefit analysis of participating in social media with respect to investors and analysts as opposed to simply customers. They state that such an exercise could involve reaching out to large investors for their views, examining how competitors handle social media, as well as carefully addressing compliance concerns (Katz & McIntosh, 2013).

4.2.1.2 Direction

The second task for the governing body is setting a direction through prioritisation and decision making (ITGI, 2007). This is done in a social media strategy, which defines the goals of social media use, and metrics to measure the achievement of these goals. How to develop and implement such a strategy, which stakeholders are involved, and which goals and metrics to use are discussed in Sections 3.3.1.1, 3.3.1.2, 3.3.1.3, and 3.3.1.4.

According to ISACA (2010) any strategy to address the risks of social media usage should first focus on user behaviour through the development of policies. Policies are an important tool for governing social media use as they represent official positions that govern the use of social media by employees in organizations, such as detailing what constitutes acceptable use or outlining official processes for gaining access to social media sites (Hrdinová, Helbig, & Peters, 2010). The authors state eight essential elements for a social media policy, which are: (1) Employee Access: describes which employees may access social media sites and what should be the process for gaining access, (2) Social Media Account Management: encompasses the creation, maintenance, and destruction of social media accounts, (3) Acceptable Use: outlines an organization's position on how employees are expected to use agency resources, restrictions on use for personal interests, and consequences for violating the policy, (4) Employee Conduct: in addition to a standard conduct code, to address issues more specific to social media, (5) Content: who is allowed to post content on official agency social media pages and who is responsible for ensuring its accuracy, (6) Security: ensure the security of data and technical infrastructure in light of the new uses, users, and technologies related to social media use, (7) Legal Issues: ensure that employees are abiding by all existing laws and regulations, (8) Citizen/Customer Conduct: whether or not allowing two-way public communication between firm and customer and rules for acceptable conduct of customers (Hrdinová et al., 2010). ISACA (2010) recommends that social media policies for companies should be split up in three sections: personal use in the workplace, personal use outside the workplace, and business use.

Another important step in directing social media use is the allocation of roles and responsibilities (EY, 2010). As said before, according to Owyang (2011), the social media responsibility can be best centralized at a social media "center of excellence." Within this CoE, some commonly found social media roles were identified, which can be used for assigning responsibilities to. Those roles were discussed in

Section 3.3.1.3. When assigning responsibilities for social media, it is common practice at companies to use RACI charts (ITGI, 2007). This chart identifies who is Responsible for, Accountable for, Consulted for, and Informed about the deliverable. An excerpt for an example RACI chart for social media policies and strategy is shown below.

	Executive board	Corporate director SM	SM leadership team	Director SM NL	Social media team
Social media policy	A	A	C	R	R
Execution of the social media policy		I	I	R	R
Annual social media strategy		A	C	R	R

TABLE 7 | EXAMPLE RACI CHART

4.2.1.3 Monitoring and reporting

The last steps in the governance process are the monitoring of performance, compliance and progress against agreed direction and objectives (ITGI, 2007), and the reporting hereof to stakeholders (Ohki et al., 2009).

4.2.2 Social media risk management

No evidence from literature was found that indicated a specific social media risk management process. Therefore, it is assumed that social media risk management falls under the ordinary risk management process, and that social media risks are included in this process. In this case, social media risk management is performed by the risk manager of the company, or any other person, team or department that is responsible for this.

For risk management, eight steps were identified in the previous section: internal environment, objective setting, event identification, risk assessment, risk response, control activities, information and communication, and monitoring. For social media risk management, those steps were comprised into the following three: risk identification (containing environment, objective setting, and event identification), risk assessment (containing risk assessment), risk mitigation (containing risk response and control activities), and monitor and report (containing information and communication and monitoring).

4.2.2.1 Risk identification

Risk identification comprises of the first three steps of the risk management process: characterizing the internal environment, setting objectives, and identifying events (COSO, 2004). Characterizing the internal environment consists of: defining the relationship of organization with its external and internal environment, performing SWOT analysis, identifying stakeholders, understanding organization's objectives and strategies, identifying key performance indicators (KPIs), identifying relevant key risk categories, identifying existing risk management practices, determining the "risk appetite" of management, and determining integrity and ethical values of the organization (COSO, 2004). Objectives must exist before management can identify potential events affecting their achievement. Enterprise risk management ensures that management has in place a process to set objectives and that the chosen objectives support and align with the entity's mission and are consistent with its risk appetite (COSO, 2004). The objective of performing risk management is to enable the organization to accomplish its

mission: (1) by better securing the IT systems that store, process, or transmit organizational information; (2) by enabling management to make well-informed risk management decisions to justify the expenditures that are part of an IT budget; and (3) by assisting management in authorizing (or accrediting) the IT systems on the basis of the supporting documentation resulting from the performance of risk management (Stoneburner et al., 2002). Then, internal and external events affecting achievement of an entity's objectives must be identified, distinguishing between risks and opportunities (COSO, 2004). Possible events, which may become risks, were identified in Section 3.2.2.

4.2.2.2 Risk assessment

Risk assessment is about determining the likelihood and impact of the identified social media risks (Stoneburner et al., 2002). First, risks are rated on the probability or likelihood they will occur, and then the impact is will have when the risk occurs is rated. The final determination of overall risk is derived by multiplying these ratings. An example hereof is given in Figure 10. The matrix below is a 3 x 3 matrix of threat likelihood (High, Medium, and Low) and threat impact (High, Medium, and Low). Another way to visualize the likelihood and impact of social media risks is by risk mapping, for example on a probability/severity chart (Scandizzo, 2005). An example of such a mapping can be found in Figure 10. Risks can be mapped according to the four mapping areas: non-threatening, disastrous, de minimis, and threatening. Some examples are given in the figure: a 'de minimis' risk is for example when the company account is hacked and the hacker posts swear words on the corporate site. A 'threatening' risk for example is when medical records are hacked or in the possession of someone that is not authorized for that, and he or she posts them online. An example of a 'disastrous' risk is social engineering. Based on the assessment of the likelihood and impact of the risk, management can assign priorities to the risk, choose a risk mitigation strategy and controls.

Impact / Likelihood	Low (10)	Medium (50)	High (100)
High (1.0)	10 x 1.0 =10	50 x 1.0 =50	100 x 1.0 =100
Medium (0.5)	10 x 0.5= 5	50 x 0.5= 25	100 x 0.5= 50
Low (0.1)	10 x 0.1 = 1	50 x 0.1 = 5	100 x 0.1 = 10

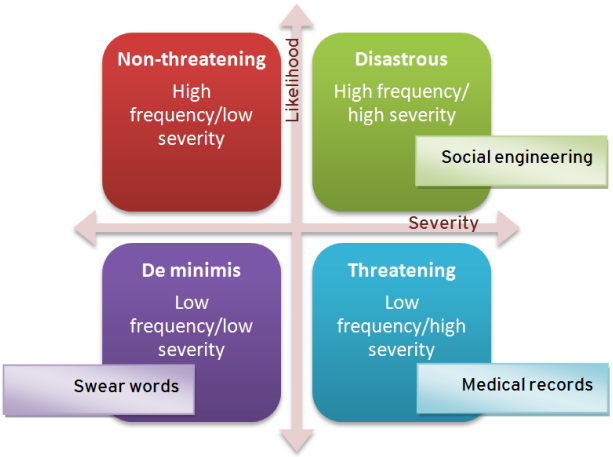


FIGURE 10 | RISK MAPPING METHODS

4.2.2.3 Risk mitigation

The output of the risk assessment process helps to identify appropriate controls for reducing or eliminating risk during the risk mitigation process. From literature, the following controls for social media use can be identified: policies and guidelines (BITS, 2011; Turban et al., 2011), training and awareness programs (BITS, 2011; Turban et al., 2011), content filtering and blocking (BITS, 2011), crisis management (BITS, 2011) and access control (Turban et al., 2011). Five risk mitigation techniques can now be distinguished: policies (guidelines and best practices), education (training and awareness), monitoring (filtering and blocking), access control, and crisis management.

Policies. Policies are set out by the governing body in order to control social media use. As a risk mitigation technique, policies are often translated to guidelines and best practices for more hands-on guidance. Guidelines provide advice on how to best use social media tools to achieve a desired result, such as eliciting customer engagement or providing suggestions for creating interesting content (Hrdinová et al., 2010). Frequently stated topics in social media guidelines are "behavioural etiquette in social media", "contact persons for social media activities", and the "separation of professional and private comments" (Zerfass et al., 2011). Next to guidelines, companies use 'best practices' for efficient use of social media. For example, they specify a target amount of posts that should be made on Facebook on a daily basis.

Education. Educating the prospective members of a social network will help not only in communicating the governance structure and policies, but may also mitigate resistance to joining and/or contributing (Turban et al., 2011). To make employees aware of the policies and guidelines concerning social media use, social media events, workshops and trainings should be given.

Swallow (2011) defines six steps to establish a social media training program, based on cases from practice: (1) Establishing a decision-making team established that is in charge of social media. In this team should be a social media strategist and key team members from the following areas: marketing, legal, product, and web development. (2) Assessing the company's needs from social media to gain a better understanding of the goals for the training program. Questions to be asked are: What is the overall social media strategy, and where does the education program fit within it? And which employees and business units should be focused on in the training program? (3) Benchmarking employees on their social media knowledge to see what they already know. (4) Setting the curriculum for the education program. (5) Creating training materials that add value to the courses, such as e-learning courses, quizzes, case studies, white papers, newsletters, and other resources. (6) Getting employees excited about and enrolled in social media training (Swallow, 2011).

Monitoring. According to Culnan, McHugh and Zubillaga (2010), companies should monitor the content that users create and subsequently monitor use for compliance. So, monitoring tools can be used to detect mentions of the company brand or name online. The company can review this comments, and decide if they want to respond to the comment, or when it is a very insensitive or untrue comment, have it removed. Monitoring can also be used to measure the compliance level in the organization. For example, online monitoring can detect when a staff member accesses a social networking website like MySpace, Twitter or Facebook or even views online pornography. Some monitoring and tracking apps can record usernames and passwords, log blog posts and identify those employees who waste time by shopping or playing games online, and track how much time an employee wastes with this (Toptenreviews, 2013). The employer can also use monitoring tools for their content filtering features or for the blocking of websites, to prevent employees from executing specific applications or accessing websites that contain objectionable content, for example online games, dating, social networking and social media websites. (Culnan et al., 2010) state that it is important to note that monitoring (knowledge) content differs from monitoring for compliance with company policies and that depending on the application, the individuals performing the monitoring could be for example, in customer service, corporate communications, or marketing.

Access control. Access control is an important mechanism that defines allowable user groups, what information users can access and their expected usage profiles (Turban et al., 2011). According to (EY, 2012d), the following access controls should be in place: (1) a change management process to document changes, (2) separation of jobs and responsibilities to prevent unauthorized or unwanted changes (3) separation between the development, test, and production environment to prevent unwanted changes, (4) a user management process to prevent the creation of users with unwanted authorization, (5) controlled access to accounts with high authority, (6) password restrictions, (7) verification of accounts and settings. Furthermore, security mechanisms that are specifically designed for Web 2.0 technologies can be employed to supplement the existing protection mechanisms of information systems infrastructure.

Crisis management. According to the BITS (2011), a company's crisis communications plan must include both defensive use of social media (that is, a program to monitor online channels and identify and escalate threats) and proactive use of social media (to publicize company developments, engage with various stakeholders, and to speedily address erroneous or malicious information that may be circulating online). They state that to detect and respond to negative content in a timely way, a company must continually monitor for threats to its reputation and image and have a plan for rapidly addressing those threats. This plan should include: (1) Clear criteria for identifying risk that is likely to develop into a crisis, (2) An escalation process that details next steps in addressing the crisis, and (3) Robust pre-crisis preparation, detailed responses for different kinds of crisis, and a process for evaluating the success of crisis response (BITS, 2011). The chart outlined in Figure 11 is an example of a decision flow-chart for a social media crisis, in this case, the breach of a policy. The chart was provided by the ASCE. The chart is intended to supplement, not supplant, a company's existing crisis communications strategy to incorporate social media considerations (Grant, 2010). Each company will need to determine the best way of integrating these steps into their traditional crisis planning.

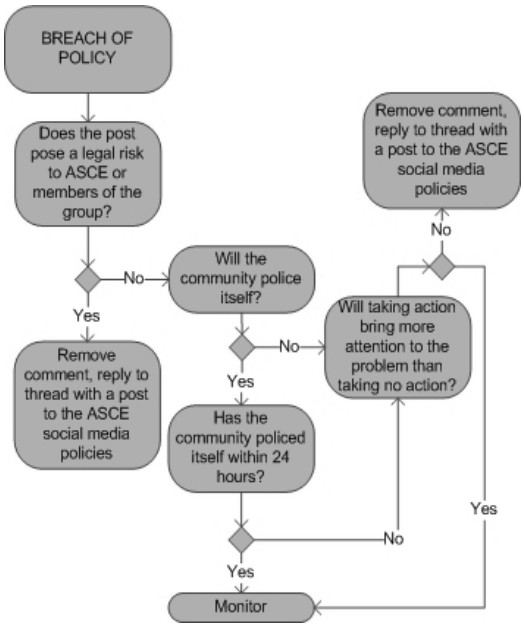


FIGURE 11 | CRISIS DECISION FLOW-CHART

4.2.2.4 Monitor and report

The results of the risk management process should be reported to the governance layer. Examples of topics included in this report are: the main risks or most important risks the company is facing, an estimation of their likelihood and impact, controls that are in place to mitigate the risk, and how effective these controls are in mitigating the risk, by for example, measuring security breaches and other violations.

4.2.3 Compliance

Compliance checks are performed be the audit function and therefore, the role that is responsible for the compliance process is the audit team. For compliance, the following steps were identified: requirements analysis, deviation analysis, deficiency management, and reporting/documentation. These steps were somewhat altered for social media compliance, resulting in the steps: requirements analysis, identify and analyse deviation, deficiency management, and monitor and report.

4.2.3.1 Identify requirement

Identifying requirements for social media may vary per organization: some companies will perform a SWOT analysis, some perform a stakeholder analysis, others try to set measurable goals. However, (Owyang, 2011) found four internal requirements that companies have in place that are more 'advanced' in their social media use than other companies. These are: (1) Baseline Governance and Reinforcement: established and reinforced a corporate social media policy that allows employees to participate professionally, (2) Enterprise-Wide Response Processes: defined processes for rapid workflow and engagement with customers in social media, (3) On-going Education Program and Best Practice Sharing: fostered a culture of learning through on-going social media education, (4) Leadership from a Dedicated and Shared Central Hub: organized in a scalable formation, with a cross-functional "Center of Excellence" (Owyang, 2011).

4.2.3.2 Identify and analyse deviation

The next step is to identify and analyse any deviations from these requirements. According to (Racz et al., 2010a), this can be examined through internal and external audits, self-assessments, and security checks. The frequency of these examinations depends on external requirements and on the impact of potential deviations. According to (ISACA, 2010), the elements of an audit should include questions about: (1) Strategy and Governance - Has a risk assessment been conducted to map the risks to the enterprise presented by the use of social media? Is there an established policy (and supporting standards) that addresses social media use? (2) People - Has effective training been conducted for all users, and do users (and customers) receive regular awareness communications regarding policies and risks? (3) Processes - Have business processes that utilize social media been reviewed to ensure that they are aligned with policies and standards of the enterprise? (4) Technology - Does IT have a strategy and the supporting capabilities to manage technical risks presented by social media? Do technical controls and processes adequately support social media policies and standards? Does the enterprise have an established process to address the risk of unauthorized/fraudulent use of its brand on social media sites or other disparaging postings that could have a negative impact on the enterprise?

Compliance can also mean the adherence of employees to the company policy. This can occur in varying levels, from 'commitment' to 'disobedience'. These levels can be found in the table below (Harris & Furnell, 2012). In order to ensure compliance, organizations should have training and awareness programs in place to make employees aware of the policies and rules on social media, and sanctions should be in place when policy is violated (Harris & Furnell, 2012).

Compliance	Culture	The ideal state, in which security is implicitly part of the user's natural behaviour
	Commitment	Security is not a natural part of behaviour, but if provided with appropriate guidance/leadership then users accept the need for it and make an associated effort.
	Obedience	Users may not buy into the principles, but can be made to comply via appropriate authority (i.e., implying a greater level of enforcement than simply providing guidance).
	Awareness	Users are aware of their role in information security, but are not necessarily fully complying with the associated practices or behaviour as yet.
Non-compliance	Ignorance	Users remain unaware of security issues and so may introduce inadvertent adverse effects.
	Apathy	Users are aware of their role in protecting information assets, but are not motivated to adhere to good information security practices.
	Resistance	Users passively work against security, through factors such as laziness and disregard for known procedures.
	Disobedience	Users actively work against security, with insider abusers intentionally breaking the rules and circumventing controls.

TABLE 8 | LEVELS OF COMPLIANCE (HARRIS & FURNELL, 2012)

4.2.3.3 Deficiency management

Deficiency management is the improvement of existing controls, or creating new controls. As stated earlier, controls that should be properly in place are: policies, education, monitoring, access control, and crisis management. Some examples are given on how these controls could be improved. Policies should be set out by the governing body, and any improvement of policies could be: increasing the awareness of employee about the policy by training and education programs, creating policies specifically for social media, and providing more hands-on guidelines and best practices for social media use. Education should also be set out by the party that is responsible for social media and should be repeated on a regular basis to keep employees knowledgeable and up-to date. An improvement here therefore could be implementing regular education programs. An improvement for monitoring could be the purchasing or updating of a monitoring tool, for example. Access control could be improved by changes in the system, and making more restrictions on who can and cannot access something. Crisis management could be improved by implementing and communicating a clear crisis response plan or triage chart.

4.2.3.4 Monitor and report

The results of the compliance process are reported to the governance layer. This report will include information on the identified deviations, and what was done in the deficiency management step to improve this.

5 Expert interviews

In this section, the results of the expert interviews are presented. For every interview, a protocol was followed, consisting of three steps. First, information about the company was gathered from the corporate website, their social media pages and other relevant websites. This information was used to get a general idea of the company, to see which social media channels the company used, and to see if they really were active on these channels and was used in the 'general' section of each company (the italic sections). The second step was to conduct an interview with a social media expert or person that was otherwise involved in social media at his or her company. The interviews were recorded and transcribed, and a summary containing key quotes and statements of the interview was created. The third step was to send the summary back to the interviewees for their validation and approval.

The aim of the interviews was first to validate the findings from literature. Were the (GRC) practices that were identified in literature in place in real-life companies? Were the social media risks found in literature seen as actual risks by the interviewed companies? The second aim of the interviews was to validate the prototype method for social media GRC. The method was shown to the interviewees for feedback: it was first explained to the interviewees and then they were asked if they would make any changes to it, or if they had any tips, additions, or other recommendations to make. The feedback was used to improve the method.

The interviews were held with subject matter experts. These persons were 'social media experts' in their organization, and they fulfilled different roles in their organization, dependent on which department was responsible for social media. For example, some interviewees were risk managers, some were from the communications department and another interviewee was from the audit. The precise role of each interviewee can be found in Table 2.

The interviews all had the same structure and questions, by using an interview guide. This guide can be found in Section 9.1. So, the interviewees were first asked some *general* questions on social media: which social media channels, which goals they try to achieve with social media, which benefits social media has in their opinion, and what their attitude is towards social media use (for example, do they see it as a 'hype,' or do they think it is the new way of doing business? Do they see a strategic value to social media use?). Then, some questions were asked about *governance* of social media in the organization: who is responsible for social media? Are there policies and guidelines for social media use? After that, some questions on social media *risk management* were posed. Did the interviewees see any risks to the used of social media? Did their company have controls in place to mitigate those risks? Finally, some questions were asked on *compliance*. How did the company ensure compliance? The interviews had a duration of 15-90 minutes and were all recorded and transcribed. For the precise duration of each interview see Table 2.

5.1 *Interview summaries*

As said before, the interviews were recorded and transcribed, and a summary containing key quotes and statements of the interview was created. These summaries are presented first, to give an idea of the general opinion and uses of social media in companies. For an overview of these summaries, see section 5.3.1.

5.1.1 Company A

Company A is a large internet retailer, operating throughout Australia, North and South America, Europe, Asia, and New Zealand. Company A has a strong presence on Twitter and Facebook and is pretty active on those social media. Social media is seen as a marketing engine primarily: it is used mainly for advertising purposes, such as communicating discounts and special offers to the customer. "I say eighty percent of what they're looking to get out of social media is advertising, word-of-mouth, expanding the customer care program, those kind of things." However, on the long term, the desire of Company A is that social media will help reach the goals the company is trying to achieve. "How can [social media] make it easier? Easier to talk to the customer, easier for the customer to have questions, see what is going on, […] talking to the consumer."

Governance

The responsibility for social media at Company A lies within the marketing department. Within the marketing department, there is a specific group that handles online communications, however it is not clear if in this group there are specific roles with specific responsibilities for social media. There are policies and written rules at Company A about the use of computers and internet, which also apply to social media.

Risks

Company A acknowledges risks associated to social media and sees reputational risk as most relevant to the company. More specifically, there are three risks that can be identified which negatively impact the company brand:

- **Negative comments.** There are a lot of customers that bring up an issue or lodge a complaint on the company's social media page. *"When you go the Company A Facebook page, you probably find a good half-dozen people going: I ordered this product and I got something else, how can you mess this up?"*
- **Client trust.** Another risk that was brought up during the interview is related to client trust. Company A tracks customers and has a lot of information about their customer that they can use. However, customers not always like the fact that this information is known, or are surprised that the company has the information. *"Sometimes when people give their information to us, they don't remember they gave it to us, and then they start asking: how did you have my address?"*
- **Pre-announcements.** Another risk that Company A acknowledges comes from inside the company. For Company A, this risk mainly comes from employees who prematurely post news about the company online. For example: "*It was a month ago, or two months ago, even our senior vice president of retail posted something on Twitter that got picked up and everybody thought it meant we were going to start selling […] products in the US, and it hit the news. It was a little premature, I don't think we were quite there yet."*

An important element of these audits is how the company is educating its user community on security and awareness or security awareness.

To control the risks associated with social media, Company A has some controls in place, amongst which are:

- **Monitoring.** Company A is tracking web- and Facebook activity. There is a team that monitors and responds to complaints posted on social media. However, there is not an active scanning or monitoring of employee posts of Company A.
- **Training and awareness.** In accordance with Company A's annual compliance requirements, every employee gets some sort of electronic security or privacy education. This can be training sessions, but also worldwide privacy days. Topics of this education are: *"remember when you are on social media, what can happen, remember you're probably privileged to submit information that the general public doesn't have about Company A, posting on Facebook or Twitter violating company policy, so there is this sort of perpetual flow of information to the average user."*
- **Blocking.** There is some blocking software in place at Company A that filters out: *"kind of the far fringe, the hate speecher, known malware locations, etcetera."*
- **Crisis response**. Company A has a crisis response plan, which is to be enacted based on any number of criteria, for example in response to a virus, or in response to the hacking of a social media account. A specific internet response group handles the crisis.

Compliance
Company A falls under a couple of different audits, of which the two biggest audits are PCI and SOX. An important element of these audits is how the company is educating its user community on security and awareness or security awareness. There is a number of methods to do that with, amongst others: awareness days, online training, sign-offs, etcetera. At Company A these mechanisms are in place, and they are audited by multiple entities in a year. There is also tracking to know who is taking what training.

When an employee is considered to be doing something illegal, unethical, or not compliant with company rules, a manager or an executive can ask for an investigation about the employee, and then the posts of that person are checked. When an employee is in breach with corporate rules, there are sanctions all the way up to termination of the contract, depending on the severity of the breach.

5.1.2 Company B

Company B is a medium-sized foundation, active in the public sector, which operates in the Netherlands. Currently, Company B is active on various social media: Twitter, Hyves, Facebook and LinkedIn. Company B also uses Narrowcasting, a form of presentation for a closed community, especially for their audiences. They use social media mostly for profiling, and creating a positive company image. An implicit objective of building a positive company image is attracting new employees or employers: "it helps to put yourself out there, because that's what we want, brand awareness, as they say in marketing terms, that is an important objective. Both to attract future staff and employers." As said before, another goal that Company B tries to achieve with the use of social media is to 'listen' to the general opinion about the company, and to be able to react quickly to any comments.

Initially, Company B did not allow the use of social media and used blocking software to prevent employees from visiting social media websites. This mainly had to do with security issues, and the fact that the company did not feel quite 'ready' for using social media yet. However, Company B eventually realized that this block could not be maintained, as they were pressured by two parties to start using social media: first, the communications department wished to start using social media, to 'listen' to online communications about Company B. Second, there was a pressure from the market, as being a 'modern' company requires the use of social media. Even with a great fear from the network administrators, the block on social media was gradually lifted. However, the company remained aware of the risk accompanied by social media. They state: "if the company wants [to use social media], then it also accepts a certain risk. And this risk cannot be entirely overseen."

At Company B, there is no specific strategy for social media and social media is not included in the company strategy. This also has to do with the fact that the company is undergoing some changes in how their business is set up. Not only changes that come from within the company, but also various external requirements that the organization has to comply to. When things are more stable again, Company B might look into this.

Governance

The responsibility for social media lies within the communications department. This department controls the social media pages, and keeps them up-to-date with content. Supportive to the communications department are the crisis team and the IT department. The crisis team is aired when there is an incident. It is not specifically focused on social media, but will definitely use social media to indicate to the outside world what happened, and how Company B will handle the situation. The IT department provides support with the technical aspects of social media.

There is no real policy specifically for social media. *"I think the policy is that we ensure that the greatest risks are mitigated, so that there are solutions put forward. You could also say that communication creates content, responding to signals from the market, we have a crisis, we have employees who sign a confidentiality agreement, so there is a policy but if you ask me: do you have a book in which all that is documented, then the answer is no. But I have no problem with that because I think we can respond quickly to new developments, without being stuck in files and documentation. So it's not really that we do not have a policy, but it is perhaps less formally organized. But we do have the intention that if something happens, we react quickly. I think that's the most important thing: that we know where to find each other when needed."* There are however, other policies in place, such as a confidentiality protocol that every employee has to sign to act in line with company rules, but these are not specific to social media.

Risks

Company B acknowledges some risks related to social media. The first one comes from a technical perspective, and focuses more on external attacks which could have impact on network security and availability: *"trying to prevent your data center from being bombarded with malware."* Another risk that is of high importance to Company B is that of damage to the company image: *"how do you ensure that an employee does not make incriminating statements? And what to do when certain tendencies arise that you do not want? That is much more difficult to control."*

Something that Company B has noticed, but which they not specifically mention as being a risk, is the loss of employee productivity. This can be twofold: it can be employees that are less productive because they spend a lot of time on social media, but it can also be the IT department that spends a lot of time on maintaining and controlling social media profiles of employees (which for example have to be adjusted to fit the company image), thereby having less time to spend on their ordinary tasks.

However, the comment is made that social media and new technology maybe costs a lot of time, but also saves time. *"We should not forget that [...] departments used to spend a lot of time and energy in making newsletters, printing these newsletters, and circulating them, and now this is all taken care of digitally. So there is a lot of time, productivity won because you have an alternative way to bringing things out in the open."* To control social media risks, the company has various technical controls and software for keeping their network safe. *"You should think of firewalls, packages that are able to detect malware, certain strings of text, and combinations to keep and which to place a kind of suspicious area so we can see what it is before it is admitted to the email environment."* Company B states that to be really aware of the risks, something should first go entirely wrong.

> *"Departments used to spend a lot of time and energy in making newsletters, printing these newsletters, and circulating them, and now this is all taken care of digitally. So there is a lot of time, productivity won because you have an alternative way to bringing things out in the open."*

Compliance
When a comment is posted online by an employee, which is damaging the company brand, then steps are taken against this employee. However, if it is just someone's opinion, then Company B only tries to contrast it to something else, to keep a balanced company image. What Company B really tries to prevent is escalation of any issues, so when an issue arises, it is quickly brought up to the board, which decides how to deal with it.

5.1.3 Company C

Company C is a global organization active in the consumer products. The company owns a variety of brands and operates in over 100 markets. The company is active on Facebook, Twitter and LinkedIn. Company C acknowledges the fact that the world has changed and that consumers have become a party which importance for a company's success should not be underestimated. By taking part in the online conversation, Company C wants to stay in touch with its consumers. "The way the world is now, with the advent of not just internet, but social media, Twitter, Facebook, and all these types of global things, it is really the first time that the consumer themselves, is also part owner of your brand. And they have the power to make or break your brand. That was not possible with print or TV. But now, very quickly, they can destroy your brand, and at the opportunity side, you can obviously communicate with millions of people." So, Company C recognizes social media is both a risk and an opportunity: "a risk is an opportunity and an opportunity is a risk. And social media is really a fantastic example of a risk and an opportunity being one and the same thing."

Company C tries to seize the opportunity by doing online campaigns, and digital media promotions to push their message to the consumer, and monitor the conversation in order to be able to react. Company C experienced social media being a risk by a social media incident, or 'crisis,' that they had a while ago, which really made the company aware of the impact social media can have on their brand.

"The good thing was; we already identified social media as a risk, but this really made it real." Company C argues that, as there is a social element to their product, they are in some respect more affected by a social media incident.

Governance

At Company C, there is not one specific department or person that is responsible for social media, but it is divided amongst several departments, and this can differ on the global, regional or local level. In most local companies there is a digital team that consists of digital marketers, which are responsible for pushing information to the consumer via social media. There is a team of IT that is involved in social media, and that provides support from an IT perspective. When there is a risk related to social media, a number of functions and teams is involved in investigating and responding to the risk. For example crisis management, this is ultimately owned by global corporate relations. Global marketing is responsible for the rules, standards and guidelines on digital communication. And there is a business department within legal, that ultimately is the board of the company, that creates the guidelines on how people should behave in general. *"So depending on what angle you're coming from there are different owners […] it's very much about the relevant parties working together, knowing who is doing what, etcetera. It is not just a marketing issue."*

Another important element is that every employee has a responsibility towards social media. *"Every employee of this company has a responsibility with regard to our brand. I mean, […] ultimately they can speak on our behalf. If I put something on my Facebook page, I can speak on behalf of the brand. Others know I work for the company, etcetera. So, everybody in this business should feel like a brand ambassador."* This means acting in accordance with social media policies and guidelines, and ultimately, also with the global code of conduct.

Risk

The risk process at Company C has several processes: risk identification and analysis, mitigating, actions, etcetera. This is an annual process, owned by the executive director strategic planning and business control, and integrated in the strategic action planning. This planning is a three-year planning cycle. So every third year there is a full risk assessment, bottom-up and top-down, and in the interim years these risks are monitored, any new emerging risks are identified, documented in a risk register, and the progress is monitored. Risks can be added each year, or can be dropped off because they are solved. Important risks are included in a top 10 risk register, and a global top 25 risk register. At Company C, social media is on the global risk register.

Global audit plays a role in helping and facilitating the risk process. The input for the audit planning comes amongst others from the risk registers. The audit function looks at specific risks associated with social media, and validates the risk and opportunity. First, they identify any risks, think about how to monitor the conversation, how to identify and respond to any issues? *"Is there an escalation procedure, who handles the communication, how timely can we respond to an issue, who is involved, marketing, corporate relations, etcetera, so who is your spokesperson?"* As a global organization, there are a lot of things that should be taken into account: for example, the number of brands that should be monitored, ranging from global to local brands, different time zones, different languages, etcetera. *"Also, audit-related: how do you document all the information, how do you store all the information, and the access to certain levels of information, who can speak on behalf of you?"* Another thing that should be considered is ownership of the monitoring process: *"will you do that in-house, or outsource it to an*

agency? If you outsource it to an agency: how do you control that you have a consistent message, that you have an SLA, that you can authorize responses by the agency, etcetera?

Company C does not only see not taking part in social media as a missed opportunity, but also as a risk. *"Even if you don't take part in social media, you don't push any advertising out etcetera, that doesn't stop you from having a problem off course. Not playing in that arena doesn't keep you out of trouble, because people now can put things out there about you and it can go around the world ten times in an hour. So whether you play there or not you can have a risk."* Company C chose to be part of the online conversations and wants to fully take the opportunities out there.

The main risk however, is reputation damage. *"Yes, you can have people obviously hacking your sites, creating fake sites. Last week we did a social media audit in Brazil and the day before the audit we Googled and found 14 illegal Facebook sites. And it's not like we as a company are able to just shut those sites down tomorrow. It's not like the people of the audit were the first one to find them, but they pop up every day. And we, the consumer doesn't necessarily know that they are not official sites."* This ultimately may have a negative impact on the company image.

Another risk comes from employee use of social media. For example, they could be less productive or share confidential information on social media. However, as was stated, this was already a risk before the advent of social media: *"even before the advent of social media that was a risk off course. I'm subject, in my role I have access to a lot of confidential information, I could leak it to a newspaper if you like, before the advent of social media. Now off course I can post it on Facebook. I'm less likely to be anonymous so that's actually more stupid that leaking it to a newspaper, but that's where the code of business conduct rules are for: to make it very clear, not just about social media, but in there is also about confidentiality, misrepresentation, very different elements of behaviour if you like."* Obviously, it's possible for every employee to do such things, but being in breach with the code of business conduct is a serious issue at Company C. To control social media risks, the company has various mechanisms in place;

At Company C, every rule is written in ORCA format, which states: what is the objective of the rule, what is the risk, what are the controls, and how do you assure compliance to the rule?

- **Rules.** Every rule is written in ORCA format. Rules are applicable to different people, however, at Company C rules are often made broadly accessible, so that anyone can be knowledgeable of any rules. *"For example, the code of conduct is applicable to everyone in the company. There you will read about your own individual responsibility when it comes to social media. But the rules on digital marketing are predominantly meant for marketers, but they are not only accessible to marketers. So everybody in the company can still read the rules on digital communication, even if you're not someone who is the key owner of that area, you can still be knowledgeable in; what are the rules, what are the guidelines, etcetera."* The rules are applicable to various levels: they state the local responsibility with regard to the rule, and what is the global functional, or regional role. In principle the rules are designed to be applicable everywhere, and then explain the different levels of responsibility or action to be taken on the different levels.
- **Guidelines.** The first control that accompanies a rule is generally that the rule owner provide standards and procedures that give more guidance to the rule, that will keep the rule up-to-date, and will communicate and train on the requirements of the rule. So for example, the local

company will comply by having this in place, and the region, it might be depending on the type of rule, has to consolidate and check certain things at the regional level. However, the standards and guidelines on social media are very new: *"as I said, when identifying social media as a risk, standards and guidelines were developed. It is also learning from incidents. So there will be various things arranged around embedding that more formally in the organization."* Social media is documented on two separate places depending on the role you have as an employee of Company C. The code of business conduct advises all employees on how to behave, and there is a specific section for social media, our communication and brand ambassadorship; and there are separate, more detailed standards and guidelines for brand owners, for marketers, people who are involved in the management of the brand equity.

- **Training.** Training can be part of a control, as was stated: *"Obviously that's something that tends to be part of a rule. Those people need to understand what's expected from them. You don't just publish a rule on an intranet site and just expect people to be compliant off course."* So at Company C, there is various training, sometimes e-learning to help embed these rules.
- **Access.** Access control is also an important aspect of controlling social media and is part of the audit process. It is more from an IT perspective, there need to be clear guidelines: who is allowed to speak for the company, who can respond on behalf of the company, who authorizes any responses on behalf of the company etcetera. That then has an IT element of controlling who can do those things. To document things, access control policies are in place. Social media rules define responsibilities, documented in RACI's, and according to these RACI's, IT access should be set up. *"we do have in different rules and guidance different IT rules and IT security policies and therefore guidelines on access control, these kinds of things. But obviously all the different systems have different access controls."*
- **Monitoring.** Monitoring plays a very important role at Company C*: "Probably the biggest control is the monitoring, not only being part of the conversation where we choose to be part of the conversation, but identifying the conversations that we are not involved in and my own personal perspective is having that monitoring in place is probably the most important element that I would pick out at the moment. Yes, training absolutely, but that's not the only one. Because you can have monitoring but how you handle the monitoring if there is an incident, if it escalates, how do you categorize, how quickly do you respond, who authorizes the response, etcetera. Obviously there is a lot more to it than just monitoring."* Some websites are specifically monitored, like the Facebook page of Company C and other official websites. For the rest of the WWW, the monitoring mainly consists of keyword search to detect any comments, either positive or negative, related to the brand.

Compliance

Compliance can be a complex issue at a global organization. As a global company, differences in global and national level should be considered. For example relatively 'easy' tasks of translating rules into a different language, and more complex tasks, for example, complying with local legislation. *"For some rules, the local legislation makes it impossible for you to comply with the rule. It could have to do with tax policies in the company for example, certain countries have different tax laws, and therefore following the company rules wouldn't fit with your local legislation."* Also, the business models of the various local companies can differ, which can cause inconsistencies, or make some rules inapplicable to those companies. At Company C, this is also taken into consideration. *"So you can also have certain whole rules or partial rules, where instead you're saying; I'm not compliant because it is not applicable to me. That 'not applicable' statement has to be approved by the global rule owner. So you even can't make that*

decision yourself." And certain controls are written in such a way that you can make it fit your organization.

Compliance is mainly checked by self-assessment and audits. A self-assessment is when the managers of the local company have to sign-off on saying whether they are fully, partly, or non-compliant with the rules. When they are partly or non-compliant with the rules, they have to have an action plan on how to become fully compliant with the rules. *"If you say; no I'm not fully compliant, I am partly compliant or whatever, [you should be able to tell] this is why, this is my action plan, we're doing this, we're doing that, there is a deadline, an owner, and that is tracked. And that is also why we do the self-assessment twice per year so that you can, more timely, also close out the plan and be compliant."* The self-assessment can be seen as the 'first line of defense.' The second line of defense is the local audit and the third line of defense is global audit. These functions consists for a large part of checking: is the rule known, is it communicated, are they compliant with the rule, etcetera. They may both check the self-assessment of the local company and may also check the action plan if that is called for.

When an employee does not act in line with the code of conduct, this could result in dismissal, and even in taking someone to court if it's very serious. The level of action that will be applied depends on the level of the breach.

5.1.4 Company D

Company D is a company that is active in the energy sector, and operates throughout Europe. They are medium-sized, with approximately a couple of hundred customers. The company is active on Twitter, Youtube, Flickr, Facebook, and Yammer. Twitter is used as an extra channel for publishing news, and for 'listening' to the online conversation that is going on about the company, and the energy world in general, and occasionally the company takes part in the conversation. For example, when the company name is mentioned in relation to activities that the company has nothing to do with, the company reacts to set things straight. There are two company Facebook pages, one is an extra channel for posting news, film, photos, and occasionally answering questions. It's run by the communications department. The other Facebook page is about a specific project of the company, and the aim for this page is to provide photo's, films, animations about the work carried out, for people who want to know more about it. "People can't have a look on-site where we're actually working, we can't open the doors to everything, so this allows people to see what is going on, and it's quite impressive work as well." Youtube and Flickr are used as technical platforms to make videos and photo's available to the public. Yammer was used more as an experiment, but it was not very successful and it's currently out of use. However, the company looks for ways to expand their intranet with internal Yammer-style functionality and use it as a more social intranet, which enables collaboration between employees, and facilitates discussion and feedback within the organization.

Company D sees the rapid development of social media and wants to bring this to its part of the energy world. *"The area we operate in is rapidly developing. It's energy and it's something that actually affects everyone ultimately. In the end, we're all involved in the energy world. So if you take that and the fact that social media is developing in the world around us generally, we need to bring these worlds together."*

The first function of Twitter is acute acknowledgement, so you can say immediately what happened. And that's why it's so absolutely crucial."

The main business reasons for using social media are maintaining a positive corporate image, being part of the online conversation, and having an extra channel to inform stakeholders, people in the energy world, and inform them in another way than just with letters and the website. *"With Facebook we reach more people."* A real benefit of social media that Company D sees is the speed with which you can respond to an event, or communicate to people what is happening when there is an incident or even a crisis. *"The speed with which you react is really crucial in a crisis. [...] The first function of Twitter is acute acknowledgement, so you can say immediately what happened. Pretty much immediately, you know within a minute you can put it on Twitter. And that's why it's so absolutely crucial."*

Even though Company D is positive about the benefits of social media, they do not expect to become a company with a full web care team required to handle multiple customer questions and complaints. Social media is really seen as an additional channel.

Governance
Social media is the responsibility of the communications department, in which there is one main person who oversees all social media initiatives. Other members of the communication department also post on social media and monitor the different channels. There are other parties involved: these are the IT department for technical support, and the security department, for 'keeping an eye on the outside world.'

Risk
The greatest risk of social media at Company D is reputation damage. For example, by negative comments that are posted by employees or people outside the company, or by incorrect information spread by employees or people outside the company. However, Company D sees social media both as an opportunity and a risk, and sees that the online conversation will continue with or without involvement of the company, so as a company you could better use it to your benefit. *"You can't stop that conversation: it will happen anyway. And one thing about it: it's another way, it's an extra way of monitoring the world around you, seeing if there are issues."* There are some measures and techniques in place to control any social media risks.

- **Access control.** Access to social media accounts is limited to the communications department. *"We protect the passwords, and no one is allowed to have these passwords, unless they are authorized."* Also, Company D uses monitoring processes and tools, such as keyword searches and Google Alerts, to know what is being said about them and to monitor their websites. *"We as the communication department regularly check for tweets about the company, and we have Google alerts. Our security department does a more 'in-depth' check of the internet. So we do monitor what's out there."*
- **Response.** If someone says anything incorrect about Company D, then depending on the amount of followers this person has and the impact of the comment, the company steps in. There is no structured procedure that states when and how to respond. *"We don't have a big chart on the wall that says: don't say this, do say that, not at all. However, there was a big issue a couple of months ago with which we thought we might be associated, and then we thought: okay, what*

are we going to do on Twitter, because there'll be a lot of tweets about it on Twitter. [...] So one of the colleagues made a standard tweet that we used for: say this if you see one of these tweets. So in that way it's structured, but it's not like we have a big handbook with what we do in each non-crisis situation. We do have a handbook for crisis situations, however."

There is currently no specific social media training for employees to teach them how to use social media, and to make them aware of social media policy. However, social media is already included in the code of conduct. *"What an employee says online about the company is covered by the code of conduct at the moment. But you know, even before social media we had rules about what you can and cannot say. But we have a new code of conduct coming up in the next few weeks that will remind everyone again of the rules."*

Compliance
If someone says something damaging about Company D, there are sanctions, which are also stated in the code of conduct. Company D has not had to apply these sanctions yet.

5.1.5 Company E

Company E is a company that is active in the utilities sector, and mainly uses Twitter, Facebook, YouTube and LinkedIn. As the company is not a commercial company, it does not have a commercial 'drive' to answer customer questions and complaints via social media. So at first, people were reluctant to use social media, because they didn't see the added value of it, and thought it only meant extra work. "But gradually it is changed into something we get information from. So that is what people should remember: use it to your advantage."

The company uses Twitter as a sort of additional news channel. Facebook is used for 'fun stuff,' that cannot be placed on the company website. "*On the website, there is information about the company, job vacancies, etcetera. Facebook is for interaction with the client, but we'll also put, for example, the prices of our product on there. And off course, you can react very quickly on actualities by using Facebook."* YouTube is used for videos of production locations, to show people how processes work. On LinkedIn, there is a group of Company E, which shows job vacancies, which functions have changed, new colleagues, etcetera. There are two important benefits of social media to the company.

1. First, social media is a great aid in finding any technical issues and malfunctions. Customers can state that something is wrong, which signals the company to do something about it. *"Recently we had a technical malfunction. At 06:55, we got the first phone call about it, and at 06:56 we got the first tweet. However, because of the tweet, I was aware of the problem, because I do not get the phone calls, they go to the call enter."* Social media is also used to show people what is done about the problem.
2. Second, social media provides a 'stage' to the company, on which they can show more of themselves. *"Some companies in our sector have investigated the use of social media and found that customers do not care for that, which is also possible. But I think it is very good for our reputation to be there and to show what we do, not only our main business, but to show that we are also contributing to development projects, sharing expertise, we do so much more than some people think we do. So that's another thing of social media: it provides a stage on which we can show much more of ourselves."*

The goal of Company E with using social media is to help their client as fast as possible. *"The customer is 'live' and as a company you have to keep up with them. You have to be there, no question about that."* An accompanying goal of helping the client as fast as possible is the profiling, maintaining a positive image, and informing people about the company. There is no formal strategy to reach those goals, but based on what is found in practice, this strategy is being created.

Governance

The company is split up in five core processes, and these processes are all involved in social media: the communication department, the web care team for the customer department, the technical department, the Company E solutions department, and two representatives of the company.

> *"The customer is 'live' and as a company you have to keep up with them. You have to be there, no question about that."*

The central responsibility for social media lies with the communication department, and this department also initiates most social media projects. The communications department is in control of the corporate account, which is also the account that is used for the complaints and questions of customers. There are two people from communication that take turns in managing the account. General tweets are now not answered. *"We want to do this and tell more proactively what we are doing. However, we don't know how yet, we're not sure about retweeting, but obviously questions should be answered."* The communication department also creates rules and policies around social media, however, they cannot enforce them, as there is no hierarchy in the involved parties.

The web care team mainly answers customer complaints and questions. The technical department is responsible for technical issues and malfunctions. A specific social media account was created for communicating information about malfunctions to the customer, and this is the responsible of one person in the technical department. There are two representatives at Company E, who have their own personal Twitter-account, and mainly interact with reporters, newspapers, and politics about the company. Another party involved with social media at Company E is the external party that set up the companies' Facebook page, and also does the community management for Company E. But in the future, this probably will be taken up by someone within the company. *"We have a web editor, which is about the internet and the intranet, but I really would like to see him also take up social media, for example, spend half the week on updating the Facebook page. [...] So in the future, I definitely see a social media manager or community manager within the communication department."*

Risk

Risks or challenges that Company E encounters with social media come mainly from employees. For example, when an employee does not agree with a certain policy and ventilates his opinion online. *"But such things are bound to happen. And as a company you just have to think carefully about how to deal with it, and correct people when they do something wrong. We also had a colleague once that stated something like: nice website, but a shame that it doesn't work with Internet Explorer 8. If you have such a comment, why don't you just go to the project manager and fix the problem. Or once we had a manager that posted his PowerPoint online, which contained investment plans. That's also not very clever."*

By a lot of people within the organization, tweets about technical malfunctions are seen as risky, because they can damage the company image. They believe that there should be very little communication about any technical issues. *"Because a lot of customers see technical malfunctions as something that we do wrong. But obviously these things just happen, whether it is caused by us or by other parties. Our task is to fix any problems as fast as possible."*

However, according to the interviewee an even bigger risk is not communicating about these issues. *"There is I think a bigger risk in not being online and not saying anything, than being there. When you have a big technical malfunction and you do not interact about it, then you have a much bigger problem than when you say: we don't know what's wrong yet, we're working on it. People accept that."*

Another risk comes from angry or dissatisfied customers. Company E experienced this with a group of angry customers, which really can become a problem to the company. *"We had a photo contest on our Facebook page. People can send in their pictures, and from the three that have the most likes, we pick the winner. However, people in this group were uploading their own photos, giving each other likes, and thereby 'infesting' our contest."* Company E chose to ignore most of the activities of this group, and leave it to the representatives of the company. To control social media risks, there are various mechanisms in place:

- **Monitoring.** Company E uses a monitoring tool to detect mentions of the company. *"This tool monitors, analyses, and provides web care. It has a sort of inbox where all Tweets, but also news articles, YouTube videos, Facebook posts, etcetera, are gathered, and from that inbox, employees can respond to the questions of the customer."* The monitoring tool also shows the influence of the Tweeter, how many followers he has, and how much interaction he has with them, and based on that we decide if we will or will not respond. Various stakeholders get information from the monitoring tool, for example project managers that get an overview of tweets related to his project, and the business development department that get information about new products related to the company.
- **Guidelines.** Employees of Company E are provided some do's and don'ts for using social media. *"These are the company rules, together with some recommendations like: "be short and snappy," some basic rules so to say. And we agreed that we respond to anything, except from insults, shout outs, etcetera. Also, there are some cases that we leave to the representatives and do not mingle in. Those really are problems with clients, with the distribution of water."* The do's and don'ts are not really formal but function as a guideline for employees. Next to the do's and don'ts, there are also 10 rules for the private use of social media for employees.
- **Training.** At Company E, there has been training for employees on social media use. This was a Twitter workshop, in which a trainer explained on how to Twitter, concerning the basics: formulating tweets, being short and snappy, etcetera. There also was a training for the monitoring tool for the involved employees.

Compliance

When an employee posts anything online that is not in line with the code of conduct, this can be detected by the monitoring tool that is used by Company E. Measures will be taken depending on the severity of the violation.

5.1.6 Company F

Company F is a company that is active in the media industry. They have accounts on Twitter, Facebook and YouTube, which are mainly used for promotion. Social media is used to attract business partners, but also to target a new and younger audience. But it is still in a very explorative phase. "Social media for us is important because it is a way to 'bind' people to the company. […] But we are still searching: how to handle this, what to do, what should we do with it and what not?" Company F tries to be 'realistic' in the added value of social media. "I think that's the big question with Facebook: everyone is crazy about it, it's 'hot,' but meanwhile there is very little known about the effectiveness and consequences of social media." However, a trend that Company F identifies is that social media is a valuable source of information for a lot of employees at Company F, and that is therefore has become a vital part of their job.

Company F sees an important role for social media in promoting their online channels to a younger generation. *"The younger generation is not very interested in the print products we offer. So we are very concerned with changing our product to make the younger as well as the older generation interested in it. How can we distribute our products digitally? And how to make money with it? Because it is very hard to make money with online content at this moment."*

Another thing that was mentioned not as much as a goal, but as a comment is that Company F thinks that people in the organization can learn a lot from each other, and that social media can aid in this. *"When you have done a campaign via Twitter, and it was successful or not successful: what went good and what went bad? I think that we still do not communicate enough about that between the different departments. And therefore, we learn too little of each other. And definitely with social media, which is very new, we can improve that a lot."* Not only documentation about setting up a campaign, but also about setting up an account, and which people are responsible for the account and can be contacted about the account could be shared through social media.

Governance

Company F is an organization that is build up from several small organizations. Those organizations are centrally controlled, but they still remain 'isles,' which has impact on communication, cooperation, and regulation, and knowledge exchange. *"At every former organization there is a certain 'culture,' and a way for doing things. So, because we have these different 'isles,' people want to reinvent things, which is really a shame, because you could use the knowledge that you have in-house to create a synergy in things. So that's definitely a missed opportunity."*

Company F tries to regulate as little as possible as they do not want to be censoring their employees. Also, they believe that every employee should be aware of his or her responsibility when it comes to social media, and that it is the responsibility of the manager to control this. *"That's part of being a manager: to know what your colleagues, your subordinates do. And when that's not okay, you are expected to do something about it."*

To give a guideline on these responsibilities, there is a code of conduct in place, which describes desired behavior, that you may not post anything online that can harm the reputation of the company, etcetera. In addition to that, there is an internet and a social media protocol in place. *"There is an internet protocol that states how you should use the internet, not only under working hours, but also outside working hours, and a social media protocol that states that you should be aware of the fact that when you put*

something online, that it is for everyone to see and can damage the company's reputation. It also includes the consequences for any violations of the protocol."

Social media is mainly used for binding customers and readers and attracting business partners. The responsibility for social media lays with the persons that use social media, for example the editors and employees, then the responsibility of the marketing and finally the responsibility of sales. The corporate communication at Company F does not use social media: they communicate via the press.

Risk

There are also some risks of social media that Company F acknowledges, the greatest risk being reputation damage. This can be caused by several things:

- **Confidential information.** Employees at Company F often have access to information that is not yet publicly known, and should not be out in the open yet. This causes some troubles with for example internal communication. *"Any news, even concerning our own company, is out in the open in the blink of an eye. […] So we try to be extra careful with communicating internally, because when there is, for example, news about a reorganization, we would like employees to hear from it from their own manager, and not read it online."*
- **Incorrect information.** Another issue with access to such information is that it is not always correct. *"But if you really say things that you haven't checked, that are not true, then you can harm the company reputation. And due to this, people can start worrying about the longevity of the company, and this may scare away customers."* The speed with which such rumors spread via the internet and social media, can be very great and the impact of this can be severe. And when something is online, it's impossible to remove.
- **Openness.** Another risk is the openness of social media. *"There are a lot of employees that use social media, also colleagues of marketing and sales, and they build a network there. At one hand this is off course very positive, as there is a lot of knowledge that can be found in such networks. At the other hand, it is an open medium, and everyone can see what you state online."*
- **Employee leave.** Another risk that Company F identifies is when an employee that has a lot of followers, leaves the company. *"For example, when an employee of a company has 16.000 followers on Twitter, and he leaves the company, then the company loses 16.000 followers. So that can be a risk."*

Something that could cause a risk is that there is no clear overview of the official social media accounts of Company F. Keeping an overview could detect any fake profiles, or inactive social media profiles and accounts. To control social media use, there are some processes in place at Company F.

- **Monitoring.** Several people at Company F use Google Alerts and Twitter Alerts to stay updated on any comments, posts, and mentions of the company name on the internet.
- **Training.** People do not get a standard training on social media. They are given the opportunity to attain a course on social media, about what it is and how it works. Also, the HR department has had a course on using social media for recruitment purposes.
- **Response.** When something is said about Company F, which originates from an external source, the policy at Company F is that they never respond to that. *"So for example, it was made known that we're going to reorganize. The next day, it's on the news, and people are saying that we are firing 500 man, saving millions, etcetera, but off course this is always more nuanced than it's in*

the news. But we do not react on such things. We do answer questions from the press. But on such a news message, we cannot confirm that it's correct, and we can also not say that they're incorrect."

Compliance
As said before, there is no specific monitoring tool or process, so compliance is not formally monitored. Especially of young, new employees, because they are expected to know how social media works. They have grown up with it. Compliance of the older generation is somewhat tougher. *"They sometimes do not believe in the added value of social media, or they only see the downsides of it, or they have a mindset of: we have done it this way for 20 years, so why should we change that?"*

When an employee violates the code of conduct, or one of the protocols, this is followed up by line management. Consequences of this violation are depending on the situation, and these are stated in the protocol.

5.1.7 Company G

Company G is a global company, which is active in the advisory and services sector. It operates across four geographic areas: Europe, Africa, America, Middle East, Japan, India and Asia-Pacific. At a global level, the company is very active with managing social media: there is a social media competence center that is responsible for social media, and that creates social media policies, guidelines and best practices. This interview was conducted at a local company of Company G and focuses on the local initiatives related to social media. Company G is mainly active on three social media channels: LinkedIn, Facebook and Twitter. Twitter is used as a sort of news channel with information about the company. Facebook is used for recruitment purposes, and to keep people aware of events and promotions of the company. LinkedIn is used to keep in touch with employees. There are some LinkedIn groups, for example for former and current employees of the company.

There was an initiative at Company G to set up a social media strategy. This strategy is not yet operational, but pointed out four focus areas that are important to the company and can be improved by the use of social media. These areas are: internal mobilization, recruitment, marketing and thought leadership, and web care. For internal mobilization, the company created a group that organized training sessions to 'mobilize' colleagues in their social media use. Recruitment focused on cost reduction by cutting out the middle man in the recruitment of new employees (i.e. head hunters, recruitment agencies). Marketing and thought leadership focused on having important people in the organization 'in the spotlight.' So, executives, managers, directors, etcetera, should be more active online, stand out, share their knowledge and expertise with others, and by doing so, contribute to the corporate image. Web care is aimed to prevent incidents. This includes having monitoring processes and tools, and a procedure on how to operate when an incident arises.

Governance
A so-called 'digital natives' group was created at Company G, to raise the awareness level of the employees on social media. The group was initiated by management with the aim to spread the awareness for social media within the organization. For this purpose, the group organized social media lunches, where people were taught on: how to create a Twitter account, how to create a LinkedIn account, for which goals to use the social media channels, etcetera. So, workshops to promote social media amongst employees, and to stimulate them to act as a thought leader online, or generate leads, etcetera.

Even with budget and staff for social media being limited, still employees are stimulated to act as so-called "brand ambassadors" at Company G. This means that they promote their organization in their own, private network: *"I often post an article on LinkedIn, for example on information security or similar topics, and spread this in my community, add a link to the company, and say: this is a topic on business continuity and we know more about it. So actually I'm promoting the company. So I use LinkedIn for private matters, but also for business matters. And I don't mind, even with a small budget, to be a leader in this."*

At Company G, "brand ambassadors" promote the organization in their own, private network, and create advertising about the company on their own initiative.

Risk

The main risk that Company G encounters with the use of social media is that of confidentiality breach. The employees of the company often visit clients, and get to know a lot of client information, and have to comply with certain rules and ethics to keep this information out of the open. *"So, when you visit a lot of clients, you have to keep in mind that if you use social media, Facebook, Twitter, that you do not accidently or on purpose use or spread client information that may or may not be confidential. That does not only damage you relationship with the client, or your company image, but also for yourself it has a great influence on your integrity and your credibility within the organization."* The impact of such a mistake can thus be very severe, not only for the organization but also for the employee.

Another risk comes from the employees that act as brand ambassadors, build up a big network, with lots of followers, and eventually leave the company. *"Imagine that those people leave the organization. The impact maybe isn't that great, but if you look here locally, […] it's a small world, you know each other. But that could be also a risk, when you have a lot of social media influence and you leave the organization."* Another risk with such kind of exposure is that employees are more 'in the spotlight' and become an interesting recruitment opportunity to competitors of the company.

Challenges

Currently, social media initiatives are not proactively stimulated. It is seen by Company G, but also by their clients, as something 'additional,' and therefore, it is not a top priority. *"Clients often see social media as a hype, a hot topic, but if you really ask them: is this a priority in your organization? Then it becomes clear that they see it as something additional."* The low priority given to social media leaves also a limited budget available for stimulating and developing social media project. This obviously also has to do with the economic downturn, which leaves most organizations no choice then to reconsider their priorities. "*So I think that at a lot of companies, also our company, because of the economic downturn, priorities are shifted, and that this is the reason that there is no or limited budget for social media."* This makes it very hard to stimulate and develop social media use more at Company G.

5.1.8 Company H

Company H is a global firm in the energy sector, which operates in more than 70 countries. The company is active on Facebook, Twitter, YouTube, LinkedIn, and Flickr. They are also doing some pilots with Instagram. The three key areas in which social media is important are engagement, brand awareness and

brand reputation, and the aim of using social media is to promote the company, generate leads, and increase sales for other areas of the company.

Governance

The center of excellence is a global team that is responsible for providing guidelines, standardization of frameworks and processes, and best practices for the company. The center consists of a social media manager, that foresees and supports the development of the strategy, and a project manager. Then there are also 'call community managers,' who are the people that will engage with the customers, followers and friends on the different social media platforms.

> Three key areas in which social media is important are engagement, brand awareness and brand reputation. The aim of using social media is to promote the company, generate leads, and increase sales for other areas of the company.

The center of excellence has a hub-and-spoke model, in which they bring, train and build capacity in different teams in different countries, and those are the people that will actually do the implementation. *"So the center of excellence is more of the strategic direction, the approach and best practices, but the implementation is actually done by the local team."*

The center of excellence is not the only place in the company where social media is used. At Company H, everyone is involved in social media. *"We do not monopolize social media activities under the center of excellence. We create certain frameworks and processes and we enable those teams. They do have different roles sometimes, they engage sometimes, they collaborate with content, but everyone can be a participant or a collaborator on social media."*

> Company H has a "center of excellence" for social media. This is a global team that is responsible for providing guidelines, standardization of frameworks and processes, and best practices.

Risk

The main risk of social media is when employees engage on behalf of the company. Company H doesn't consider this as a big problem, as they believe that this risk can be properly mitigated. *"I think there is always a risk that someone can say something that is not appropriate but with the right training and capacity, that is not a problem."* For example, by having good and solid social media guidelines, so employees understand how to use social media effectively and within a good ethical foundation. The other risk is related to that fact that the company is exposed, and that people for example can use social media to organize campaigns against your company. *"But I think everything is manageable, if you have the right structures and resources in place."* To control social media risk, several measures are taken.

- **Training.** There is training in place, an online training, which is mandatory, and is focused on creating awareness, and an advanced training for those that want to use social media or use social media as part of their role in the company.
- **Monitoring.** Monitoring is also done within Company H, as an in-house process. There is a full department that manages the social media monitoring, and they work closely together with the center of excellence.

- **Guidelines.** There are social media guidelines and policies in place. These pertain to the tone of respect, the language, how content is moderated, and things like that. Company H does not obtain information on social media for any purpose.
- **Access.** The guidelines specify who has access to social media channels, and a person can only edit the content if he or she has been authorized and trained by the center of excellence.

5.1.9 Company I

Company I is a global company that is active in the food sector. It is active in more than 70 countries and owns over 30 different brands. The company uses Twitter, YouTube, Facebook, LinkedIn and Pinterest. Facebook is used as a promotion page of the company, focused on consumers. Twitter is used as a channel to communicate about press articles, projects the company is developing, etcetera, to (potential) business partners. LinkedIn is used for posting news articles related to the products of Company I, and for posting job vacancies. Pinterest is used for uploading artistic photos that radiate the sphere of the company.

Social media is seen as both an opportunity and a risk. *"On the one hand, we can monitor what is said about us and where we stand, and we can respond to that if we want to. On the other hand, you see that tiny issues can become big problems on social media. Maybe even bigger than they would have several years ago."*

Governance

Social media is the responsibility of the communications department. *"There is one person of corporate communication who, from the head office, coordinates and controls social media. Then there is a president of communication who is responsible for the content of the message. This person will decide whether or not the company will respond to certain things, which channels to use, and he will coordinate this."* Furthermore, in each country that the company is active in, there is someone in charge of social media, to locally keep control of social media.

> *"On the one hand, we can monitor what is said about us and where we stand, and we can respond to that if we want to. On the other hand, you see that tiny issues can become big problems on social media. Maybe even bigger than they would have several years ago."*

Risk

One risk that Company I identifies is that tiny issues can become big problems on social media. To control this risk, there are various mechanisms in place:

- **Training.** There are four workshops that are given across the world, which the general management and the operational management have to attend. And in those workshops, social media is discussed and its role in communication. Also topics like: what to publish, who decides what is published, but also: is it allowed that you publish something? *"There are three or four men in communication who travel over the world for trainings etcetera. There is also a director operations with them because a lot of times, what you see is: when something goes wrong in a factory for example, and an employee posts something about that event online, then we have to check: how big was the impact, are there a lot of reactions to the post, how many people are following that employee? Because when something spreads like wildfire, then possibly there has*

to be done something about it." When an event starts to escalate, an escalation procedure is initiated. Also, the director of productions will be involved, to provide information about the event and how much impact it had, to make sure that things are not blown out of proportion.

- **Crisis management.** When someone posts a complaint or something insulting online about the company, these are normally not removed, unless they go too far. When something escalates, there is a procedure available, which is a document that contains the names of people that should be contacted, in case something happens. *"These people also have back-ups, in case they are away, or on vacation or something like that. So it really gets scheduled in such a way that there is always one of the two available."* This escalation procedure is not specific for social media, but for communication in general, so also press related messaged, websites, interviews, etcetera. *"For example, when we have to take back our entire production of last month in Germany, because something is wrong with it, which will not go unnoticed in the press, not only in Germany but also in other countries. So in that case, we want a person at head office who takes the final decision and tells us what to do. That's how we communicate: a press message, which then also is posted on our website, on Twitter, and Facebook, etcetera."*
- **Monitoring.** There is a monitoring process in place that keeps track of the number of mentions on Twitter, Facebook, in newspapers, websites, blogs, etcetera. However, Company I does not want to monitor continuously to detect any comments or responses, in order to be able to react on them. *"It gives customers the idea that when they send an e-mail, then it takes a week before they get a reaction, but if they post something on Twitter then they get a response in 30 seconds. So we don't want to have that."*

Compliance

Company I has rules and policies that are created centrally, and have a sort of 'laisser-fair' approach in the compliance to those rules. *"The local Facebook page of Hungary, for example, is not a big concern to us. There are some rules that they have to comply to and we check that once or twice in a year, to see if they are still in line with the policy, etcetera. We believe that every country should be able to do business in its own way, and therefore we try to be not too restrictive in enforcing the rules."*

5.2 *Findings from the interviews*

Now the results from the interview summary are analysed and visualised for every question of the interview guide (see Section 9.1). This was done by counting the number of companies that gave a certain answer on a certain question, and this number was depicted in a bar chart. The companies could provide multiple answers for the questions asked. For example, they could state multiple social media channels, if they used more than one, or they could state multiple parties that were involved in the social media process. The interview results are visualised per question to gain insights in the most used social media channels, goals, and the most experienced benefits; the generally used responsibilities and policies for social media; the main risks and controls for social media; and the most used compliance mechanisms. For an overview of the interview findings, see section 5.3.3.

5.2.1 Social media channels

The first question the interviewees were asked was: *"Which social media channels does your organization use and for which business purposes/reasons?"* Twitter and Facebook were used by all companies. These two channels are very important to companies, as they are used for communicating to two important parties: business partners and customers. Twitter is used by companies as an extra news channel for publishing news, and for 'listening' to the online conversation that is going on about the company. The communication via Twitter is most of the times focused on business partners. Facebook is the channel for communicating with the customer. The Facebook page often is used as a promotional page, on which the customer can find special discounts, promotions, events, contests, etcetera. Company D created a Facebook page to keep people informed about a specific project that the company was doing. *"The aim for this page is to provide photos, films, animations about the work carried out, for people who want to know more about it. People can't have a look where we're actually working, we can't open the doors to everything, so this allows people to see what is going on, and it's quite impressive work as well."* Company G also used Facebook for recruitment purposes.

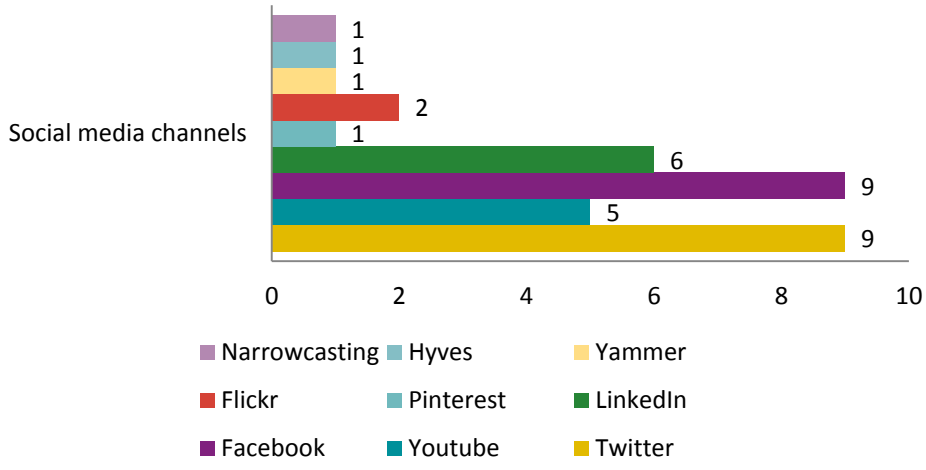


FIGURE 12 | SOCIAL MEDIA CHANNELS USED BY COMPANIES

Youtube and Flickr were used by companies that have a production location, to upload photos and videos of this production location, and to show people how the production process works. LinkedIn was used by most companies for posting news articles related to the products of our company, for posting job vacancies, showing which functions have changed within the organization, new colleagues, and keeping in touch with (former) employees.

Other channels that were used are Instagram, Pinterest, Yammer and Hyves. Instagram and Pinterest were used for uploading photos of the company, company processes, and the atmosphere at the company. Yammer was used as a pilot; however, currently it is not used anymore. However, the company is looking at ways to use Yammer as an intranet to encourage internal collaboration and communication. Hyves was used at Company C because some employees still have a profile there. Narrowcasting was mentioned by Company B, for the sharing of PowerPoint presentations.

5.2.2 Goals

Next, interviewees were asked: *"Does the organization use goals for their social media use?"* Social media channels were mainly used by companies for promoting their products. Under promotion, also advertising and marketing are gathered. The next thing that social media channels were used for is image building. Under image building, also 'profiling', and 'binding people to the organization' are gathered. One interviewee states that: *"It helps to put yourself out there, because that's what we want, brand awareness, as they say in marketing terms, that is an important objective."* Another interviewee stated that social media provides a 'stage' to the company, on which they can show more of themselves: *"Some companies in our sector have investigated the use of social media and found that customers do not care for that, that is also possible. But I think it is very good for our reputation to be there and to show what we do, not only our main business, but to show that we are also contributing to development projects, sharing expertise, we do so much more than some people think we do. So that's another thing of social media: it provides a stage on which we can show much more of ourselves."* 'Listening' to the customer was also mentioned by three companies (Company B, D and E) as a goal for social media use. Informing stakeholders also was a goal mentioned by Company D and E.

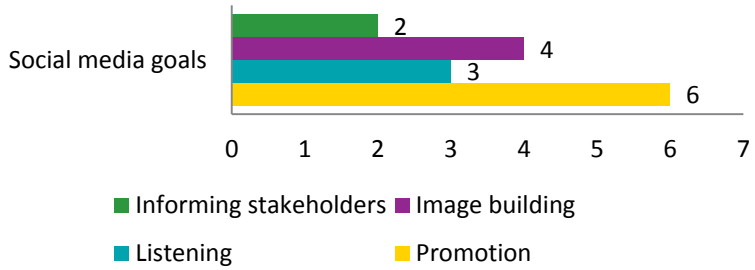


FIGURE 13 | GOALS OF USING SOCIAL MEDIA

Two companies indicated that they felt like it was 'inevitable' to use social media. As one interviewee states: *"being a 'modern' company requires the use of social media."* This is not really a goal for social media and therefore it is not included as such, however, it is an important motivation to use social media.

5.2.3 Benefits

Interviewees were also asked: *"Do you see any effects, either positive or negative, of social media use?"* Companies obviously also experience a lot of benefits of social media. The most mentioned benefit is the speed with which a company can respond to anything that is said online. This is especially convenient in a crisis. So, when something goes wrong with the company or in some company process, the company can explain immediately to involved parties what happened and what's done about it. *"The first function of Twitter is acute acknowledgement, so you can say immediately what happened. Pretty much immediately, within a minute you can put it on Twitter. And that's why it's so absolutely convenient."*

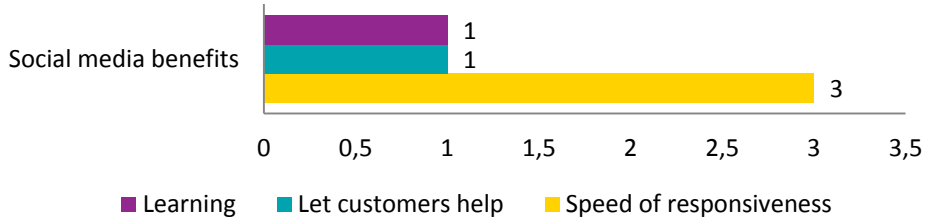


FIGURE 14 | SOCIAL MEDIA BENEFITS MENTIONED

Social media is also a great aid in making the company aware of things that go wrong. Employees or customers can much easier state that something is wrong, and help the company with finding that errors or issues. Company E experienced this with a technical malfunction they had recently. *"At 06:55, we got the first phone call about it, and at 06:56 we got the first tweet. However, because of the tweet, I was aware of the problem, because I do not get the phone calls, they go to the call enter."*

Social media is also a valuable source of information, and provides the opportunity of learning from one another. Company F sees a supportive role for social media in encouraging learning within their company. *"When you have done a campaign via Twitter, and it was successful or not successful: what went good and what went bad? I think that we still do not communicate enough about that between the different departments. And therefore, we learn too little of each other. And definitely with social media, which is very new, we can improve that a lot."*

5.2.4 Responsibility

Then, interviewees were asked: *"Which responsibilities are assigned to/by the governing body?"* Responsible persons for social media vary, based on various things. For a small, local company, social media could be just the responsibility of the communication department. However, for a large, global company, social media is the shared responsibility of different departments and teams. As one of the interviewees stated: *"depending on what angle you're coming from there are different owners. […] It's very much about the relevant parties working together, knowing who is doing what, etcetera."* Below, an inventorisation was made of the different departments, teams and other parties that are involved in social media in the interviewed companies.

Global responsibility. In global organizations, the responsibility for social media on a global level is often assigned to one person. Then, also per country someone is assigned that has local responsibility. Some companies have one person per country, others have a team. At Company C, there is team of IT that is involved in social media, and that provides support from an IT perspective, crisis management is ultimately owned by global corporate relations, global marketing is responsible for the rules, standards and guidelines on digital communication, and there is a business department within legal, that ultimately is the board of the company, that creates the guidelines on how people should behave in general.

In one company that was interviewed, a 'Center of Excellence' for social media exists. This is a global team that is responsible for providing guidelines, standardization of frameworks and processes, and best practices for the company. The center consists of a social media manager, that foresees and supports the development of the strategy, and a project manager. Then there are also 'call community managers,' who are the people that will engage with the customers, followers and friends on the different social

media platforms. The center of excellence has a hub-and-spoke model, in which they bring, train and build capacity in different teams in different countries, and those are the people that will actually do the implementation. *"So the center of excellence is more of the strategic direction, the approach and best practices, but the implementation is actually done by the local team."*

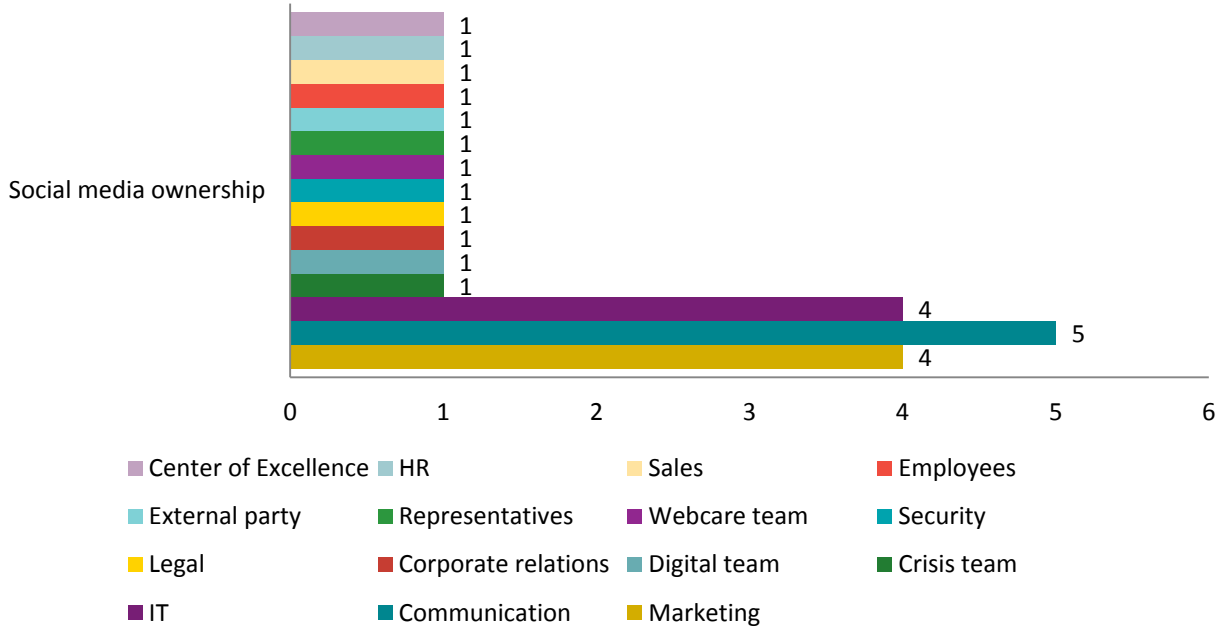


FIGURE 15 | OWNERSHIP OF SOCIAL MEDIA

Local responsibility. In most local companies, social media is a responsibility that is shared by multiple teams or departments. At Company I, G and E, this responsibility is concentrated in the communication department, with one person in this department that keeps oversight. At Company F, it was the responsibility of the persons that used social media, and of the marketing and sales department. At Company A, the responsibility for social media lay within the marketing department.

Other involved parties. There were also other parties found to be involved in social media. This was the IT department for technical support, the security or legal department for 'keeping an eye on the outside world,' and legal matters concerning social media, the web care team for answering customer complaints and questions, possible external parties to which the managing of social media account is oursourced, the monitoring department for monitoring the online conversation, and representatives of the company, that are responsible for informing reporters, newspapers, and the politics about the company.

Individual responsibility. Something that is heard quite often in global organizations, is that employees are also responsible for social media on an individual level. This was mentioned by the center of excellence: *"We do not monopolize social media activities under the center of excellence. We create certain frameworks and processes and we enable those teams. They do have different roles sometimes, they engage sometimes, they collaborate with content, but everyone can be a participant or a collaborator on social media."* This is also true at Company G. Every employee of this company has a responsibility with regard to the corporate brand. *"If I put something on my Facebook page, I can speak on behalf of the brand. Others know I work for the company, etcetera. So, everybody in this business*

should feel like a brand ambassador." A brand ambassador is someone who promotes their organization in their own, private network: *"I often post an article on LinkedIn, for example on information security or similar topics, and spread this in my community, add a link to the company, and say: this is a topic on business continuity and we know more about it. So actually I'm promoting the company. So I use LinkedIn for private matters, but also for business matters. And I don't mind [...] to be a leader in this."*

5.2.5 Policies, guidelines, rules

Next, interviewees were asked: *"Are there any policies, guidelines, or best practices in place for social media use?"* At every company that was interviewed, there was a code of conduct in place to describe desired behaviour in the company and to set out standards, guidelines and rules. Often, this code of conduct is not specific to social media, but for behaviour and communication in general. However, communication via social media and online behaviour can be covered with the existing code of conduct, according to a lot of the interviewed companies. Sometimes companies have a general code of conduct, with a specific section for social media, *"our communication and brand ambassadorship; and there are separate, more detailed standards and guidelines for brand owners, for marketers, people who are involved in the management of the brand equity."*

A good example of rules was at Company C. They have rules, accompanied by standards, guidelines and controls. Every rule is written in ORCA format: what is the objective of the rule, what is the risk, what are the controls, and how do you assure compliance to the rule? The rules are applicable to various levels: they state the local responsibility with regard to the rule, and what is the global functional, or regional role. In principle the rules are designed to be applicable everywhere, and then explain the different levels of responsibility or action to be taken on the different levels.

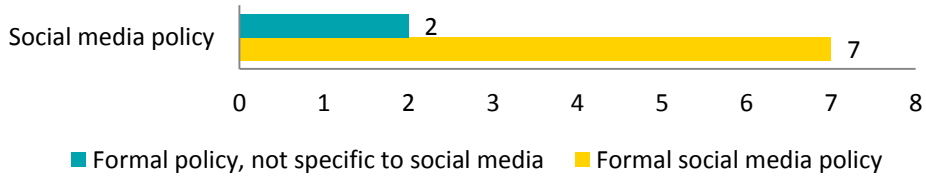


FIGURE 16 | SOCIAL MEDIA POLICY

Standards and procedures. According to one of the interviewees, the first control that accompanies a rule is generally that the rule owner provides standards and procedures that give more guidance to the rule, which will keep the rule up-to-date, and will communicate and train on the requirements of the rule. When this was asked in the interviews, most companies stated that they had some sort of standards, guidelines, policies and rules. For example, come companies that were interviewed have a specific internet and social media protocol in place. *"There is an internet protocol that states how you should use the internet, not only under working hours, but also outside working hours, and a social media protocol that states that you should be aware of the fact that when you put something online, that it is for everyone to see and can damage the company's reputation. It also includes the consequences for any violations of the protocol."* At Company H, there are specific social media guidelines and policies that pertain to practical things about social media, amongst others the tone of respect, the language, how content is moderated, etcetera. Employees of Company E are provided some do's and don'ts for using social media for work-related purposes. *"These are the company rules, together with some recommendations like: "be short and snappy," some basic rules so to say.* Next to the do's and don'ts, there are also 10 rules for the private use of social media for employees.

There were also some companies that did not have policies and rules specifically for social media. At Company B, for example, specific social media policies and rules are purposefully not in place, to prevent social media from being stuck in files and documentation. Also, at some companies specific social media rules are not in place, because there are already general rules on communication, which also cover social media use according to the companies.

5.2.6 Risks

The following question was: *"Are there any risks, related to social media, which you/your company encounters?"* There are various risks related to the use of social media. During the interviews, the companies were asked to indicate which social media risk(s) they experienced, and which they thought were most important or most threatening to the company. As it turned out, all companies saw reputation damage as the main risk. This risk can be caused by different parties, of which the companies saw employees as the main source of risk. The main risks are the spreading or leaking of incorrect, confidential or premature information, employee (mis)use, and reputation damage. These risks for a great part stem from employees. Employees create risks when they divulge confidential or premature information, when they leave the company, or when they post something embarrassing about the company online.

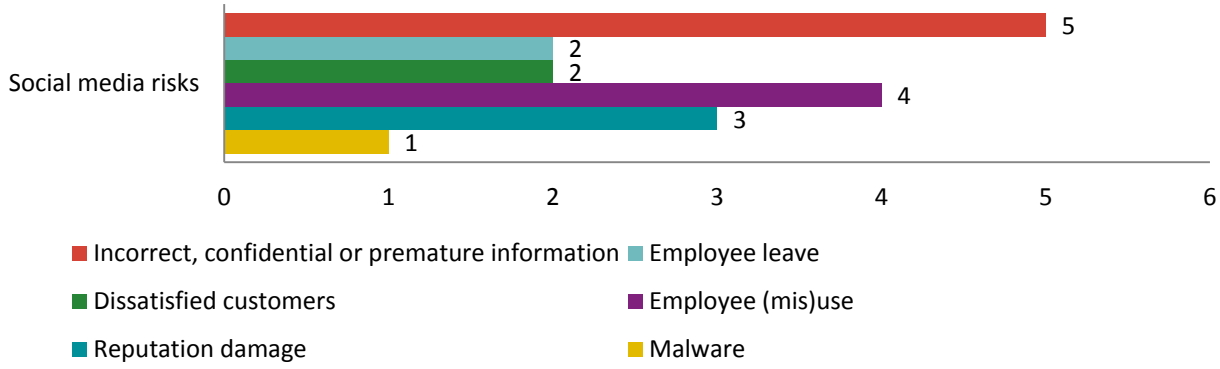


FIGURE 17 | SOCIAL MEDIA RISKS

Spreading information. At Company G, confidentiality is very important, as employees have access to confidential client information. *"You have to keep in mind that if you use social media, Facebook, Twitter, that you do not accidently or on purpose use or spread client information that may or may not be confidential. That does not only damage you relationship with the client, or your company image, but also for yourself it has a great influence on your integrity and your credibility within the organization."* At Company F, employees often have access to information that is not yet publicly known. This information does not have to be confidential, however, if it is published too soon, it can have unwanted consequences. Another issue with access to such information is that it is not always correct. *"But if you really say things that you haven't checked, that are not true, then you can harm the company reputation. And due to this, people can start worrying about the longevity of the company, and this may scare away customers."* This risk was also acknowledged by Company A, who see employees who prematurely post news about the company online as being a risk. However, one of the interviewees stated that: *"even before the advent of social media that was a risk off course. I'm subject, in my role I have access to a lot*

of confidential information, and I could leak it to a newspaper if you like, before the advent of social media. Now off course I can post it on Facebook."

Employee (mis)use. For Company H, an important risk of social media is when employees engage on behalf of the company. As one interviewee puts it: *"how do you ensure that an employee does not make incriminating statements? And what to do when certain tendencies arise that you do not want? That is much more difficult to control."*

Employee leave. Another risk that was identified by Company G and Company F related to employees is when an employee that has a lot of followers, leaves the company. *"For example, when an employee of a company has 16.000 followers on Twitter, and he leaves the company, then the company loses 16.000 followers. So that can be a risk."*

Reputation damage. As said before, employees may post something embarrassing online about the company, or in the name of the company. Also, posts of dissatisfied customers may negatively impact the company reputation.

Dissatisfied customers. At Company A, they experience a lot of customers that bring up an issue or lodge a complaint on the company's social media page. Customers of Company E sometimes experience technical malfunctions and see that as something the Company Goes wrong. *"But obviously these things just happen, whether it is caused by us or by other parties. Our task is to fix any problems as fast as possible."* A risk with such angry customers is that they can use social media to organize campaigns against your company. Company E experienced this. *"We had a photo contest on our Facebook page. People can send in their pictures, and from the three that have the most likes, we pick the winner. However, people in this group were uploading their own photos, giving each other likes, and thereby 'infesting' our contest."*

Malware. Other risks coming from outside the company are more of a technical nature. Websites or social media profiles can be hacked, malware can enter the company network, and fake profiles can be created. As one interviewee puts it: *"Yes, you can have people obviously hacking your sites, creating fake sites. Last week we did a social media audit in Brazil and the day before the audit we Googled and found 14 illegal Facebook sites. And it's not like we as a company are able to just shut those sites down tomorrow. It's not like the people of the audit were the first one to find them, but they pop up every day. And we, the consumer doesn't necessarily know that they are not official sites."*

Other risks that were mentioned are the openness of work- or company related communication via social media and difficulties with maintaining client trust.

5.2.7 Controls

Next, interviewees were asked: *"Which techniques or mechanisms are in place to handle/mitigate these risks?"* To ensure compliance to the rules, controls are in place. Most companies have training programs in place to make employees knowledgeable on social media, and monitoring tools or processes to detect any non-compliant behaviour.

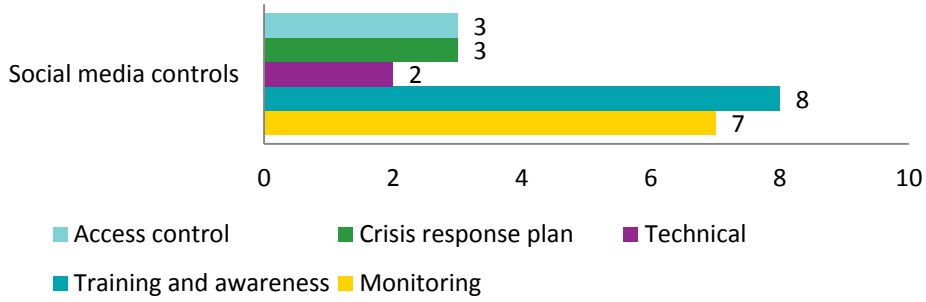


FIGURE 18 | SOCIAL MEDIA CONTROLS

Training. Most companies (8 out of 9) has some sort of social media training or awareness plan or program. Training often is part of a rule, to make employees aware of the rule and what they should do to comply with the rule: *"Obviously that's something that tends to be part of a rule. Those people need to understand what's expected from them. You don't just publish a rule on an intranet site and just expect people to be compliant off course."* Training can come in various forms, amongst others: e-learning courses, workshops, and training and awareness days or events. At Company H, there is a mandatory online training, which is focused on creating awareness, and there is an advanced training for those that want to use social media or use social media as part of their role in the company. At Company I, there are various workshops given on social media, and its role in communication. Topics discussed in these workshops are: what to publish, who decides what is published, and also: what are you allowed to publish? At Company A, there are training sessions, but also worldwide training days focused on specific topics. Concerning social media, topics that are discussed on such days are: *"remember when you are on social media, what can happen, remember you're probably privileged to submit information that the general public doesn't have about our company, posting on Facebook or Twitter violating company policy."*

Monitoring. Seven of the interviewed companies had some sort of monitoring tool or process in place. At Company C, monitoring is seen as probably the biggest control. *"Not only being part of the conversation where we choose to be part of the conversation, but identifying the conversations that we are not involved in and my own personal perspective is having that monitoring in place is probably the most important element that I would pick out at the moment. […] You can have monitoring but how do you handle the monitoring if there is an incident, if it escalates, how do you categorize, how quickly do you respond, who authorizes the response, etcetera. Obviously there is a lot more to it than just monitoring."* At Company H, monitoring also has high priority. Monitoring is an in-house process, which is managed by a whole department, which works closely with the Center of Excellence. At Company A, there is a team that monitors and tracks web- and Facebook activity, and responds to complaints posted on social media. Company E uses a monitoring tool to detect mentions of the company. *"This tool monitors, analyses, and provides web care. It has a sort of inbox where all Tweets, but also news articles, Youtube videos, Facebook posts, etcetera, are gathered, and from that inbox, employees can respond to the questions of the customer."* The monitoring tool also shows the influence of the Tweeter, how many followers he has, and how much interaction he has with them, and based on that information, Company E decides if they will or will not respond. At Company D and Company F, Google Alerts is used to stay updated on any comments, posts, and mentions of the company name on the internet.

Crisis management. The interviewed companies all had their different approaches in managing a crisis. For example, Company F, decided never to respond to anything that is said about the company online. *"So for example, it was made known that we're going to reorganize. The next day, it's on the news, and people are saying that we are firing 500 men, saving millions, etcetera, but off course this is always more nuanced than it's in the news. But we do not react on such things."* Company B tries to prevent escalation of any issues. So when an issue arises, it is quickly brought up to the board, which decides how to deal with it. At Company D, there is a handbook for crisis situations, but when something happens, first a quick, practical response will be created so that the organization can react in a fast and uniform way. *There was a big issue a couple of months ago with which we thought we might be associated, and then we thought: okay, what are we going to do on Twitter, because there'll be a lot of tweets about it on Twitter. [...] So one of the colleagues made a standard tweet that we used for: say this if you see one of these tweets. So in that way it's structured, but it's not like we have a big handbook with what we do in each non-crisis situation. We do have a handbook for crisis situations, however."* At Company I, there is an escalation procedure in place, which lists the names of all people involved in social media that should be contacted in case something happens. *"These people also have back-ups, in case they are away, or on vacation or something like that. So it really gets scheduled in such a way that there is always one of the two available."* At Company A, there is a crisis response plan, which is to be enacted based on any number of criteria, for example in response to a virus, or in response to the hacking of a social media account. A specific internet response group handles the crisis.

Access control. At Company C, access control is also an important aspect of controlling social media and is part of the audit process. For access control, there need to be clear guidelines on: who is allowed to speak for the company, who can respond on behalf of the company, who authorizes any responses on behalf of the company etcetera. That has an IT element of controlling who can do those things. To document this, access control policies are in place. Social media rules define responsibilities, these are documented in RACI's, and according to these RACI's, IT access should be set up. *"We do have in different rules and guidance different IT rules and IT security policies and therefore guidelines on access control, these kinds of things. But obviously all the different systems have different access controls."*

Technical. At Company B, there are several technical controls in place. For example: *"firewalls, packages that are able to detect malware, certain strings and combinations of text, that should be examined so we can see what it is before it is admitted to the email environment."* At Company A, they use blocking software to filter out: *"kind of the far fringe, the hate speecher, known malware locations, etcetera."*

5.2.8 Compliance

Then, interviewees were asked: *"How is compliance to company policies, laws and regulations ensured?"* Compliance mechanisms mentioned are self-assessments, audits, sign-offs, and sanctions. All companies have sanctions in place in case someone is in breach with (social media) policy. Not a lot of other compliance mechanisms were mentioned, but this can have to do with the roles of the interviewees. Only one interviewee, at Company C, was involved in audit, and thus knew a lot about compliance checks.

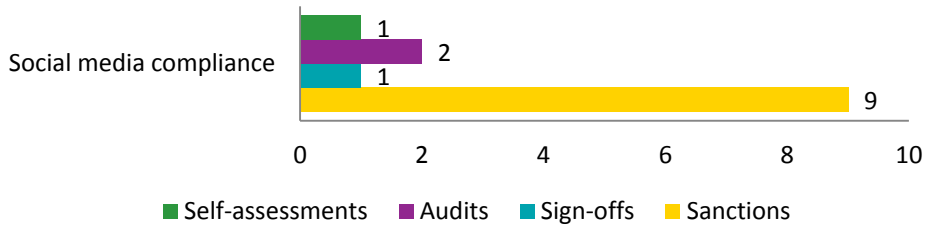


FIGURE 19 | SOCIAL MEDIA COMPLIANCE

The audit function at Company C looks at specific risks associated with social media, and validates the risk and opportunity. First, they identify any risks, think about how to monitor the conversation, how to identify and respond to any issues? *"Is there an escalation procedure, who handles the communication, how timely can we respond to an issue, who is involved, marketing, corporate relations, etcetera, so who is your spokesperson?"* As a global organization, there are a lot of things that should be taken into account: for example, the number of brands that should be monitored, ranging from global to local brands, different time zones, different languages, etcetera. *"Also, audit-related: how do you document all the information, how do you store all the information, and the access to certain levels of information, who can speak on behalf of you?"* Another thing that should be considered is ownership of the monitoring process: *"will you do that in-house, or outsource it to an agency? If you outsource it to an agency: how do you control that you have a consistent message, that you have an SLA, that you can authorize responses by the agency, etcetera?*

A self-assessment is: "*when the managers of the local company have to sign-off on saying whether they are fully, partly, or non-compliant with the rules. When they are partly or non-compliant with the rules, they have to have an action plan on how to become fully compliant with the rules. If you say; no I'm not fully compliant, I am partly compliant or whatever, [...] this is why, this is my action plan, we're doing this, we're doing that, there is a deadline, an owner, and that is tracked. And that is also why we do the self-assessment twice per year so that you can, more timely, also close out the plan and be compliant."*

At Company C, the self-assessment can be seen as the 'first line of defense.' The second line of defense is the local audit and the third line of defense is global audit. These functions consists for a large part of checking: is the rule known, is it communicated, are they compliant with the rule, etcetera. They may both check the self-assessment of the local company and may also check the action plan if that is called for.

5.3 *Overview*

As the information given in the previous sections is a lot to take in at once, in this section an overview is given of the interview results. This starts with an overview of the interview summaries of section 5.1. Then, a comparison of the interview summaries is given, considering the differences between the local organizations (only operating in the Netherlands) and the multinational and global organizations (operating throughout multiple countries) that were interviewed. After that, an overview is given of the findings from the interviews as presented in section 5.2.

5.3.1 Overview of interview summaries

The overview of the interview summaries is shown in Table 9. The table is distributed by the topics mentioned in the interviews: general, governance, risk management, and compliance. General subjects were the social media channels the company is active in, the goals the company is trying to achieve with its social media use, and the benefits that they experience from their social media use. Governance topics were social media responsibility or ownership, and the policies regarding social media. Risk management topics were social media risks, and controls that were in place to mitigate those risks. Compliance was about the checks that were done to ensure adherence to the policy. Some additional notes and remarks that were said in the interviews, and that could not directly be related to one of the topics, were pointed out in separate sections.

	General			**Governance**		**Risk management**		**Compliance**
	Channels	*Goals*	*Benefits*	*Responsibility*	*Policies*	*Risks*	*Controls*	
Company A	Twitter, Facebook (FB)	Promotion	-	Marketing department	For SM use, computer use	Negative comments, trust issues, pre-announcements	Monitoring, training, blocking, crisis plan	Sign-offs, sanctions
	Additional notes: ➢ Social media for helping the company reach its goals							
Company B	Twitter, FB, Hyves, LinkedIn Narrow-casting	Promotion, Image building 'listening'	-	Communication department, IT department, crisis team	Not formal for SM	Malware, reputation damage	Technical	Sanctions
	Additional notes: ➢ Lost productivity of employees, but also time gain in some aspects ➢ Being a 'modern' company requires social media use ➢ Something should first go entirely wrong							
Company C	Twitter, FB, LinkedIn	Promotion	-	Digital team, IT team, corporate relations, legal, marketing	Standards and guidelines for SM	Reputation damage, employee (mis)use	Training, access control, monitoring	Sanctions, audits and self-assessments
	Additional notes: ➢ Customer more involved ➢ Social media is both a risk and an opportunity ➢ Every employee is responsible for SM							

Company D	Twitter, FB, Flickr, Youtube, Yammer	'Listening,' image building, inform stakeholders	Speed of respon-siveness	Communication department, IT and security	Not formal for SM	Reputation damage, employee (mis)use	Access control, monitoring, crisis response	Sanctions
	Additional notes: ➢ Social media is both an opportunity and a risk							
Company E	Twitter, FB, Youtube, LinkedIn	'Listening,' image building, inform stakeholders	Find technical issues and provide a 'stage'	Communication, web care team, representatives, external party, IT	SM do's and don'ts, guidelines	Employee (mis)use, angry customers	Monitoring, training	Sanctions
	Additional notes: ➢ You have to keep up with the customer							
Company F	Twitter, FB, Youtube,	Promotion	-	Employees, marketing, sales	Internet and social media protocol	Confidentiality breach, incorrect info, openness, employee leave	Monitoring, training	Sanctions
	Additional notes: ➢ Social media is a 'hype' ➢ Every employee is responsible for SM							
Company G	Twitter, FB, LinkedIn	Image building	-	Communication department, HR, marketing	Guidelines, policies, do's and don'ts	Confidentiality breach, employee leave	Training	Sanctions
	Additional notes: ➢ Brand ambassadors							
Company H	Twitter, Flickr, FB, Youtube, LinkedIn, Instagram	Promotion	-	Center of Excellence	SM guidelines and policies	Employee (mis)use, angry or dissatisfied customers	Access control, monitoring, training	Sanctions
	Additional notes: ➢ Everyone can be a participant or contributor on social media							
Company I	Twitter, FB, Youtube, LinkedIn, Pinterest	Promotion	-	Communication department	Yes, for SM	Magnifying effect of social media	Training, crisis plan, monitoring	Sanctions
	Additional notes: ➢ Social media is both an opportunity and a risk							

TABLE 9 | OVERVIEW OF INTERVIEW RESULTS

5.3.2 Comparison

It would be interesting to compare the global and local organizations that were interviewed, to find if there are any differences in the way these organizations handle social media. For this purpose, the global organizations have been highlighted in the table, to make them easier to identify.

Something that immediately stands out is the fact that global organizations have a much more positive attitude towards social media, as can be seen in the additional notes. Remarks made in this section are 'social media is both an opportunity and a risk,' it 'improves the speed of responsiveness,' it makes 'customers more involved' and helps with 'reaching company goals.' When looking at the remarks of local companies, they seem less positive. Examples are 'social media is a hype,' or the company won't do anything to structure social media more before 'something goes entirely wrong.' Also noticeable is that two local companies see social media as a necessity, something they have to participate in, like it or not. They state that 'being a modern company requires social media use' and 'you have to keep up with the customer.'

In the table below, an overview is given with the differences in which local and global organizations handle their social media channels, strategy, ownership, responsibility, policies, risks, controls and sanctions. This comparison was made based on the statements in the interview summaries. Local companies were Company B, E and F. Global companies are Company A, C, D, G, H and I.

	Local	**Global**
Channels	Not all social media channels used by local companies had a clear purpose.	Not all SM channels used by global companies had a clear purpose
Strategy	Not one local company had a formal social media strategy in place, with defined goals and metrics	One global company mentioned a specific social media strategy.
Ownership	At local companies, social media is often the responsibility of a communications team or department, with the support of the IT team or department.	At global companies, more parties are involved, such as legal and PR.
Responsibility	At local companies, responsibilities were often not very clearly defined.	At global companies, responsibilities are assigned globally and per country to a person or team.
Policies	At most local companies, social media policies and guidelines were not formally in place. For this purpose the existing standards and guidelines for communication were used.	At global organizations, social media specific rules and policies were formally established.
Risks	The main risk impact was seen by all organizations as reputational damage. The main risk source was employees.	The main risk impact was seen by all organizations as reputational damage. The main risk source was employees.
Controls	Monitoring is seen as the biggest/most important control by most companies, as this is an on-going process. Monitoring at local companies was done either by using free online monitoring tools or paid monitoring tools	Monitoring at global companies was the responsibility of an entire department
Sanctions	Sanctions were used by all companies for disciplining employees. No company specifically measured compliance of employees. At local companies, not much was known about audits and self-assessments	Global companies had more expertise with (social media) compliance audits and self-assessments

TABLE 10 | LOCAL VS. GLOBAL COMPANIES

5.3.3 Overview of key findings

Some key findings from the interview results are shown in the table below, to provide a quick overview of this section. These key findings are structured into: (1) general questions, considering the social media channels, the goals of SM, and the benefits; (2) governance, considering social media ownership and policies; (3) risk management, considering social media risks and controls; and (4) compliance, considering compliance mechanisms.

General	Channels	➢ Twitter and Facebook were used by all companies. Twitter is used for business communications, Facebook for communication with the customer
	Goals	➢ Main goals for social media are promotion and image building. ➢ Promotion is advertising products. Image building is about the company's image.
	Benefits	➢ The speed of responsiveness with which a company can react on certain things is seen as the greatest benefit of social media
Governance	Ownership	➢ The communication department is often the owner of social media in local organizations. Communication uses SM for 'talking' to the customer ➢ Marketing is owner of SM when it is used for promotional purposes ➢ The IT department has an important supportive role in social media.
	Policies	➢ Social media can be included in general policies, such as the communication policy ➢ Specific social media policies are about practical things about social media, amongst others the tone of respect, the language, how content is moderated, etcetera
Risk management	Risks	➢ Main risk source is employees and main risk impact is reputational ➢ Main risks are the distribution of incorrect, confidential or premature information, employee (mis)use and reputational damage
	Controls	➢ Most implemented controls are monitoring and training ➢ Controls are not always formal, but often ad-hoc processes
Compliance	Compliance	➢ Every interviewed company has sanctions in place for violating the policy ➢ Not much was said about self-assessments, audits, and sign-offs

TABLE 11 | OVERVIEW OF ANALYSIS

6 Social media GRC method

In this section, a method is constructed that describes the GRC processes of a company for social media. As said before, a situational method engineering approach was taken as proposed by Van de Weerd and Brinkkemper (2009), by using so-called Process-Deliverable Diagrams (PDD) (see Section 2.2.3). First, a list with observations and recommendations is compiled from different sections of the thesis. The observations and recommendations from this list were added into the PDD's of the GRC processes that were constructed in Section 4 to create methods for social media GRC. In this section, the observations and recommendations are presented, together with the different methods for the social media governance, risk management, and compliance process, and combined into an overall social media GRC method.

6.1 *Observations and recommendations*

Based on the observations made in the interviews, some recommendations are given for the governance, risk management and compliance process. These can be found in Table 12, 13 and 14. The recommendations and findings are again divided into 'governance,' 'risk management' and 'compliance.' The answers to the 'general' questions were included in the governance process, as they are strategic, and creating a strategy is done in the governance process. This made the following structure: (1) governance, considering strategy, ownership and policies, (2) risk management, considering risks and controls, and (3) compliance, considering sanctions. The observations in the table are originating from Table 10 and Table 11. The recommendations given are general recommendations that stem from the contents of the thesis. How to implement those recommendations is explained by key statements that were taken from the contents of the thesis, which refer to the specific sections they are further addressed in.

Before presenting the recommendations for social media governance, risk management and compliance, some overall remarks should be made. The first remark is about the attitude of organizations towards social media. This attitude is not a quantifiable 'thing,' and therefore it is hard to circumstantiate. However, by some quotes from the interviews, it becomes apparent that a lot of the interviewed companies sees social media as a hype, and has not included it in the organization's strategy. But can these organizations still be sure that social media is just a hype and not the new way of doing business? As some influential, leading companies such as IBM see social media as the new way of doing business and have their companies set up as 'social businesses,' it seems hard to believe that social media is just a hype. Also the popularity and the magnitude of social media use seems to indicate that social media is here to stay.

Another observation that was made, which is related to this, is that social media is often the responsibility of one or multiple departments within the company. Sometimes with the support of executives within the company, but often without the active involvement of these executives, board members, or other decision makers. Without the involvement of such strategic players, it is very improbable that social media is used for strategic purposes, and most likely does not have a strategic value to the company.

When companies realize that social media is not just a hype, and start to use it in a more strategic way, by setting a proper strategy, with appropriate goals and metrics for social media, it certainly can have a strategic value for a company, and will possibly make social media use also more efficient and effective.

	Governance		
	Observation (Table 10)	***Recommendation***	***Explanation***
Strategy	Not all social media channels used by the interviewed companies had a clear purpose.	Use separate social media channels for communicating to different stakeholders	• Stakeholders in social media are: citizen/customers, employees, suppliers and corporate customers, government, investors, the firm itself, and affected persons within the firm (Section 3.3.1.1) • Use Twitter for business communication, Facebook for communication with the customer (Table 11)
	Only one, global company had a formal social media strategy in place, with defined goals and metrics	Create a social media strategy with appropriate goals and metrics	• Use the 4C's as guideline for developing a strategy (section 3.3) • Use goals and metrics as identified in Table 6 • Make social media goals SMARRT (see section 3.3.1.2) • Have as main goals promotion and/or image building (Table 11)
Ownership	At local companies, SM is often the responsibility of a communications team or department, with the support of the IT team or department. At global companies, more parties are involved, such as legal and PR.	Establish clear ownership for social media	• Governing bodies are the C-team, the board, and the social media team, CoE, or hub (see Section 4.2.1) • Make sure the communication department is involved in social media for content creation, together with the IT department for supportive tasks, other parties are involved when necessary (Table 11)
	At local companies, responsibilities were often not very clearly defined. At global companies, responsibilities are assigned per country to a person or team.	Define clear roles for social media and assign responsibilities to them	• Commonly found SM roles are: social strategist, community manager, business unit liaison, education manager, SM manager, social analyst, web developer, content strategist, digital strategist, agency partners (see Section 3.3.1.3) • Use RACI charting to assign responsibilities to the roles (see Table 7)
Policies	At most local companies, social media policies and guidelines were not formally in place. For this purpose the existing standards and guidelines for communication were used. At global organizations, social media specific rules and policies were formally established.	Create a specific social media policy	• The policy should discuss: employee access, social media account management, acceptable use, employee conduct, content, security, legal issues and customer conduct (Section 4.2.1.2) • Use the ORCA format when establishing rules in the policy: what is the objective of the rule, what is the risk, what are the controls, and how do you assure compliance to the rule? (Section 5.1.3)

TABLE 12 | OBSERVATIONS AND RECOMMENDATIONS FOR GOVERNANCE

	Risk management		
	Observations (Table 10/Table 11)	***Recommendation***	***Explanation***
Risks	The main risk impact was seen by all organizations as reputational damage. The main risk source was employees.	Use the risk matrix in Table 5	• Risks can originate from the organization, employees, and from external parties (Section 3.2.1) • Risks can have operational, legal and reputational impacts (Section 3.2.2)
Controls	Monitoring is seen as the biggest/most important control by most companies, as this is an on-going process. Monitoring ranges from using free, online tools to special monitoring tools. Training is seen as second most important control.	Implement the following controls: policies, education, monitoring, access control and crisis management	• Policies should discuss: employee access, social media account management, acceptable use, employee conduct, content, security, legal issues and customer conduct (see Section 4.2.1.2) • Education has six steps: establish a decision-making team, assess the company's needs from SM, benchmark employees on their social media knowledge, set the curriculum, create training materials, get employees excited (Section 4.2.2.3) • Monitoring is twofold: it can be done on the content that is created online, and on compliance of employees (Section 4.2.2.3) • Access controls that should be in place are: change management, separation of jobs and responsibilities, separation of development, test, and production environment, user management, controlled access to high authority accounts, password restrictions, verification of accounts and settings (Section 4.2.2.3) • Create a crisis response plan that states: clear criteria for identifying risk, an escalation process, and robust pre-crisis preparation (see Section 4.2.2.3)

TABLE 13 | OBSERVATIONS AND RECOMMENDATIONS FOR RISK MANAGEMENT

	Compliance		
	Observations (Table 10/Table 11)	***Recommendation***	***Explanation***
Sanctions	Sanctions were used by all companies for disciplining employees. No company specifically measured compliance of employees. Not much was known about audits and self-assessments at local companies. Global companies had more expertise with (social media) compliance audits and self-assessments	Identify the level of compliance at the company using Table 8	• Requirements are: baseline governance and reinforcement: enterprise-wide response processes, on-going education program and best practice sharing, leadership from a dedicated and shared central hub (Section 4.2.3.1). • Perform audits or self-assessments that include questions about: strategy and governance, people, processes and technology (see Section 4.2.3.2)

TABLE 14 | OBSERVATIONS AND RECOMMENDATIONS FOR COMPLIANCE

6.2 *Governance*

In the figure below, the method for social media governance is shown. In this method, first stakeholder needs, conditions and options are identified (Section 4.2.1.1). A stakeholder (see Section 3.3.1.1) need could be that customers want or demand the organization to be online. Such a need is analysed based on potential costs and benefits. In addition to this analysis, a PEST analysis is performed to scan the environment (Section 3.3.1.4) and see, for example, what competitors are doing. All this information is transformed into a strategy for social media, with the goals that are envisioned with social media usage, and metrics for measuring the achievement of those goals (see Table 6). Also a policy is set out, to provide guidance and rules in using social media (Section 4.2.1.2). The last step of the governance process is monitoring and reporting (Section 4.2.1.3). In this step, adherence to the policy and achievement of the social media goals is monitored, and the results hereof are reported to stakeholders.

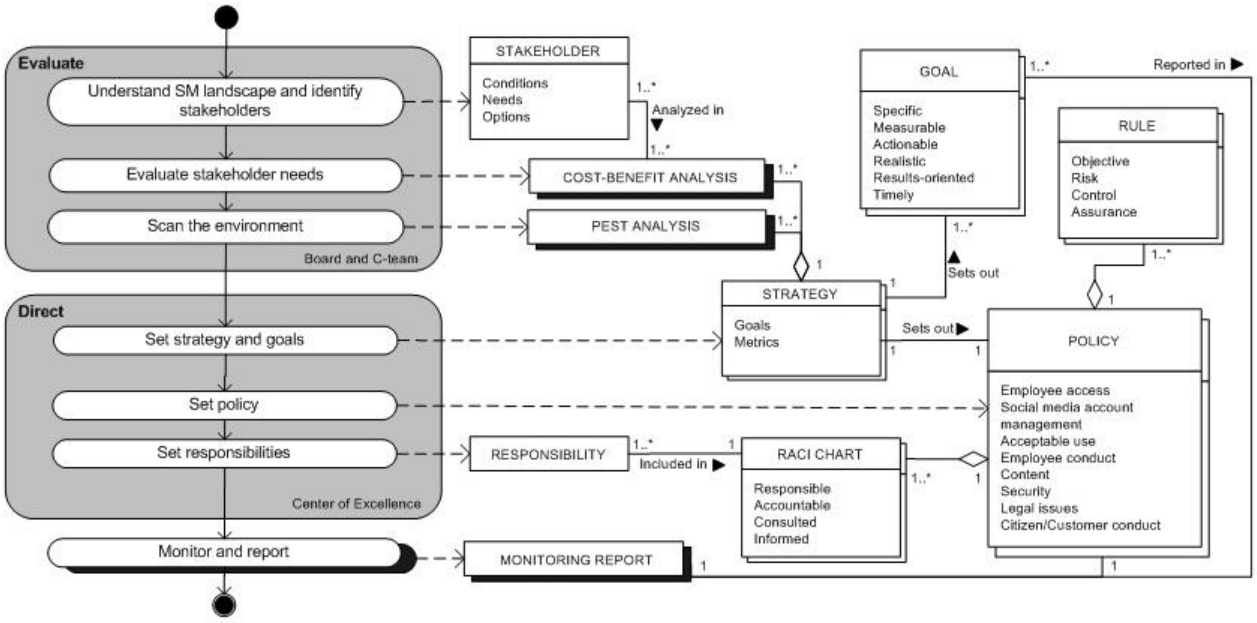


FIGURE 20 | METHOD FOR SOCIAL MEDIA GOVERNANCE

6.3 *Risk management*

The risk management process starts with the characterization of the internal environment: the risk management philosophy, appetite, integrity and ethical values. After this, risk objectives are set. Then, events are identified that could affect the achievement of the risk objectives. These events may be positive, which makes them opportunities, but they can also be negative, which makes them risks (Section 4.2.2.1). The risks are assessed, based on their likelihood and impact in a risk assessment. This can be visualised in a risk matrix or risk mapping (see Section 4.2.2.2). Based on the assessment, the risks get a priority and an appropriate risk response is chosen. Appropriate controls are set out to manage the risks (Section 4.2.2.3). The last step of the risk management process is the monitoring of the effectiveness of these controls and reporting this (Section 4.2.2.4).

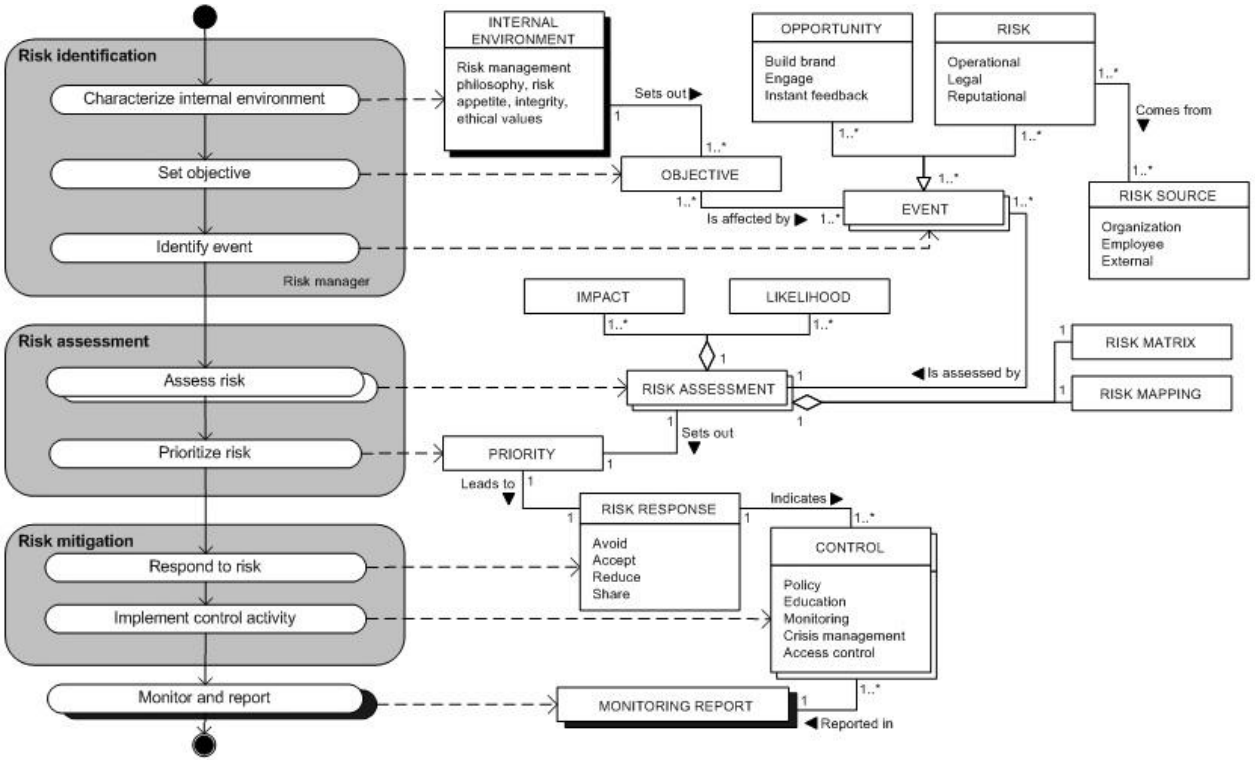


FIGURE 21 | METHOD FOR SOCIAL MEDIA RISK MANAGEMENT

It is very hard to give the risk management process for social media specific roles that are responsible for the process, because at one company, the risk manager (or any other key risk role as described in section 4.1.2) may be responsible for social media risk management, but at another company, it could be the responsibility of the social media CoE. Therefore, the roles for social media risk management are not specified, and only indicated by 'risk manager.' The company should fill in this role according to its own interpretation of the role.

6.4 *Compliance*

The compliance process is shown in Figure 22, and starts with the identification of any compliance requirements. These can be requirements from internal policy, external regulations and other obligations that the company has to adhere to (Section 4.2.3.1). Then, any deviations from those requirements are identified. The number of deviations indicates the compliance level in the company: the more deviations, the lower the compliance level is. The deviations are analysed in audits, self-assessments, security checks, and similar processes (Section 4.2.3.2). Based on this analysis, a number of deficiencies are identified, which are managed by improving controls, creating new controls or changing controls (see Section 4.2.3.3). This is all monitored and reported, which is the final step of the compliance process (Section 4.2.3.4).

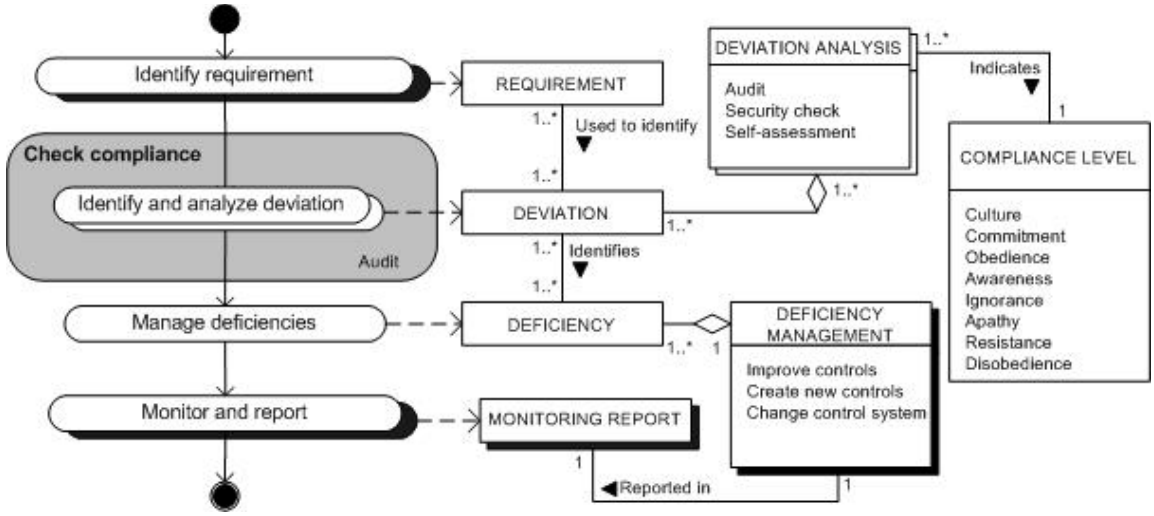


FIGURE 22 | METHOD FOR SOCIAL MEDIA COMPLIANCE

As stated earlier, compliance roles are amongst others compliance manager, head of compliance, compliance officers, compliance assistants and other regulatory compliance positions. When audits are required, often third-party experts are involved, such as auditing companies, to perform the audit (Section 4.1.3). For social media compliance, it is also hard to find a specific role within the company that should be responsible for the process. However, as the audit function is very important in checking compliance, this was chosen as the compliance role in the social media compliance process. This role, just as the role for social media risk management, may change as the company has a different interpretation of the role.

6.5 *Overall method*

The separate social media governance, risk management and compliance processes are combined into one overall method, that was termed the social media GRC method. This method depicts the processes and practices that a company should implement in order to ensure a safe and efficient social media process, by integrating social media into corporate GRC processes. As the method is a so-called process-deliverable diagram (PDD), the method shows social media GRC processes at the left, and the deliverables of these processes on the right. The activities and concepts mentioned in the processes and deliverables are further explained in activity- and concept tables, which can be found in section 9.3 and section 9.4.

The social media GRC method is an integration of the methods that were presented in the previous sections and will not be explained in more detail, as these descriptions for the separate governance, risk management and compliance processes were presented before. The method is shown on the next page and includes an excerpt to show the appropriate governing bodies, governance structures, and social media roles. These were described earlier in section 3.3.1.3 and section 4.2.1.

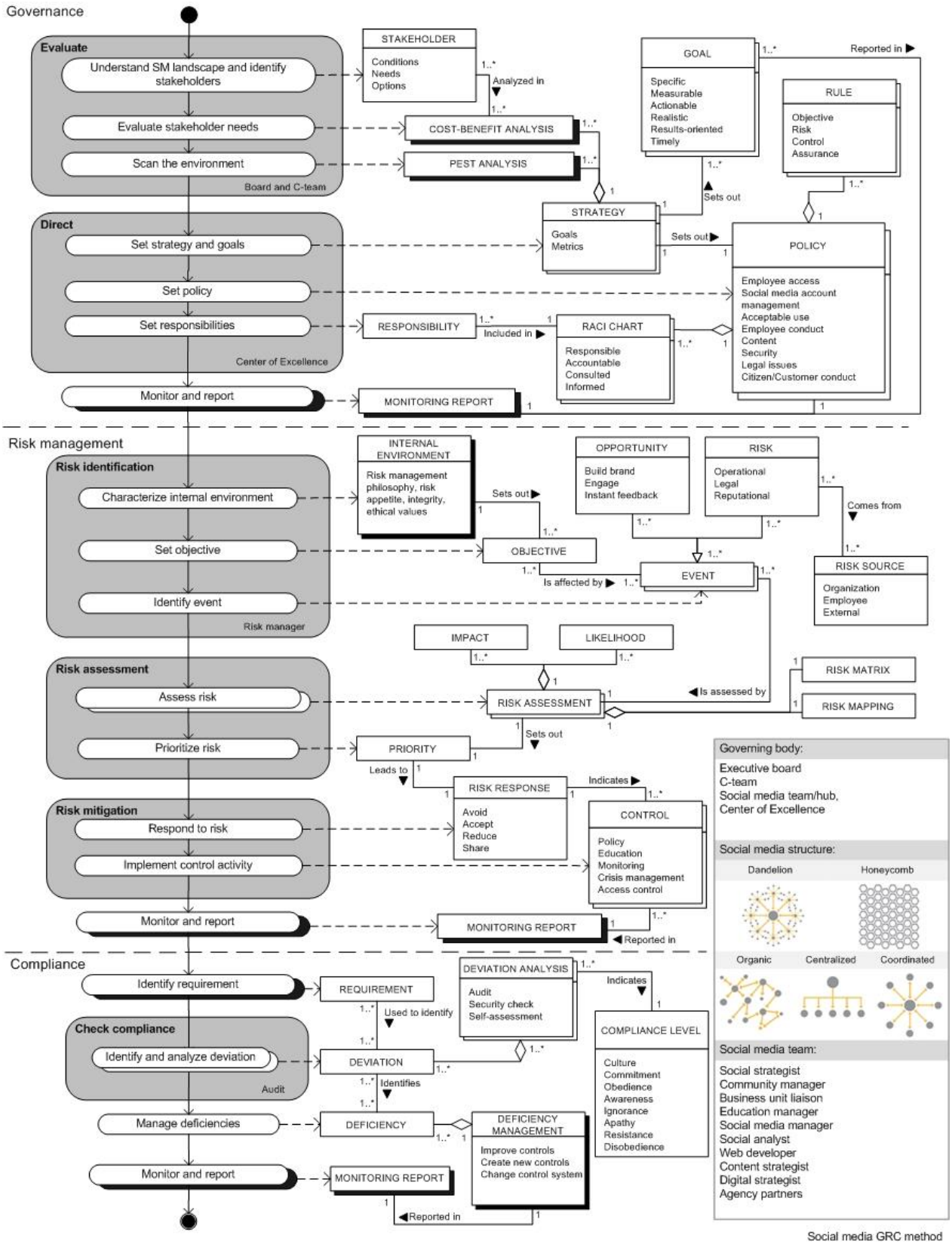


FIGURE 23 | SOCIAL MEDIA GRC METHOD

7 Discussion and conclusion

In this section, the findings of the thesis are discussed. First, the research questions and shortly recapped and the findings from the thesis that are related to this research question are presented. These are findings from literature, and from practice, as they also come from the expert interviews. The findings all refer to the specific sections in the document that provides more information about the topic. Second, the comments that were made during the evaluation session of the social media GRC method by a social media and GRC expert from EY are presented. These comments give an indication of the validity of the method and were used to optimize the method. Third, the limitations of this research are discussed, together with possible opportunities for future work in this specific area.

7.1 *Research questions*

The research question to this research was: *"In which way could social media processes be integrated in corporate GRC processes, in order to make corporate social media use safer and more efficient?"* The three sub questions are used to provide an answer to this question. Therefore, the sub questions and their findings in this thesis are presented below.

The first sub question was: *"Which governance structures and processes are appropriate for social media use?"* Appropriate governance structures for social media are: organic, centralized, coordinated, multiple hub and spoke, and holistic (Figure 9). Important governing bodies that should be present in this structure are the C-team, the board, and a social media team, center of excellence, or hub (section 4.2.1). Social media governance processes are evaluate, direct and monitor and report (Section 4.1.1). The governing body evaluates social media in terms of costs and benefits (Section 4.2.1.1) and sets out a direction for the company, which is communicated by a strategy and policy (Section 4.2.1.2). The adherence to this direction is monitored and reported to stakeholders (Section 4.2.1.3).

The second sub question was: *"Which risks and controls are relevant for social media risk management and what are the appropriate risk management processes?"* The risk management processes are risk identification, risk assessment, risk mitigation, and monitor and report (Section 4.2.2). Social media risks can either have an operational, legal or reputational impact (Section 3.2.2) and can originate from the organization itself, its employees, or from external parties (Section 3.2.1). These risks are assessed based on their likelihood and impact. For assessing risks, either a risk matrix or other risk mapping techniques could be used (4.2.2.2). In the risk mitigation, the company chooses a risk response and appropriate controls. The most relevant controls to prevent social media risks are monitoring, education, policy, crisis management and access control (Section 4.2.2.3). Then the effectiveness of these controls is monitored and reported on (Section 4.2.2.4).

The third sub question was: *"Which compliance mechanisms and processes should be in place?"* Compliance processes are: identify requirement, identify and analyse deviation, manage deficiency and monitor and report. Requirements could originate from internal policy, external regulations and other obligations that the company has to adhere to (Section 4.2.3.1). Any deviations indicate the compliance level in the company (Section 4.2.3.2). Deficiencies that are identified are managed by improving controls, creating new controls or changing controls (see Section 4.2.3.3). This is all monitored and reported (Section 4.2.3.4).

7.2 *Evaluation*

To test the validity of the method, it was evaluated by an expert on both social media and GRC. This expert was a manager in the audit sector, and had extensive knowledge on both governance, risk management and compliance as she was involved in all three processes.

The first comment that was made was about monitoring. In the model, the monitoring is included in the processes 'monitor and report,' which can be found in all three GRC activities. According to the expert, monitoring should not be shown as separate processes or steps, as it is a continuous process. More specifically, she comments on the monitoring step in the compliance process: "I think you monitor regardless of deviations. Monitoring is an in-build step to avoid or react timely to not necessarily deviations in your own actions, but also deviations in desired behaviour from the outside world." She also states that there are different types of monitoring. For example, when someone simply checks the stock level in a company, it can be called monitoring, but also when the entire internet is checked on comments or mentions of the company, it can be called monitoring. There is a very big difference in that. "So it's a different level of monitoring now that you're talking about, part of it obviously monitoring your own success, but you are actually monitoring the whole world for what someone might say about you."

The second comment that was made was about the risk assessment process. She expert remarks: "Yes, this makes sense. When I see risk assessment, I automatically think impact, likelihood." The expert gives a tip in rating the risk, which she does with the use of a table that shows likelihood and impact. "And then the likelihood is highly unlikely to almost certain. But on the impact scale, there are three different types of impact scale: financial, achievement of objectives and reputational." The financial impact is an obvious one off course, as everything can come back to an estimate of a number in terms of financial impact, which is often a percentage of financial impact. The achievement of objectives indicated if the risk influences the ability of the company to achieve its objectives, and could be something like project success. The last one is reputational risk, and this impact has changed with the rise of social media. The expert states on this: "What we used to see, and I'm sure this is seen in many companies, was that you had local and short-lived, up to huge, wide-spread reputation risk. I don't think there is something as local and short-lived anymore, when it comes to reputational damage." So the reputational risk is now very difficult to put a likelihood on, or the level of impact. Nowadays, when something bad is said about a company, it can either remain local, in the local newspaper, or it can be blasted across the internet for all to see within an hour or a few days.

> *"When it comes to reputation, it is very difficult to put a cross in the box of likelihood and impact."*

A third comment that the expert makes is about the functions or roles that are shown in the PDD. She questions the roles that are in the method, saying: "Who are the governing body, risk management and compliance function? So obviously yes, the compliance function could be audit off course, look at requirements, deviations, and report. That makes sense. When you say the risk management I take it to be the topic owner. And the governing body, the board and the executive committee." She gives a hint in this by stating that in global companies, the responsibility for managing risks would also be globally assigned, and this global team would also set the standards, the policies and the procedures about social media. For a local company, that is part of a global structure, these responsibilities are arranged somewhat differently: "When you come down to a local level, then you could say: at a local level the 'digital rock star' is the risk manager for his company, and then global commerce are the governing

bodies, because they design the standards, the tools, the SLA's, the methodology on how you should operate. And then the global or internal audit, you can even have it that the global function designs the rules, local companies and regions follow those rules, and the global function again, checks the compliance."

A fourth comment is made about the identification of risks. The expert states on this: "You could argue that identifying risks is kind of in both [governance and risk] camps." This also is dependent on the structure of the company. For a global company, the expert describes the responsibilities as follows: "You can have social media managed by a global social media team; they evaluate the risks and opportunities, they say this is what we want to do, put in the standards and guidelines and the training etcetera. And then actual risk management is done on a more local level, where you then identify the particular risk and opportunity in my market, with the way I manage it, and who's doing my monitoring, etcetera. And then set either the corporate function or an audit function look at what they're doing, see if they are in compliance with the rules."

The final comment is about responding to a risk. "If this is a local company, and a risk pops up, should they just immediately handle it and respond to it themselves, or should they, go back up to the brand owner to seek approval?"

7.3 *Limitations and future work*

A limitation to this research was the little body of knowledge on social media "G," "R", "C" subjects. A lot has been written on social media uses, benefits and risks, but on the structured use of social media, scientific literature is very lacking. Certainly on the area of (integrated) GRC, which is a term that emerged from business literature, much progress can be made. Another limitation of this thesis was that the interviewees of the expert interviews had very varying roles, and not every interviewee was equally informed on social media GRC in his or her organization. Therefore, it was not only hard to compare the interview results, but also to validate the proposed method.

This work aims to contribute to the body of knowledge on social media and GRC by building a method on how to integrated social media in corporate GRC processes. There are sufficient opportunities for future work in this area, as it is still very new and unknown. Especially on how to use social media in a structured way – by having a social media plan, program or strategy – would be a great addition to the body of knowledge on social media. Also, more research should be conducted on ownership or responsibility of social media. Zerfass et al. (2011) are already conducting research on this topic, but there is still room for improvement, especially when there would also be a focus on the role of the board, C-suite and other executives in social media. Also, it would certainly be beneficial to perform more scientific research on GRC. This is a term that originated from business, and that is also mentioned a lot in business literature, such as white papers and reports. The focus here should be on the integrated of GRC processes, to create a holistic and integrated approach to GRC without the entire enterprise. Furthermore, this thesis would be helped with future work that focuses on the expansion and validation of the social media GRC method. This method was already shown to an expert on social media and GRC, but this is just one person. By showing the method to other experts, and discussing potential up- and downsides of the method, the method could be improved to fit practice better. Also, more 'best practice' examples could be included in this way, to create an optimized and structured way of using social media in an organization.

8 References

Scientific articles used:

1. Back, A., & Koch, M. (2011). Broadening Participation in Knowledge Management in Enterprise 2.0. *it - Information Technology*, *53*(3), 135–141. doi:10.1524/itit.2011.0635
2. Bernoff, J., & Li, C. (2008). Harnessing the Power of the Oh-So-Social Web. *MIT Sloan Management Review*, *49*(3), 36–42.
3. Boyd, D. M., & Ellison, N. B. (2007). Social Network Sites: Definition, History, and Scholarship. *Journal of Computer-Mediated Communication*, *13*(1), 210–230. doi:10.1111/j.1083-6101.2007.00393.x
4. Culnan, M. J., McHugh, P. J., & Zubillaga, J. I. (2010). How large US companies can use Twitter and other social media to gain business value. *MIS Quarterly Executive*, *9*(4), 243-259.
5. Dutta, S. (2010). What 's Your Personal Social Media Strategy? *Harvard Business Review*, *88*(11), 127–130.
6. Harris, M., & Furnell, S. (2012). Routes to security compliance: be good or be shamed? *Computer Fraud & Security*, *2012*(12), 12–20. doi:10.1016/S1361-3723(12)70122-7
7. Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design Science in Information Systems Research. *MIS quarterly*, *28*(1), 75–105.
8. Hrdinová, J., Helbig, N., & Peters, C. S. (2010). *Designing social media policy for government: Eight essential elements*. Center for Technology in Government, University at Albany.
9. Kaplan, A. M., & Haenlein, M. (2010). Users of the world, unite! The challenges and opportunities of Social Media. *Business Horizons*, *53*(1), 59–68. doi:10.1016/j.bushor.2009.09.003
10. Katz, D., & McIntosh, L. (2013). The Board, Social Media and Regulation FD. *New York Law Journal*.
11. Kietzmann, J. H., Hermkens, K., McCarthy, I. P., & Silvestre, B. S. (2011). Social media? Get serious! Understanding the functional building blocks of social media. *Business Horizons*, *54*(3), 241–251. doi:10.1016/j.bushor.2011.01.005
12. Larson, K., & Watson, R. (2011). The value of social media: toward measuring social media strategies. *Thirty Second International Conference on Information Systems, Shanghai*, 1–18.
13. Lincoln, Y. S., & Guba, E. G. (1985). *Naturalistic Inquiry*. Newbury Park, CA: Sage Publications.
14. Mittal, A. (2012). Enabling Collaboration and Broad Communication Through Social Media At Workplace. *IT Matters*, *10*(1), 15–21.
15. Molok, N. N. A., Chang, S., & Ahmad, A. (2010). Information Leakage through Online Social Networking: Opening the Doorway for Advanced Persistence Threats. *Proceedings of the 8th Australian Information Security Management Conference* (pp. 70–80).
16. Myers, M. (1997). Qualitative research in information systems. *Management Information Systems Quarterly*, *21*(2), 241–242.
17. Nelson, S., & Simek, J. (2011). Mitigating the Legal Risks of Using Social Media. *Information Management Journal*, *45*(5).
18. Ohki, E., Harada, Y., Kawaguchi, S., Shiozaki, T., & Kagaya, T. (2009, November). Information security governance framework. In *Proceedings of the first ACM workshop on Information security governance* (pp. 1-6). ACM.
19. Oreilly, T. (2007). What is Web 2.0: Design patterns and business models for the next generation of software. *Communications & strategies*, *65*(65), 17–37. doi:10.2139/ssrn.1008839
20. Peffers, K., Tuunanen, T., Rothenberger, M. a., & Chatterjee, S. (2007). A Design Science Research Methodology for Information Systems Research. *Journal of Management Information Systems*, *24*(3), 45–77. doi:10.2753/MIS0742-1222240302
21. Racz, N., Weippl, E., & Seufert, A. (2010a). A process model for integrated IT governance, risk, and compliance management. *Proceedings of the Ninth Baltic Conference on Databases and Information Systems (DB&IS'10)*, 155–170.
22. Racz, N., Weippl, E., & Seufert, A. (2010b). A frame of reference for research of integrated governance, risk and compliance (GRC). *Proceedings of the 11th Joint IFIP TC6 and TC11 Conference on Communications and Multimedia Security*, 106–117.
23. Safko, L., & Brake, D. K. (2009). *The Social Media Bible: Tactics, Tools, and Strategies for Business Success*. Hoboken, NJ: John Wiley & Sons
24. Scandizzo, S. (2005). Risk mapping and key risk indicators in operational risk management. *Economic Notes*, *34*(2), 231-256.
25. Turban, E., Bolloju, N., & Liang, T.-P. (2011). Enterprise Social Networking: Opportunities, Adoption, and Risk Mitigation. *Journal of Organizational Computing and Electronic Commerce*, *21*(3), 202–220. doi:10.1080/10919392.2011.590109
26. Van de Weerd, I., & Brinkkemper, S. (2009). Meta-Modeling for Situational Analysis and Design Methods. *Handbook of Research on Modern Systems Analysis and Design Technologies and Applications* (pp. 35–54)

27. Van Grembergen, W., De Haes, S., & Guldentops, E. (2004). Structures, processes and relational mechanisms for IT governance. *Strategies for information technology governance*, 1-36.
28. Van Zyl, A. S. (2009). The impact of Social Networking 2.0 on organisations. *Electronic Library, The*, *27*(6), 906-918.
29. Verhoeven, P., Tench, R., Zerfass, A., Moreno, A., & Verčič, D. (2012). How European PR practitioners handle digital and social media. *Public Relations Review*, *38*(1), 162–164
30. Zerfass, A., Fink, S., & Linke, A. (2011) Social Media Governance: Regulatory frameworks as drivers of success in online communications. In *Pushing the envelope in public relations theory and research and advancing practice, 14th International Public Relations Research Conference* (pp. 1026-1047). Gainesville, FL: Institute for Public Relations.

White papers and reports used:

1. BITS. (2011). *Social media risks and mitigation.* Washington: BITS
2. COSO. (2004). *Enterprise risk management: Integrated framework*. New Jersey: AICPA.
3. EY. (2010). *Top privacy issues for 2010*. London: EYGM Limited.
4. EY. (2011). *The digitisation of everything*. London: Ernst & Young LLP.
5. EY. (2012a). *Fighting to close the gap: Ernst & Young's 2012 Global Information Security Survey*. London: EYGM Limited.
6. EY. (2012b). *Protecting and strengthening your brand*. London: EYGM Limited.
7. HBR. (2010). *The New Conversation: taking Social Media from talk to action*. Boston: Harvard Business School Publishing.
8. IBM. (2011). *The Social Business: Advent of a new Age*. Somers: IBM Corporation.
9. ISACA. (2010). *Social Media: Business Benefits and Security , Governance and Assurance Perspectives*. Rolling Meadows: ISACA.
10. ISO. (2008). *31000:2009. Risk management – Principles and guidelines*. Geneva: ISO.
11. ITGI. (2007). *COBIT 4.1*. Rolling Meadows: ITGI.
12. Merril, T., Latham, K., Santalesa, R., & Navetta. (2011). *Social Media: The Business Benefits May Be Enormous, But Can the Risks -- Reputational, Legal, Operational -- Be Mitigated?* Zurich: ACE Limited
13. Nielsen. (2012). *State of the media: the social media report 2012.* New York: The Nielsen Company
14. Owyang, J. (2011). *Social business readiness: how advanced companies prepare internally*. San Mateo: Altimeter Group.
15. Rozwell, C., Lapkin, A., & Fletcher, C. (2010). *Look Beyond Marketing for Competitive Advantage With Social Media.* Stamford: Gartner
16. Stoneburner, G., Goguen, A., & Feringa, A. (2002). *Risk Management Guide for Information Technology Systems Recommendations of the National Institute of Standards and Technology*. Washington: U.S. Dept. of Commerce

Websites used:

1. Donston-Miller, D. (2011). *5 Enterprise Social Trends For Next 5 Years*. Retrieved from http://www.informationweek.com/social-business/news/social_crm/231600408
2. Facebook (2013). *Key facts*. Retrieved from http://newsroom.fb.com/Key-Facts
3. Goodchild, J. (2011). *Social engineering: 3 examples of human hacking.* Retrieved from http://www.csoonline.com/article/663329/social-engineering-3-examples-of-human-hacking
4. Grant, M. (2010). *10 Reasons to Have a Social Media Response Triage Flowchart*. Retrieved from http://www.socialfish.org/2010/11/social-media-response-triage.html
5. Swallow, E. (2011). *HOW TO: Build a Social Media Education Program for Your Company*. Retrieved from http://mashable.com/2011/01/18/social-media-training/#
6. Toptenreviews. (2013). *Employee Monitoring Software: What to Look For.* Retrieved from http://employee-monitoring-software-review.toptenreviews.com/

9 Appendix

9.1 *Interview guide*

To have consistent interviews, questions and content, an interview guide was created and the interviews were conducted according to this guide. The main goal of the expert interviews is to explore if the theoretical assumptions made in the theoretical background are correct and justified. Also, the interviews will identify current governance, risk management and compliance practices for social media in the enterprise: how has the company assigned ownership of social media? Do they see any risks related to social media use? In order to accomplish this, the questions were categorized according to the three GRC topics.

First, some general questions about the interviewee, his position and experiences with social media were asked. Also, the interviewee was asked which social media channels were used in the company, and what goals the company tried to achieve with this. Those general questions were asked to get a general picture of the company's social media use, and its/the interviewees attitude towards social media. The next questions were about governance. Those questions were asked to identify who was responsible for social media in the organization, and which structures for decision-making were in place, and to identify if there was a policy and strategy for social media in place.
The next set of questions was on risk management. Those questions identified which risks the company/interviewee experienced from their social media use, and which controls the company had in place to mitigate those risks. The next questions, that were on compliance, identified how compliance was checked or measured in the organization. The questions are listed below.

Questions about interviewee
- What is your current position at the company?
- What are your tasks and responsibilities in regard to social media?
- What is your experience or opinion with/about corporate social media use?

General questions?
- Which social media channels does your organization use and for which business purposes/reasons?
- Does the company experience any effects, either positive or negative, of social media use?
- Does the organization use goals and metrics to identify/measure those effects?

Governance
- Who has ownership of social media? If there are multiple parties involved, how is the decision-making structure between those parties?
- Are there any policies, guidelines, or best practices in place for social media use?

Risk management
- Are there risks, related to social media, that you/your company encounters?
- Which techniques or mechanisms are in place to handle/mitigate these risks?

Compliance
- How is compliance to company policies, laws and regulations ensured?
- How is non-compliance handled?

9.2 *Social media risks*

Operational

Risk	Description	Control
Identity Theft	People share a lot of personal information on SM. Criminals use this information to commit identity theft.	• Establish a SM use policy and best practices and raise awareness through training and communications. • Monitor for compliance with corporate policy and for the use of corporate brand on the Internet. • Modify security challenge questions to eliminate information that may be readily available on SM sites. • Require unique and complex passwords for access to systems containing confidential customer or corporate information. • Consider a cyber liability policy for the intentional leakage of customer data by an employee or customer
Spreading Malware	Potentially increasing threats of malware attacks to the institution's infrastructure and data due to employee use of social networks on company property and through remote access devices.	• Use a third-party vendor to monitor IT infrastructures, scan all files downloaded and keep security patches up to date. • Make sure employees use effective passwords and multifactor authentication technology. • Enforce security policies and procedures and implement a security awareness program to educate employees • Prohibit employees from installing unauthorized software. • Deploy an automated backup software to safeguard data and utilize full-disk encryption software to render hard drive data • Use of key fobs to log in to a secure network from an unsecure access when employees work remotely. • Monitor website traffic and restrict access to sites that pose significant risk. • Have an emergency communication and response plan. • Have a SM disclosure that advises customers not to click on links posted by other users • Create and consistently use a unique shortened URL so that customers recognize your institution's links
Social Engineering	Social engineering is a collection of techniques used to manipulate people into performing actions or divulging confidential information, namely the unauthorized acquisition of sensitive information or inappropriate access privileges by a potential threat source.	• Create a security aware culture, by continual training and policies enforcement • Train staff in being sceptical of unusual requests. Employee monitoring, requests for change in the level of access, and other insider threat related concerns are essential to detect social engineering attempts. • Deploy an intelligent web proxy to block certain functionality on SM sites identified as risky. • Deploy a DLP solution on web traffic to block information classified as sensitive • Deploy a DLP solution and content blocking on corporate email to identify attacks. • Given high instances of usage by employees of all sites in question, an internal assessment of security should be made. Those employees who are at higher risk for social engineering should be investigated and educated
Measuring success	Calculating a SM return on investment (ROI) presents a challenge.	• Decide upon which tools and metrics to use for measuring the effectiveness of SM efforts. Then, the first step in measuring is to determine its objectives for SM use, what it wants to measure and how. Three categories of metrics can be identified: exposure, engagement and outcomes

Products Lack Maturity	SM is not yet mature. This presents potentially serious consequences that can affect brand image, security reputation, the bottom line and customers' personal and account information.	• Create a policy for the overall organization regarding SM and for the specific individual that have will be accessing the company SM profiles. If necessary, limit access to only select individuals, or use tools to allow multiple employees to have access to the profiles and assign and monitor tasks. • Post SM disclosures on your profiles and company site advising customers that your organization will never ask for personal or account information, that the company is not responsible for the security, privacy or any other operations of SM sites. • Assign a SM team to actively manage company profiles and keywords for suspicious activity with the use of SM monitoring • Develop a strategy to manually log and measure SM measurements, or find sites that provide some analytical data. • Create a SM workflow for yourself or your team to help you optimize and manage time when researching new SM announcements and upcoming site updates.
Managing Access	It's important to carefully manage employee access to SM sites. Restricting SM access to only those employees that have a legitimate business need will make monitoring much easier.	• Access controls, for example limiting access to SM sites to those with formal approval to use such sites, or permitting employees to access SM sites only during lunch breaks under certain conditions • Policies and guidelines, and train employees on this • Have HR, Compliance, Information Security and/or the SM administrators monitor mentions of the company on SM, with the use of free or fee-based tools. • Develop training to educate employees on the policies
Lack of centralized governance	A clear and well-publicized governance structure for overseeing and coordinating SM activity that enables employees to closely coordinate their activities across businesses and have a clear understanding of chain of command and accountability will ensure consistent messaging and preserve data security.	• As a company develops a SM program, it's essential that it organize a group of individuals to manage and implement policies, strategy and procedures • Three elements of good SM governance include executive management and involvement, an organizational structure for managing SM, and a clear policy and set of procedures. • Establish a decision-making structure. Companies that are just beginning to use SM tend to use a highly centralized top-down approach, whereas more experienced institutions use a more flexible "hub and spoke" approach • Three roles are key to managing SM: Overall strategist(s) and leader, Moderators or managers liaising with different parts of the company and serving as resources, and Key SM manager within the business units deploying SM that provide on-the-ground support, oversight and liaison with the SM moderators • Optimal governance requires full collaboration among between the oversight function, Legal and Compliance, Technology Risk Management, and other departments identified within the institution.
Physical security risk	Revealing too much in SM may pose a physical security threat, for example stalking or even kidnapping	• Limit the information you share on SM sites to prevent physical security risks, such as stalking or kidnapping • Keep your personal information private. Don't post your full name, social security number, address, phone number, etc • Don't "friend" someone you don't personally know. Stalkers are masters at creating fake personas • Be alert and be wary. When all else fails, remove your SM accounts.
SM content is forever	For many company of size, there is a large number of posts, positive and negative, about them online, outside official marketing channels.	• Contact the hosting provider to request content removal. • Make negative online content irrelevant. By adding many positive entries that outweigh the negative ones, so that when search results for the company are shown, only the positive ones are seen • Use services such as Reputation Defender and iCrossing, for acting upon negative SM events on behalf of the company.
Lack of Productivity	The use of SM can be a contributing factor to lost productivity in the work place.	• Monitor use of SM sites and block SM sites if necessary • Create a SM policy, encourage self-policing of SM use and provide proper supervision.

TABLE 15 | OPERATIONAL RISKS AND MITIGATION

Legal

Risk	Description	Mitigation
Lack of Separation of Personal and Professional Communications	When employees use SM for both personal and professional purposes, there is greater risk of mistakenly using work-related accounts to express personal opinions or of accidently communicating with personal contacts through a work account.	• Only read and respond to messages, alerts or postings from the specific webpage to which they are attached. • Ensure that personal and business alerts are directed to separate mail accounts or cell numbers. • Only link work-related accounts to the same third-party platform (such as HootSuite) on business and personal computers and mobile device applications. • Attach a disclaimer to personal messages that states that the views expressed do not reflect those of the company • Make it company practice to: review all SM message drafts, and conduct all work-related SM contacts at work
Civil Litigation	When an employee acts as a representative of their firm, their actions could potentially be used against the firm.	• Policies and procedures outlining the use of SM, professionally and personally • Employee training policies, procedures and consequences for failing to comply.
eDiscovery	Information on SM sites falls under the category of ESI. There are several aspects of legal discovery,, which impacts eDiscovery and potentially leads to risks associated with the use of SM.	• Policies on the use of SM sites and the use and preservation of information, Train employees on these policies • Establish an information retention program, and document gaps and plans for remediation. • Take inventory of used SM sites that are used, and research controls and policies on these sites • Look into software for the preservation and production of SM information. • Maintain consistency with retention and discovery practices
Compliance to company policy, laws and regulations	Companies need to understand the laws, including those in countries in which they do business.	• Create SM policies and train employees on those policies and on risks • Consider whether a particular platform is appropriate for the nature of the interaction or information being shared. • Perform a risk assessment prior to implementing a SM presence and review content prior to posting. • Establish on-going site content monitoring, identification, escalation and remediation of any issues
Information Retention Management	How quickly are firms expected to retain public communications?	• Education for employees to make them aware of the policy • Training should be given to employees to help them make appropriate decisions when interpreting the SM policy • Companies should assess their current record retention capabilities to determine their suitability for SM requirements
Endorsement Guidelines	Care must be taken when using SM conversations in the context of advertising.	• Online publishers must disclose relationships with advertisers when they receive free products for review • Policies, practices and guidelines around required disclosure format should be created.
Labour Relations	The use of SM by employees and employers is increasingly being impacted by issues related to employment and labour laws. These issues include pre-employment screening and hiring practices, unfair labour practices, harassment and safety issues.	• SM policy around the usage of SM on and off network • Carefully consider reason for discipline, and consult with the Legal and HR departments. • Understand labour laws and maintain a relationship with Legal and HR. • Have transparent processes and documentation when vetting potential employees • Verify information obtained on SM – not all information is accurate. • Review liability insurance programs to ensure financial coverage when sued
Disclosure of Sensitive Information	Users of SM can share information that is considered sensitive or proprietary from a business perspective.	• Establish training for employees and create of two sets of policies – one governing personal usage by employees and the other governing business usage.

TABLE 16 | LEGAL RISKS AND MITIGATION

Reputational

Risk	Description	Mitigation
Reputation threat	Reputational threats originating from employees or external sources that may damage the image and reputation of a company	• Training employees on SM use, risks, company policies and guidelines is the first line of defence for preventing inappropriate dissemination of content and for sensitizing them to potential reputational risks from outside sources. • An institution should clearly identify reputational threats and the criteria for determining potential risk to a company's reputation.
Lack of monitoring	To effectively use and manage SM, a company will need to closely monitor posts, tweets or comments regarding the firm	• Clear monitoring objectives • Clear response plan and escalation contacts for negative or harmful postings from both external and internal sources. Additionally some standards for immediate post/comment removal for inappropriate content should be in place • Use different tools for monitoring and determine which keywords to monitor
Insufficient employee training	Reputational and other forms of risk in use of SM can arise when employees, customers and other stakeholders are not made fully aware of a company's approved policy, procedures and strategy for proactive SM use.	• A company should set about informing its employees and external audiences with a PR campaign about its SM program. • Since employee involvement in SM will vary based on roles within the company, it might be more efficient to offer levels of training: high-level overview of SM in general, more in-depth look at SM tools with specific demonstrations of how they work, hands-on training in using the tools, best practices for privacy settings • A company may also want to sensitize its clients and other external stakeholders of best practices and risks of using SM.
Negative brand impacts	Missteps in use of SM by company employees, false or inaccurate information circulating through SM, or misuse of corporate trademarks, present potentially serious, long-lasting negative impact on a company's brand and reputation.	• A robust 24/7 monitoring system, also known as an Online Reputation Management platform, to listen for negative or defamatory content in real-time. • A company must develop and implement a clear crisis communications plan. • Timeline responses are important. A failure to respond in a timely way can reflect poorly on the company • A tiered response time outline is recommended. The outline should contain a minimum of three levels, high, medium and low, with definitions and examples of each to explicitly define each. • Responses to comments and complaints must always be sincere and direct. • Comprehensive training should be mandatory for staff members who monitor/assess potential threats or client queries
Responding to a crisis	A company should have a crisis communications plan that should include both defensive and proactive use of SM	• An effective communications plan should include: Clear criteria for identifying risk that is likely to develop into a crisis , An escalation process that details next steps in addressing the crisis, and Robust pre-crisis preparation, detailed responses for different kinds of crisis, and a process for evaluating the success of crisis response.

TABLE 17 | REPUTATIONAL RISKS AND MITIGATION

9.3 *PDD activity tables*

Governance

Evaluate	Understand SM landscape and identify stakeholders	Recognize and understand the social media landscape (Kietzmann et al., 2011) and identify STAKEHOLDERS (Larson & Watson, 2011)
	Evaluate stakeholder needs	Evaluation of STAKEHOLDER needs, conditions and options (ITGI, 2007), in a COST-BENEFIT ANALYSIS (Katz & McIntosh, 2013)
	Scan the environment	Scan of the environment in order to understand the velocity of conversations and other information flows that could affect current or future position in the market (Kietzmann et al., 2011), for example with a PEST ANALYSIS.
Direct	Set strategy and goals	The firm needs to develop a STRATEGY that is congruent with, or suited to, different social media functionalities and the GOALS of the firm (Kietzmann et al., 2011).
	Set policy	Any STRATEGY to address the risks of social media usage should first focus on user behaviour through the development of a POLICY ISACA (2010). The POLICY should set out RULES on acceptable use (Hrdinová et al., 2010).
	Set responsibilities	Direct social media use with the allocation of roles and RESPONSIBILITIES (EY, 2010), which should be included in the social media POLICY (Hrdinová et al., 2010) and can be documented in a RACI CHART (ITGI, 2007).
Monitor & report		The performance, compliance and progress against agreed direction and objectives is monitored (ITGI, 2007). The results hereof are communicated to relevant stakeholders in a MONITORING REPORT (Ohki et al., 2009).

TABLE 18 | ACTIVITY TABLE FOR GOVERNANCE

Risk management

Risk identification	Characterize internal environment	The INTERNAL ENVIRONMENT sets the basis for how risk is viewed and addressed by an entity's people, including risk management philosophy and RISK appetite, integrity and ethical values, and the environment in which they operate (COSO, 2004).
	Set objective	Enterprise risk management ensures that management has in place a process to set OBJECTIVES and that the chosen OBJECTIVES support and align with the entity's mission and are consistent with its risk appetite (COSO, 2004)
	Identify event	Internal and external EVENTS affecting achievement of an entity's OBJECTIVES must be identified, distinguishing between RISKS and OPPORTUNITIES (COSO, 2004).
Risk assess-ment	Assess risk	RISKS are analysed, considering LIKELIHOOD and IMPACT, as a basis for determining how they should be managed. RISKS are assessed on an inherent and a residual basis.
	Prioritize risk	Based on LIKELIHOOD and IMPACT of a RISK, the RISK is assigned a PRIORITY
Risk mitigation	Respond to risk	Management selects RISK RESPONSES – avoiding, accepting, reducing, or sharing RISK – developing a set of actions to align RISKS with the entity's risk tolerances and risk appetite (COSO, 2004).
	Implement control activity	Policies and procedures are established and implemented to help ensure the RISK RESPONSES are effectively carried out (COSO, 2004)
Monitor & report		The entirety of enterprise risk management is monitored and modifications made as necessary. monitoring is accomplished through on-going management activities, separate evaluations, or both (COSO, 2004). This is documented in MONITORING REPORT.

TABLE 19 | ACTIVITY TABLE RISK MANAGEMENT

Compliance

Identify req.ment		Identify regulatory, legal, contractual, and other obligations that affect the organization's operations (Racz et al., 2010a).
Manage compliance	Identify and analyse deviation	Adherence is examined for instance through internal and external audits, self-assessments, and security checks. The frequency of these examinations depends on external requirements and on the impact of potential DEVIATIONS (Racz et al., 2010a).
	Manage deficiencies	The results of the DEVIATION ANALYSIS define the requirements for DEFICIENCY MANAGEMENT. At this stage existing DEFICIENCIES are eliminated through improvement of existing controls, creation of new controls, or through a makeover of parts of the control system (Racz et al., 2010a).
Monitor and report		All actions taken are documented, and relevant information is communicated to internal and external stakeholders in a MONITORING REPORT (Racz et al., 2010a).

TABLE 20 | ACTIVITY TABLE COMPLIANCE

9.4 *PDD concept table*

STAKEHOLDER	STAKEHOLDERS from a firm's perspective that might interact via social media, are: customers, employees, suppliers and corporate customers, government, investors, and the firm itself. Within the firm, affected parties can be stakeholders.
COST-BENEFIT ANALYSIS	Weighing the costs and benefits of participating in social media with respect to investors and analysts as opposed to simply customers. This could involve reaching out to large investors for their views, examining how competitors handle social media, as well as carefully addressing compliance concerns (Katz & McIntosh, 2013)
PEST ANALYSIS	PEST analysis is often used in strategic management and describes four macro-environmental factors: political, economic, social and technological.
STRATEGY	Sets out direction of social media use, and provides goals and metrics (Safko & Brake, 2009). Develop by using a SWOT analysis to evaluate strengths and weaknesses, as well as opportunities and threats.
GOAL	Organizations should carefully consider which GOALS they are trying to reach with social media. ITGI (2007) recommends these to be: Specific, Measurable, Actionable, Realistic, Results-oriented and Timely (SMARRT).
POLICY	Represent official positions that govern the use of social media by employees in organizations, and should consider: employee access, social media account management, acceptable use, employee conduct, content, security, legal issues, and citizen/customer conduct (Hrdinová et al., 2010).
RULE	A RULE should have the ORCA format: what is the OBJECTIVE, what is the RISK, what are the CONTROLS, and how to provide assurance?
RESPONSIBILITY	The RESPONSIBILITY of an employee in social media, can be documented in RACI CHART
RACI CHART	A RACI CHART identifies who is Responsible for, Accountable for, Consulted for, and Informed about the deliverable (ITGI, 2007).
MONITORING REPORT	REPORT on MONITORING the performance, compliance and progress against agreed direction and OBJECTIVES
INTERNAL ENVIRONMENT	Encompasses the tone of an organization, and sets the basis for how RISK is viewed and addressed by an entity's people, including risk management philosophy and risk appetite, integrity and ethical values, and the environment in which they operate (COSO, 2004).
OBJECTIVE	OBJECTIVE of the risk management process

EVENT	EVENTS can be internal or external and affect the achievement of an entity's objectives. A distinction is made between RISKS and OPPORTUNITIES.
OPPORTUNITY	An EVENT that has a positive consequence for the company
RISK	An EVENT that has a negative consequence for the company
RISK SOURCE	The source that risk originates from. This can either be the organization, an employee, or an external party (EY, 2012b)
RISK ASSESSMENT	The process of determination of LIKELIHOOD and IMPACT after identification of risk EVENTS (COSO, 2004).
IMPACT	The adverse IMPACT of a risk
LIKELIHOOD	The LIKELIHOOD that a risk occurs
PRIORITY	Based on the risk levels presented in the RISK ASSESSMENT, the implementation actions are prioritized (Stoneburner et al., 2002)
RISK MATRIX	A MATRIX for visualising the likelihood and impact of social media risks
RISK MAPPING	A MAPPING for visualising the likelihood and impact of social media risks, for example a probability/severity chart (Scandizzo, 2005).
RISK RESPONSE	The development of a set of actions to align risks with the entity's risk tolerances and risk appetite. RISK RESPONSE can either be: avoiding, accepting, reducing, or sharing risk.
CONTROL	Activities to ensure the risk responses are effectively carried out.
MONITORING REPORT	REPORT on the MONITORING of the risk
REQUIREMENT	Regulatory, legal, contractual, and other obligations that affect the organisation's operations (Racz et al., 2010a)
DEVIATION	The DEVIATION between REQUIREMENTS and practice
DEVIATION ANALYSIS	Checking adherence
COMPLIANCE LEVEL	Level of compliance in the organization, ranging from: culture, commitment, obedience, awareness, ignorance, apathy, resistance, disobedience
DEFICIENCY	A missing control, incomplete control, or control that is not properly executed
DEFICIENCY MANAGEMENT	Elimination of existing DEFICIENCIES through improvement of existing controls, creation of new controls, or through a makeover of parts of the control system.
MONITORING REPORT	REPORT on the MONITORING of the risk. May include incidents, sign-off status, dashboards monitoring the status of compliance activities, or key risk indicators (Racz et al., 2010a).

TABLE 21 | CONCEPT TABLE ENTIRE PDD

9.5 *Literature review citations*

The third cycle of the literature review consists of citation counting. Below, a list is shown of the literature used , and how often it is cited by other authors. The number of citations was taken from Google Scholar. Not all literature used was cited by other authors, and those articles were left out. The list below starts with the article with the highest number of citations.

Scientific literature	
Reference	*Cited by*
Lincoln, Y. S., & Guba, E. G. (1985). Naturalistic Inquiry. Newbury Park, CA: Sage Publications.	31970
Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design Science in Information Systems Research. MIS quarterly, 28(1), 75–105.	4109
Oreilly, T. (2007). What is Web 2.0: Design patterns and business models for the next generation of software. Communications & strategies, 65(65), 17–37. doi:10.2139/ssrn.1008839	2434
Kaplan, A. M., & Haenlein, M. (2010). Users of the world, unite! The challenges and opportunities of Social Media. Business Horizons, 53(1), 59–68. doi:10.1016/j.bushor.2009.09.003	1638
Myers, M. (1997). Qualitative research in information systems. Management Information Systems Quarterly, 21(2), 241–242.	1462
Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. Journal of management information systems, 24(3), 45-77.	612
Safko, L. (2010). The social media bible: tactics, tools, and strategies for business success. John Wiley & Sons.	280
Kietzmann, J. H., Hermkens, K., McCarthy, I. P., & Silvestre, B. S. (2011). Social media? Get serious! Understanding the functional building blocks of social media. Business Horizons, 54(3), 241-251.	226
Bernoff, J., & Li, C. (2008). Harnessing the Power of the Oh-So-Social Web. MIT Sloan Management Review, 49(3), 36–42.	169
Van Grembergen, W., De Haes, W., & Guldentops, E. (2004). Structures, processes and relational mechanisms for IT governance. Strategies for information technology governance (pp. 1–36).	167
Culnan, M. J., McHugh, P. J., & Zubillaga, J. I. (2010). How large US companies can use Twitter and other social media to gain business value. MIS Quarterly Executive, 9(4), 243-259.	81
Scandizzo, D. (2005). Risk Mapping and Key Risk Indicators in Operational Risk Management, 34(2), 231–256.	51
Van de Weerd, I., & Brinkkemper, S. (2009). Meta-Modeling for Situational Analysis and Design Methods. Handbook of Research on Modern Systems Analysis and Design Technologies and Applications (pp. 35–54). IGI Global.	47
Dutta, S. (2010). What ’s Your Personal Social Media Strategy ? Harvard Business Review, 88(11), 127–130.	37
Van Zyl, A. S. (2009). The impact of Social Networking 2.0 on organisations. The Electronic Library, 27(6).	34
Hrdinová, J., Helbig, N., & Peters, C. (2010). Designing social media policy for government: Eight essential elements. The research foundation of State University of New York.	27

McAfee, A. (2009). Shattering the myths about enterprise 2.0. IT Management Select, XIII(1), 1–6.	27
Racz, N., Weippl, E., & Seufert, A. (2010b). A frame of reference for research of integrated governance, risk and compliance (GRC). Proceedings of the 11th Joint IFIP TC6 and TC11 Conference on Communications and Multimedia Security, 106–117.	23
Back, A., & Koch, M. (2011). Broadening Participation in Knowledge Management in Enterprise 2.0. it - Information Technology, 53(3), 135–141. doi:10.1524/itit.2011.0635	12
Racz, N., Weippl, E., & Seufert, A. (2010a). A process model for integrated IT governance, risk, and compliance management. Proceedings of the Ninth Baltic Conference on Databases and Information Systems (DB&IS'10), 155–170.	12
Turban, E., Bolloju, N., & Liang, T.-P. (2011). Enterprise Social Networking: Opportunities, Adoption, and Risk Mitigation. Journal of Organizational Computing and Electronic Commerce, 21(3), 202–220. doi:10.1080/10919392.2011.590109	10
Zerfass, A., Fink, S., & Linke, A. (2011). Social Media Governance: Regulatory frameworks as drivers of success in online communications. 14th Annual International Public Relations Research Conference (pp. 1–22).	6
Molok, N. N. A., Chang, S., & Ahmad, A. (2010). Information Leakage through Online Social Networking : Opening the Doorway for Advanced Persistence Threats. Proceedings of the 8th Australian Information Security Management Conference (pp. 70–80).	5
Ohki, E., Harada, Y., Kawaguchi, S., Shiozaki, T., & Kagaua, T. (2009). Security Governance Framework. Proceedings of the first ACM workshop on Information security governance.	5
Verhoeven, P., Tench, R., Zerfass, A., Moreno, A., & Verčič, D. (2012). How European PR practitioners handle digital and social media. Public Relations Review, 38(1), 162–164.	4
Nelson, S. D., & Simek, J. W. (2011). Mitigating the Legal Risks of Using Social Media.	2
Larson, K., & Watson, R. (2011). THE VALUE OF SOCIAL MEDIA: TOWARD MEASURING SOCIAL MEDIA STRATEGIES. Thirty Second International Conference on Information Systems, Shanghai, 1–18.	1
Harris, M., & Furnell, S. (2012). Routes to security compliance: be good or be shamed? Computer Fraud & Security, 2012(12), 12–20. doi:10.1016/S1361-3723(12)70122-7	0
Katz, D., & McIntosh, L. (2013). The Board, Social Media and Regulation FD. New York Law Journal.	0
Mittal, A. (2012). Enabling Collaboration and Broad Communication Through Social Media At Workplace. IT Matters, 10(1), 15–21.	0

TABLE 22 | LIST WITH CITATIONS

9.6 *Prototype method*

Below, the prototype GRC method is presented, constructed from the separate governance, risk management and compliance methods as presented in Section 4.1. This prototype method was constructed from literature only, recommendations from practice were included after feedback from interviewees to improve this method and construct the final social media GRC method.

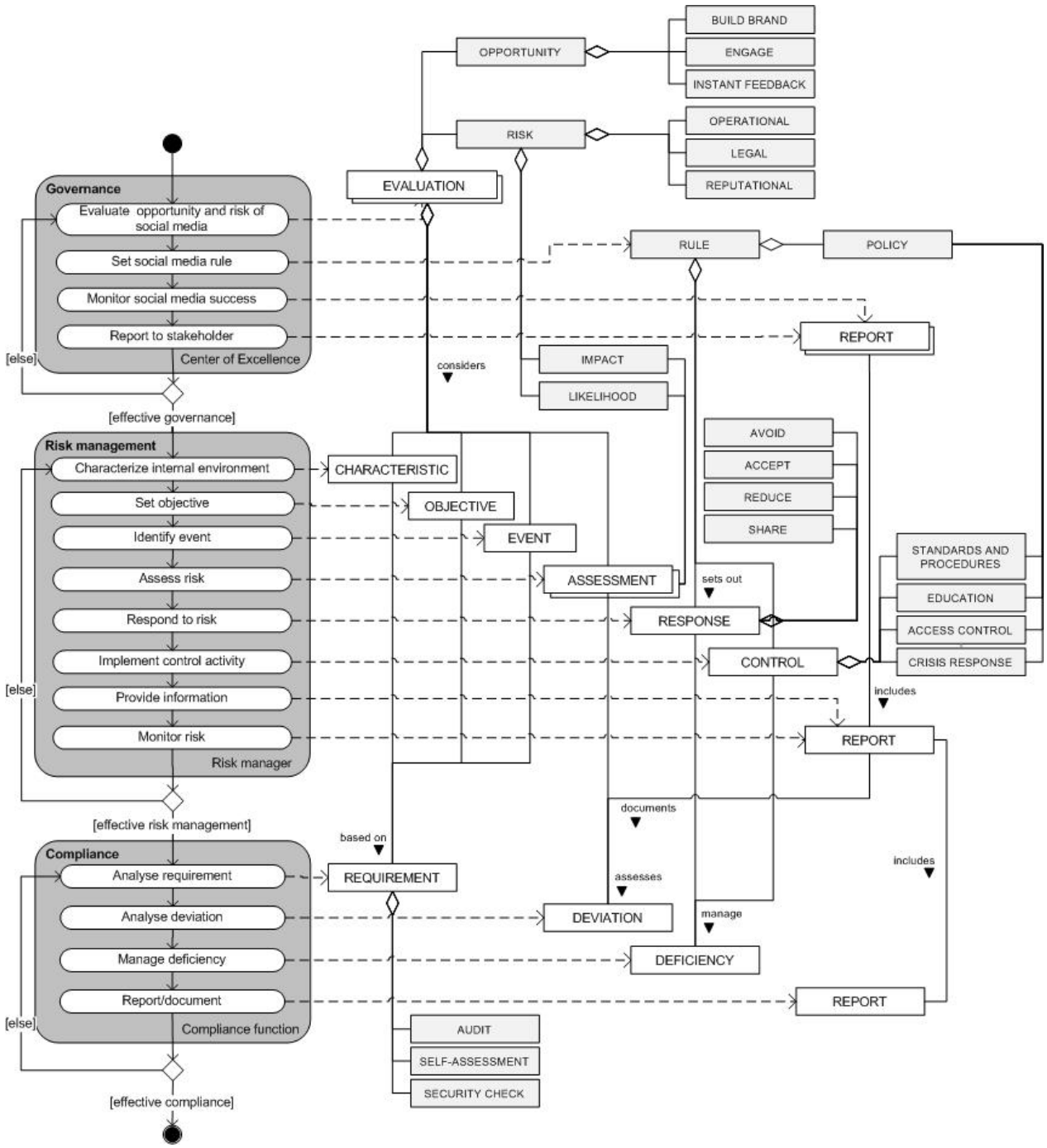


FIGURE 24 | PROTOTYPE METHOD