2014

STRATEGIES IN SECURING THE SOCIAL MEDIA

Daniel W.K. Tse
City University of Hong Kong, iswktse@cityu.edu.hk

Dennis C.K. Lee
City University of Hong Kong, dennislee3-c@my.cityu.edu.hk

House H. Gong
City University of Hong Kong, hong2-c@my.cityu.edu.hk

Puttipong M. Sae
City University of Hong Kong, psaema3-c@my.cityu.edu.hk

Jason W. Lam
City University of Hong Kong, wlam389-c@my.cityu.edu.hk

See next page for additional authors

Follow this and additional works at: http://aisel.aisnet.org/pacis2014

Recommended Citation
http://aisel.aisnet.org/pacis2014/2

This material is brought to you by the Pacific Asia Conference on Information Systems (PACIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in PACIS 2014 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.
STRATEGIES IN SECURING THE SOCIAL MEDIA

Daniel W.K. Tse, Department of Information Systems, City University of Hong Kong, Hong Kong, iswktse@cityu.edu.hk

Dennis C.K. Lee, Department of Information Systems, City University of Hong Kong, Hong Kong, dennislee3-c@my.cityu.edu.hk

House H. Gong, Department of Information Systems, City University of Hong Kong, Hong Kong, hgong2-c@my.cityu.edu.hk

Puttipong M. Sae, Department of Information Systems, City University of Hong Kong, Hong Kong, psaema3-c@my.cityu.edu.hk

Jason W. Lam, Department of Information Systems, City University of Hong Kong, Hong Kong, wlam389-c@my.cityu.edu.hk

David Z. Lu, Department of Information Systems, City University of Hong Kong, Hong Kong, zichaolu3-c@my.cityu.edu.hk

Abstract

According to the “Burson-Marsteller (2013) Check-up insight”, Social Media already became a powerful tool for enterprises across the globe, it showed that “the top 225 companies use Twitter, Facebook, YouTube, blogs and for the first time, Google+, 65% of Latin America companies are now active on at least one Social Media platform..” It’s 2010 study showed that “of the Fortune Global 100 companies, 65% have active Twitter accounts, 54% have Facebook fan pages..”. Social Media is no longer used as an option for business, but taken as a weapon for today’s business expansion. Yet, organizations are very cautious about any possible negative impact such as cyber-attack, privacy violation, damage to branding, lack of control over its content, and non-compliance to the company-policies, etc. In order not to lag behind by competitors, many enterprises are seeking ways to leverage Social Media – as a “double-edged sword”, and seek ways to avoid any business risks. Thus it is vital that a proper enterprise strategy and a risk-plan be adopted to address those risks. Through the case-study approach, this paper aims to study the possible strategies that organizations taking to manage the negative impact in Social Media, to investigate what influence their decisions in choosing the strategies and if there could be a better governance framework to address these issues.

Keywords: SMEG, Social Media, Online Social Networking, Cyber-attack, Privacy, Securing Social Media, IT Governance, Governance Model, COBIT-5, Security Threats.
1 INTRODUCTION

Social Media is considered as a great revolution of the way people communicate. Social Media sites in particular have expanded remarkably to the limit that Social Media is now considered the top activity on the internet (Qualman 2009). Until June in the year of 2013, the total number of active Facebook users has exceeded 1.11 billion (Astuti 2014), this means that if Facebook were a country, it would be the 3rd largest country in terms of population immediately after China and India! (Bahadur, et al 2012)

As the name implies, Social Media is a name given to web-based and mobile technologies that are used to turn communication into what you can call as an ‘interactive dialogue’ (Agrawal). Some people may describe Social Media as one of the Web 2.0 products, which enables interactive platform for people and organizations to communicate with each other ubiquitously.

Despite the possibilities of the Social Media benefits offered to the organizations, many organizations are not aware of the challenges and risks with its adoption. Whether or not the benefits outweighing its issues or challenges can be controversial, yet an organization without realizing the needs to govern its use may fall into the business risks or crisis, eventually it may ruin the organization branding immediately. Even it is just a slight mismanagement causing employee’s personal mistakes can damage his / her own or the organization’s reputations. For example in recent reputation crisis - the stranded Carnival Cruise: “passengers of the ship were stranded for close to a week with no running water, no air conditioning...” and the “Burger King’s lettuce stomper”. (Osterholm 2013) Thus it is vital that an appropriate Social Media Governance Model and a comprehensive Social Media policy can be adopted to address the possible incidents, crisis and associated risks.

Many senior executives around the world are considering and implementing different strategies to create business value from the use of the social media websites. Some organizations are focusing on whether to block external social media while others are proactively exploring using these social network websites for different applications such as project collaboration, recruitment, learning and development, and other business applications. Surprisingly, although threats of social media to organizations have been a worldwide phenomenon, the relevant research paper in social media governance or risk management are not available.

Therefore, the main objective of this research is to study the risks & challenges faced by organization in adopting social media in business based on the Case-Study methodology and one of the renowned IT & security / risk frameworks, to conduct a research and to propose a conceptual governance model on social media adoption.

2 LITERATURE REVIEW

2.1 Social Media Trend

With a rapid growth of using social media and new technologies in our daily life, many organizations realize the market potential and benefits of the social media. Since social media is becoming indispensable business tool, there are hundreds of millions of these tools to fulfill various needs.

Most organizations allow employees use social media for personal use during working hours “with common sense to apply” (44.8%). More than half the organizations (51.5%) allow only a few approved individuals to comment about the organization and work-related issues in social media .. this is somewhat restrictive.. More than 65% private & public sector organizations have no specific policies or guidelines in relation to social media. This study was conducted with target organizations in Australia, New Zealand, Singapore & HK who engage with social media at least to some extent as part of their business. It indicated that there is social media governance lacking or very limited in most organizations. (Macnamara 2011)

2.2 Risk & Security Governance Framework

However, there are many risks and threats associated with the social media when used as an integral part of strategy for business without governance. Many frameworks are developed to govern those IT
related activities. The most widely and popular used for the IT governance by the organization are ISO27001, COBIT 5 and SOX.

SOX (Robb 2009) - the Sarbanes-Oxley Act (SOX), which was enacted by the Federal Government in 2002, arose from the number of major corporate and accounting scandals, concerns and are mostly focused with reference of the Enron Corporation case. SOX cover the issues such as Independent Auditing Requirements, Corporate Governance Internal Control Assessment and Enhanced Financial Disclosure and it established a new and enhanced standard for all US public companies and for organizations not directed at government but had a significant impact on internal accounting controls in public agencies focusing on management of how fiscal information within the organization is created, accessed, stored, processed and transmitted within automated and manual record system.

ISO27000 (Commissum 2014) is a set of standards of Information Security Management which is widely-accepted internationally. It is mainly developed for Security and Risk Compliance. The certificate standard ISO/IEC27001 is for organization. This standard helps an organization defining a framework for managing information security more effectively and aligning with a number of other topics such as ISO 9000 and ISO 14000 (The ISO27000 Directory ). ISO27000 is followed by a plan of action to help an organization to establish a roadmap to the level of compliance which requires an organization with the short-term actions’ aim to address any higher priority risks as identified.

COBIT-5 (ISACA) - Control Objectives for Information and Related Technology (COBIT) is a framework created by ISACA for information technology (IT) management and IT governance in 1996 (COBIT ). With more than 15 years’ practical usage, ISACA published the latest version, COBIT-5, in 2012. It is the latest framework and providing an End-to-End business view of the governance of Enterprise IT so that it can help to reflect its central role of information and technology in creating value for Enterprises. COBIT-5 helps and benefits an enterprise to create an optimal value from IT by maintaining a balance between realizing the benefits and optimizing the risks level and resources required.

The COBIT-5 is more suitable for the governance of the social media among three different frameworks because COBIT-5 is a more high-level management and governance framework. It is more practical in managing resources, infrastructure, processes, responsibilities and control. However, COBIT-5 covers many areas which cannot be fully applied to the social media. Therefore, this paper will propose a more comprehensive model based on the COBIT-5 for governance of the social media.

3 CASE STUDIES

3.1 Research Cases

Due to the resources limitation, second hand data from published research articles were used. Two papers were selected, including data from five different organizations.

Four of them were from the case study of Abdul Molok, et al. (2013) about information security issues brought by Social Media. Another case organization came from the research work of Kuikka & Akkinen (2011). These case organizations were chosen because classification and protection of information was important to their business processes. The detail information of case organizations is listed in Table 1.

<table>
<thead>
<tr>
<th>Pseudonym</th>
<th>Type of Organization</th>
<th>Number of Employees</th>
<th>Informants</th>
</tr>
</thead>
<tbody>
<tr>
<td>UNI</td>
<td>University</td>
<td>4000</td>
<td>IT Director, Security Manager, Security Consultant, Security Lecturer</td>
</tr>
<tr>
<td>SB</td>
<td>Statutory Body</td>
<td>360</td>
<td>Deputy Director (Security), IT Manager, Security Manager, Social Media Manager</td>
</tr>
<tr>
<td>PSU</td>
<td>Public Service Unit</td>
<td>5000</td>
<td>IT Manager, IT Compliance Manager, Security Manager, Incident Response Manager</td>
</tr>
<tr>
<td>SC</td>
<td>Security Company</td>
<td>360</td>
<td>Research Director, Incident Response Director, Security Manager, HR Manager</td>
</tr>
<tr>
<td>Metal</td>
<td>Manufacturing Company</td>
<td>7610</td>
<td>HR Manager, Communication manager, Marketing Manager, R&amp;D Manager</td>
</tr>
</tbody>
</table>

Table 1: The List of the case Organizations and Participants

<table>
<thead>
<tr>
<th>Access Control of Social Media</th>
</tr>
</thead>
<tbody>
<tr>
<td>UNI All employees were given full access to Social Media without formal controls.</td>
</tr>
<tr>
<td>SB Employees were allowed to use Social Media but notgame, apps and chats. Full access would be allowed for working purpose.</td>
</tr>
<tr>
<td>PSU All employees were allowed to access Social Media outside office hours.</td>
</tr>
<tr>
<td>SC All employees were given full access to Social Media. Video streaming was only allowed for 15 minutes.</td>
</tr>
<tr>
<td>Metal From 2010 all white collar staff was given full access to Social Media. No notifications were given to the employees regarding this change until the summer of 2010.</td>
</tr>
</tbody>
</table>

Table 2: Access Control of Social Media
Abdul Molok, et al. (2013) interviewed employees to understand how and why work-related information would be disclosed on social media. They summarized their findings into three hypothetical scenarios and asked security managers from case organizations about their opinion of these scenarios. Kuikka & Akkinen (2011) held informal interviews with company representatives first to determine informants and research questions. Semi structured interviews and full-day workshop were used by them to get results. Both researchers reviewed policies and other company documents about social media.

### 3.2 Research Finding

From case studies, it was found out access controls of social media were different across case organizations as shown in Table 2. In general employees were allowed to use social media with some restrictions.

To manage the use of social media, case organizations had developed or were developing company policies. However the implementations of these policies were not enforced. Some case organizations used security education, training and awareness (SETA) Whitman & Mattord (2012) programs to teach employees how to properly use social media.

### 3.3 Challenges in Managing Social Media

Based on their research findings, challenges organization facing were identified and classified them into two categories; internal challenges and external challenges. Internal challenges refer to the management challenges within the company. External challenges are issues related to company image and relationships with public.

### 4 CASE ANALYSIS & COBIT-5 FRAMEWORK

It is the great interest of many organizations to utilize the social media services; on the other hand, reducing the security risks and challenges related to the adoption of the use of the social media is the main objective for many organizations. Chang and Ahmad discussed the advantages and disadvantages of commonly used means for managing social media (Abdul Molok, et al. 2010). They thought installing a computer system inside organization to monitor all traffic towards social media was costly and impractical. Organization should rely on policies and SETA. Information security policy can help...
employees understand what they cannot say on Social Media and how to handle them. It must be well-documented to suit the needs of specific organization. After the research & literature review, the conceptual model was designed, which was derived from the COBIT-5 Framework. It is proposed to help any organization to build their policies and guidelines. This model is named as the Social Media Enterprise Governance (SMEG).

4.1 Governance Structure between Organization & Vendor

Based on the proposition that the social media is facilitated under the Internet-based services, namely a Software-as-a-Service (SaaS Cloud-Model), the IT Governance Structure on the Cloud Computing (Verstraete 2011) between the Organization and Vendor can be illustrated by the Figure 1. The “Control-tendency” shift from the Organization to the Vendor from left to right, (i.e. from “green” to “red”) gradually, which indicates that the organization tends to release its control to vendor from the infrastructure foundation to the top level of application sides – where the different types of Social-Media are normally residing in the most of the right column SaaS.

4.2 Management versus Governance

To start with the explanation of the Conceptual Model for Social Media Governance, in order to have an effective security policy and governance guidelines implemented, firstly its Management and Governance should be differentiated: this is because “Management” is concerned about the daily operational activities, while “Governance” is about the long-term direction, alignment among the Social Media (as it’s the IT enabler) and the business, control and measurement. Therefore, it involves longer-term of “Value Creation” as the organization objective, which shown in Figure 2.

As the COBIT-5 is mainly designed for the IT Governance Framework, while social media is categorized as one of the IT enabling tools to facilitate by a cloud service model, with a general understanding that stakeholders are those internal departments of corporation marketing, public relation / corporate communication, or further the human resources. Therefore, social media can be one of those IT areas that COBIT-5 can be adopted to govern it. There is no specific need to purchase additional hardware or software with IT services. The basics of Goals (Quality & Security) can be the availability & accessibility of the public internet, bandwidth for the SaaS, so the data-backup and services continuity are difficult to be provided, as social media like Facebook or Twitter cannot be guaranteed with a service level agreement on availability, data-backup and/or disaster recovery, which is out of IT’s control.

4.3 Organizational Structures & Processes

Figure 3 specifies the organizational structures of enabler dimensions to its performance management, specifically the “Life Cycle” and “Good Practices” under the Enabler Dimension would be studied in details as these are the specific Practices for Processes which involves governing of the Social Media where the research is focused. Once the organization structures have been clarified with the Stakeholders, Goals, Governance Life-Cycle, and Good-practices of the
Security Policy, particularly the “red” as highlighted in the content & arrows (flow) above would be further elaborated next.

The complete set of 37 governance and management processes is shown in Figure 4. As the social media is a Software-as-a-Service, thus its governance framework can be treated as a part of the Cloud Computing for IT Governance, yet minimizing the irrelevant parts (as the application’s infra-structure & platform are out of the IT Departmental control). The following model extracts the possible processes which are relevant to the Social Media and highlighted with light-green color in Figure 4.

![COBIT-5 Process Reference Model](image)

**Figure 4: COBIT-5 Process Reference Model**

The Governance (Evaluate, Direct & Monitor) Processes consist of five areas as listed below:
- EDM01: Ensure Governance Framework settings & maintenance
- EDM02: Ensure Benefits Delivery
- EDM03: Ensure Risk Optimization
- EDM04: Ensure Resource Optimization
- EDM05: Ensure Stakeholder Transparency

With relevance on Social Media Governance, the Management Processes are grouped as below:
- MEA01: Monitor, Evaluate and Assess the Performance & Conformance
- MEA02: Monitor, Evaluate and Assess the System of Internal Control
- MEA03: Monitor, Evaluate and Assess the Compliance with External Requirements
- APO02: Align, Plan & Organize – Manage Strategy
- APO11: Align, Plan & Organize – Manage Quality
- APO12: Align, Plan & Organize – Manage Risk
- APO13: Align, Plan & Organize – Manage Security
- BAI06: Build, Acquire & Implement – Manage Changes
- BAI08: Build, Acquire & Implement – Manage Knowledge
- BAI10: Build, Acquire & Implement – Manage Configuration
- DSS01: Deliver, Service & Support – Manage Operation
- DSS02: Deliver, Service & Support – Manage Service Requests & Incidents
- DSS03: Deliver, Service & Support – Manage Problems
- DSS04: Deliver, Service & Support – Manage Continuity
5 DISCUSSION & RECOMMENDATION

As discussed previously, the social media has been emerged and become pervasive in enterprise businesses. Organization is inevitably attracted to adopt the social media for marketing, public relations, corporation communication, resources management and information sharing among customers, partners and internal employees; while exposing themselves to many risks. Based on the COBIT5 IT Governance Framework (ISACA), this chapter introduces a Conceptual Model of Social Media Enterprise Governance (SMEG), which is developed for any organization with a need to formulate its own Social Media Strategy/Policy, IT Governance and Risk Management.

5.1 Design Principles of the proposed SMEG Model

As the Social Media Enterprise Governance (SMEG) Model is originated from COBIT-5, therefore, the SMEG design principles cover the five foundation principles (4-8) of COBIT-5 (ISACA 2009) with three additional principles (1-3):

5.1.1 Versatile Approach: As this framework should not be implemented for just one particular social media tool (Facebook, Twitter or YouTube), or for just one organization (Enabler), it should be flexible enough to cater for different business (Stakeholders) needs and to meet different defined goals, or run in a life-cycle for best practices. It is versatile to cover the organization needs in terms of data security protection, quality and risk management, etc.

5.1.2 Self-Empowerment: A framework should be simple enough to let non-IT end-users understand well. This ensures that the end-user department / organization can implement the processes and refine its process life-cycle & best practices under the Social Media policy.

5.1.3 Conform to the COBIT Framework: With over 15 years of practical usage and application history of COBIT frameworks by many enterprises, COBIT current version 5 is chosen to be based for the proposed Governance Model of the Social Media. In order not to leave behind the technological and market changes by time, this proposed model shall be reviewed & re-assessed regularly to conform to the possible changes made in COBIT, not making it as a silo without matching the changing needs of the industry.

5.1.4 Meeting Stakeholder Needs: Enterprises exist to create value for their stakeholders by maintaining a balance between the realization of benefits and the optimization of risk and use of resources. COBIT-5 provides all the required processes and other enablers to support business value creation through the use of IT (Social Media is an enabling IT tool).

5.1.5 Covering the Enterprise End-to-end: COBIT-5 integrates governance of enterprise IT into enterprise governance:

- It covers all functions and processes within the enterprise; COBIT-5 does not focus only on the ‘IT function’, but treats information and related technologies as assets that need to be dealt with just like any other asset by everyone in the enterprise.
- It considers all IT-related governance and management enablers to be enterprise-wide and end-to-end, i.e., inclusive of everything and everyone, internal and external, that is relevant to governance and management of enterprise information and related IT.

5.1.6 Applying a Single, Integrated Framework: There are many IT-related standards and good practices, each providing guidance on a subset of IT activities. COBIT-5 aligns with other relevant standards and frameworks at a high level. Thus, it can serve as the overarching framework for governance and management of enterprise IT

5.1.7 Enabling a Holistic Approach: Efficient and effective governance and management of enterprise IT require a holistic approach - taking into account several interacting components. COBIT-5 defines a set of enablers to support the implementation of a comprehensive governance and management system for enterprise IT. Enablers are broadly defined as
anything that can help to achieve the objectives of the enterprise. The COBIT-5 framework defines seven categories of enablers:
- Principles, Policies and Frameworks
- Processes
- Organizational Structures
- Culture, Ethics and Behavior
- Information
- Services, Infrastructure and Applications
- People, Skills and Competencies

5.1.8 Separating Governance from Management: The COBIT-5 framework makes a clear distinction between Governance and Management, with separation of duties among the roles of governance and management.

5.2 Proposed SMEG Conceptual Model

The proposed Social Media Governance Conceptual Model (for enterprises) “Process-References” can be divided into three layers similar to COBIT-5 (ISACA/Enabling 2012). After trimming-down some irrelevant processes, the first model release consists of similar processes in COBIT-5 – with Governance and the Management perspectives. The figure 5 illustrates the Process References Model of the framework.

Figure 5: COBIT-5 based Conceptual Model of Social Media Governance

The processes at the bottom layer usually have greater impact on the daily business processes and are handled by the enabler-organization. The middle layer builds and implements the processes with sustaining records and knowledge of the processes such that the staff turnover and changing of settings would not bother the future operations. The top layer is to align, plan and organize the enabler organization goals to realize the organization benefits, with optimized resources and minimized risks.

The MEA’s three processes (shown on the rightmost column) are the Management Processes that monitor, evaluate and assess throughout the Processes for Organizational Governance of the Social Media (three layers in the middle); which are also controlled by the five Processes of Governance “Evaluate”, “Direct” and “Monitor” (EDM).

After refining the above proposed Conceptual Model of SMEG with an approach to include the governance Life-Cycle (namely Plan, Build and Deliver), within which the processes are being managed (Monitor, Evaluate & Assess), and also being governed by the enterprise Risk Committee (Evaluate, Direct & Monitor). The schematic diagram of the Conceptual Model (SMEG) with the
added Life-Cycle, Governance & Management Processes is drawn below as a full illustration of the concept.

![Diagram of SMEG Model](image)

The diagram above is a self-explanatory model, which suggests a continuous improvement approach where firstly, the current situation may not be fully-aware of the social media risks or issues, the desired state is initiated with the SMEG model with three main process groups “Plan” (Align Plan & Organize), “Build” (Build, Acquire & Implement) and “Deliver” (Deliver, Service & Support). For example, from establishing the Social Media Governance / Risk Committee (e.g. comprising the CIO, CMO, respective heads of those user-department: e.g. Marketing, Public Relations), setting up the respective user-department user groups (who need to conduct the daily Social Media activities) responsible for the processes shown in the three color triangles as shown in Figure 6. There are three main Management Processes in the Governance Model – represented by the white triangle in the center of the diagram. The five yellow arrows are pointing outwards from the triangles, meaning that they are all reporting the issues/challenges to the Governance body – probably the senior management team concerned about the Internal Control, associated risks and benefits created when adopting the social media. The major departments responsible or accountable for the processes identified above are the IT Department (covering the Systems /Network administration and Information Security staffs) and the user-department of the social media services. The central control or management of the processes represented by the “white triangle” would constantly monitor, evaluate and assess the social media user department(s), continuously improve and refine the procedures & processes – within the life-cycle.

5.3 Implementing SMEG Model

This section mainly illustrates how to derive a sounded Social Media Governance Model & policy for enterprise. In order to allow the handy adoption of the model, this section will provide the basic hints to start SMEG model implementation for any organization. Starting from going through the SMEG model on the organization’s own priorities and goals to determine the level of adoption within their organization as every enterprise has different priorities in its goal-setting; priorities may change over time by different Stakeholder organization or even the Stakeholder unit/department.
As explained in the previous Chapter, the IT Department has not much IT control of the social media services as acquired by the user-department (especially for those free social media services). Therefore, there is a limitation of the IT Governance on the social media (SaaS) – except for the “Availability” that it can be assured like the on-premises networking connection of the End-user computers, and those network upload or download from the respective (known IP address or domain) websites can be enabled or disabled. The IT Department or Information Security Manager may have control on the IP address or domain access by controlling the whitelist or blocking the malicious websites (requested by the User-department manager or the Information Security Manager…etc.).

5.3.1 Points to Ponder

There are some points to consider when implementing the SMEG model into practices:

1. IT (Social Media) Governance cannot be implemented in a big-bang approach as users need to gain their experience when learning the social media issues and the preventive measures on information leakage or malicious attack, and any other possible challenges (as stated in previous chapters).

2. A governance-aware enterprise culture is the foundation for successful implementation: It requires the support of organization-wide program like Security Education & Training Awareness (SETA).

3. Management support is a critical success factor.

4. If the above points are ready, the implementation of the governance model can start, with a standard policy derived with the compliance with this Model being rolled out to staffs, particularly the Social Media user department(s).

5.3.2 The Process Reference guide

Process identification
- Process label — The domain prefix (EDM, APO, BAI, DSS, MEA) and the process number
- Process name — A short description, indicating the main subject of the process
- Area of the process — Governance or management
- Domain name: e.g. Evaluate, Direct & Monitor
- Process description — An overview of what the process does and a high-level overview of how the process accomplishes its purpose
- Process purpose statement — A description of the overall purpose of the process
- Goals cascade information — Reference and description of the IT-related goals that are primarily supported by the process, and metrics to measure the achievement of the IT-related goals
- Process goals and metrics — A set of process goals and a limited number of example metrics
- RACI chart — A suggested assignment of level of responsibility for process practices to different roles and structures. The enterprise roles listed are shaded darker than the IT roles.
  - R(esponsible) — Who is getting the task done? This refers to the roles taking the main operational stake in fulfilling the activity listed and creating the intended outcome.
  - A(ccountable) — Who accounts for the success of the task? This assigns the overall accountability for getting the task done. Note that the role mentioned is the lowest appropriate level of accountability; accountability is broken down as far as possible. As a principle, accountability cannot be shared.
  - C(onsulted) — Who is providing input? These are key roles that provide input. Note that it is up to the accountable and responsible role(s) to obtain information from other units or external partners, too. However, inputs from the roles listed are to be considered and, if required, appropriate action has to be taken for escalation, including the information of the process owner and/or the steering committee.
  - I(nformed) — Who is receiving information? These are roles who are informed of the achievements and/or deliverables of the task. The role in ‘accountable’, of course, should
always receive appropriate information to oversee the task, as does the responsible roles for their area of interest.

- Detailed description of the process practices — For each practice:
  - Practice title and description
  - Practice inputs and outputs, with indication of origin and destination
  - Process activities, further detailing the practices
- Related guidance — References to other standards and direction to additional guidance

As an illustration, Figure 7 shows the RACI chart (ISACA/Implementing 2012) for a few activities/processes as defined with the responsibilities played by different management roles.

**RACI Chart**

<table>
<thead>
<tr>
<th>Activities</th>
<th>C</th>
<th>I</th>
<th>A/R</th>
<th>I</th>
<th>C</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link business goals to IT goals.</td>
<td>C</td>
<td>C</td>
<td>R</td>
<td>A/R</td>
<td>C</td>
</tr>
<tr>
<td>Identify critical dependencies and current performance.</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>C</td>
</tr>
<tr>
<td>Build a Social Media strategic plan.</td>
<td>A</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>C</td>
</tr>
<tr>
<td>Build Social Media tactical plans.</td>
<td>C</td>
<td>I</td>
<td>A</td>
<td>C</td>
<td>C</td>
</tr>
<tr>
<td>Analyse programme portfolios and manage project and service portfolios.</td>
<td>C</td>
<td>I</td>
<td>A</td>
<td>C</td>
<td>C</td>
</tr>
</tbody>
</table>

Figure 7: RACI Chart for the (IT) Social Media plans

Based on the generic IT Risk Framework (ISACA 2009) to manage the possible IT Risk associated with the Social Media, Figure 8 gives you the Risk Governance overview.

**Domain Goal:**

Ensure that IT risk management practices are embedded in the enterprise, enabling the enterprise to secure optimal risk-adjusted return.

**Risk Governance**

- Establish and Maintain a Common Risk View
- Make Risk-aware Business Decisions
- Integrate with IAM
- Manage Risk
- React to Events

**Risk Evaluation**

- Detect and Analyze Risk
- Maintain Risk Profiles

**Risk Response**

- Actuate Risk

**Risk Communication**

**Domain Metrics:**

- The degree to which the strategic use of IT in leveraging enterprise resources reduces overall enterprise risk
- Percentage of risk management positions filled by staff trained in critical risk management techniques (e.g., standard risk analysis techniques, crisis management, project management, skills of people [audit, etc.] to detect when something IT-related is amis

5.4 SMEG Model Process Maturity

Based on the COBIT-5 Capability Model (ISACA/Implementing 2012) format, the following Process Maturity Model (Figure 9) could enhance the process performance. The Generic Process Capability Attributes – Performance Attributes (PA) processes are grouped by Maturity Level 1 to 5 for the Process Capability assurance. The Capability Levels are (0) Incomplete Process. (1) Performed

Although there was no test done on this SMEG model since this research focused on developing of the Social Media Enterprise Governance Model conceptually, the practical nature of COBIT-5 (which SMEG model was based on), it can be justified to be applied to the real environment. Therefore, the SMEG model or this Process Capability Model is theoretically enough to be applied in real environment after testing and fine-tuned using real cases.

6 CONCLUSION

Social Media introduces a launch list of new business opportunities, together with corporate and technology risks as highlighted in the previous chapters. After reviewing a few major IT Governance frameworks, the COBIT-5 Framework was chosen as a basis to build a versatile & flexible Conceptual Model of Social Media Enterprise Governance (SMEG) framework. This framework has been specifically designed for any organization having the need to adopt the pervasive social media tools. Riding on the COBIT-5 Framework has the advantage that the numbering of the processes is in common, which means the details of each process definition, the Capability Maturity and the Implementation guidelines behind can also be referred when needed, without the need to read through the whole COBIT-5 documentations.

This framework does not provide any specific organization structure or responsibility matrix for organization to follow, which allows flexibility and full empowerment in implementation – and aligns closely with the original design principles of this SMEG model. It is preferable to use incremental approach to execute this social media model for governance. In order to ensure a smooth successful implementation of Social Media Governance and its Policy, it is vital to be supported by the senior management with a series of user & organization-wide trainings. Further research can be done in the adoption of this model with the practical cases in realizing this model within the organization, and also the quality measurement by the Capability Maturity Processes as defined in the COBIT-5.

Figure 9: Generic Process Capability Attributes
REFERENCES


