sifma

Internal Auditors Society

Internal Audit Guidelines

Social Media Risk Management

July 2015

Table of Contents

Deloitte & Touche LLP (D&T) and SIFMA's Internal Auditors Society (IAS), whose members include internal auditors from banks, broker-dealers, insurance companies, mutual funds, public accounting firms, and self-regulatory organizations associated with the securities industry, provide these audit guidelines for information purposes only. The regulatory requirements, social media risks, and controls that apply to any particular firm may vary depending on the firm's organizational structure, social media and general business activity, and other factors. D&T and IAS recommend that firms seek the advice of their own legal, accounting and/or other advisers with respect to these matters and any questions concerning the application or interpretation of accounting and auditing standards.

I. Introduction and background

I. INTRODUCTION AND BACKGROUND

A. Overview

Social media is an umbrella term for a host of sites and technology that facilitate social interaction and the sharing and creation of user-generated content, opinions and recommendations. With ever more financial institutions embracing social media, the increasing use of this platform presents behavioural, application, and technology-related risks. The social media risk landscape is vast and continuously evolving. Significant risk arises from a lack of appropriate due diligence to determine the security of a hosted or public social media offering.

Concerns around social media can be attributed to its ability to act as an accelerant to other risks. For example, social media may also exacerbate risks associated with financial disclosures in violation of Securities and Exchange Commission (SEC) rules. Other inherent social media risks include information leakage, reputational damage to brand, non-compliance with regulatory requirements, and third-party risks. In each of these risk categories, Internal Audit (IA) can play a critical and proactive role in understanding the potential risks of engaging in social business. IA can also provide directional guidance in developing controls that will mitigate risks associated with unintended consequences and assume responsibility for monitoring compliance periodically.

Risk scenario

While social media is essential and pervasive — as well as a facilitator and an avenue for achieving business objectives — this very pervasiveness makes the management of social media difficult and risky, even more so given the increased use of mobile, wireless, and web-enabled devices. Only by viewing the entire social media risk picture can organizations make informed decisions about risk mitigation. **Social media risk** refers to the potential damage or negative impact that can be incurred by an organization as a result of using these tools and technologies inside and outside the organization. Managing the risk requires a strong policy, enforcement, training, and awareness to help ensure that employees, contractors, vendors, service/sourcing providers, and customers understand the enterprise's acceptable use of social media. Preventive measures are most important. But it is also essential to identify, report, and resolve any issue or violation in a timely manner. The organization must have adequate resources in place to monitor all social media activity and report ethical issues effectively.

Brand and reputation risk

One of the preventive measures an organization should take is to develop and implement a clearly defined social media policy. Another capability that an organization should build is a crisis management plan that includes how to respond via social channels when an incident occurs. The plan should call out the types of crises that the organization could face, content that should be used in the response, tone of the message when responding to incidents, who will be involved, and the appropriate response time frames.

IA should be involved in identifying crisis events and providing guidance on the impact that each of these events may have on the organization. IA can also play a role in identifying the integration points of the social media crisis management with other crisis management plans (e.g., businesses continuity management). To support the crisis management plan, organizations should build capabilities and systems to listen and detect events on social channels that may damage their brands.

Regulatory compliance (US only)

Some regulations and guidelines that govern enterprise social media use include the following.

- Employee rights under Section 7 of the National Labor Relations Act (NLRA) must be considered when creating a social media policy or disciplining an employee for social networking activity.
- The Federal Financial Institutions Examination Council (FFIEC) mandates that financial institutions have a risk management program commensurate with the breadth of the financial institution's involvement in social media, which allows it to identify, measure, monitor, and control the risks related to this medium.
- The Gramm Leach Bliley Act (GLBA) requires information protection, monitoring for sensitive content and ensuring that such content is not sent over public channels.
- While the SEC and the Financial Industry Regulatory Authority (FINRA) oblige organizations to store records and make them accessible, public correspondence requires approval, review, supervision and retention. This is also extended to social media.
- The Payment Card Industry Data Security Standard (PCI DSS) requires organizations to make sure that cardholder data is not sent over unsecured channels
- Section 409 of Sarbanes-Oxley (SOX) requires companies to disclose material changes in their financial conditions or

operations, by updating information on your social media networking sites. It requires public companies to "disclose to the public on a rapid and current basis such additional information concerning material changes in the financial condition or operations of the [company], in plain English." "Material changes" may include, for example, events that would require a company to issue a Form 8-K or Regulation FD disclosure.

- The Jumpstart Our Business Startups Act or JOBS Act was passed to encourage funding of small businesses by easing various securities regulations. To implement the Act, the SEC adopted Rule 506(c) which states that issuers may use general solicitation and advertising, including websites, email and social media, when raising capital provided that the issuer takes reasonable steps to verify that all purchasers are accredited investors. Firms that use social media to solicit new investors for securities offering should ensure that procedures are in place to comply with the SEC's requirements for verifying accredited investor status.

Internal Audit can assist with guidance on the policies that need to be developed to help ensure that social media activities comply with current regulations. IA can also perform gap assessments of the organization's current policies and procedures against legal and regulatory requirements (e.g., FINRA, NLRA).

Information leakage

Because social media allows employees to speak to broad audiences, insufficient controls could lead to the disclosure of sensitive information, such as personal accounts, intellectual property, customer data, personally identifiable information, etc. IA may provide directional guidance on data classification methodology to help ensure that appropriate loss prevention controls are applied to data that will be shared in social channels, to avoid tarnishing brand image as well as legal consequences.

Third-party risk

For an organization outsourcing its social media activities, significant risks also arise from an inability to identify a clear end-state vision for a social media alliance or a joint venture. Organizations should put in place a risk-based vendor governance structure to define outsourcing strategy and objectives and to provide directions on vendor risk profiling (i.e., due diligence). The governance structure should also include responsibilities to monitor business partners, vendor selection criteria, Service Level Agreement (SLA) requirements, vendor behavior management, and trend analysis and validation of the SLAs with a legal cell (legal review of outsourcing contract).

Internal Auditors should confirm whether vendor selection takes place through a structured approach to identify the vendor with a social media offering that is most aligned with the organization's business strategy. While designing the audit approach for vendor selection and evaluation, some principles should be kept in mind:

- Strategic alignment – The vendor should be able to support social media-related information technology (IT) operations and key strategic initiatives; work collaboratively with all organizational units; and align with business objectives and priorities, as well as enterprise-level organization design principles.
- Performance – Organizations should monitor, measure, and communicate vendor performance; align social media metrics with Service Level Agreements (SLAs) and Operational Level Agreements (OLAs) and contractual documents; and develop tools that support continuous improvement.
- Clear roles and responsibilities – Responsibilities of the organization, vendors, key stakeholders, and their interaction points must be clearly defined. Organizations should also move decision-making authority and responsibility to those directly influencing vendor performances.
- Partner relationships – Leading practices and knowledge should be effectively captured and disseminated. An operating model for developing a partner relationship with vendors helps to ensure that functional responsibilities are shared.

Governance

Lack of governance can result in many uncoordinated and inefficient activities, which can also lead to missed opportunities for gaining competitive advantage or sustaining market leadership. The board of directors or their delegates should develop a governance framework for organizational social media and ensure that the definition, establishment, and management of the framework align with the mission, vision and values of the enterprise. The board of directors or their delegates must also ensure that this is disseminated throughout the organization which could be achieved by developing a policy regarding social media risk management. This policy should include clear statements on the following:

- The linkage of business and social media plans, defining the social media value proposition and how it should be aligned to IT and enterprise operations;
- Roles and responsibilities of the director in charge and the board of directors or equivalent organization with regard to social media risk management;
- Identification, assessment, monitoring, control, and mitigation of social media risks;
- Establishment of controls for organization's social media ecosystem; and

- Establishment of performance indicators to measure the contribution of social media to the business and the delivery of promised business value

The board of directors or their delegates should review and revise the policy in a regular and timely manner.

B. Objectives

The primary objective of these guidelines is to be used as a knowledge source for audit practitioners as they develop their audit programs to test the design and operating effectiveness of internal controls with respect to the risk of using social media. These guidelines are not designed or intended to serve as an audit program over social media risk. Specifically, the objectives of the social media audit guidelines are to:

- Provide management with a list of controls to effectively manage the enterprise's social media policies and processes;
- Determine the adequacy and effectiveness of controls relating to social media risk management; and
- Review controls over compliance with requirements of regulators such as FINRA, SEC, etc.

C. Scope

Internal Audit Scope Areas	Key Control Areas
Governance	• Guiding Principles • Board Structure and Leadership • Reputation and Stakeholder Relations • Corporate Responsibility and Sustainability (CR&S) • Risk Oversight and Supervision
Strategy and Planning	• Geopolitical, Economic, and Demand Landscape • Laws, Regulations, and Policies • Business Model and Technology Adoption Social Media Strategy • Outsourcing • Digital Crisis Management (DCM)

Ethics and Compliance	• Code of Ethics and Compliance Culture • Monitoring, Reporting, and Investigations • Corrective Action, Supervision, and Discipline • Ethics Training and Communications
Operations	• Social Media Management Team • Knowledge and Content Management • Internal and External Communication • Integrated Marketing Systems • Public Relations • Intellectual Property and Copyright/Trademark Infringement • Human Resource Management • Innovation, Research, and Development
Technology and Infrastructure	• Social Media Security, Privacy, and Data Protection • Security and Analytics Infrastructure • Identity and Access Management • Technology Contracting, Outsourcing, and Licensing • Disaster Recovery Management

II. Audit guidelines

II. AUDIT GUIDELINES

Risks to be Managed	Types of Controls to Manage Risks	Potential Audit Work Steps
A. Governance		
Guiding Principles i. Inability to set and abide by guiding principles for social media participation ii. Unclear goals for the social media program and nonalignment of guiding principles with those goals iii. Failure to consider and socialize all stakeholders while defining guiding principles	There is a social media policy along with supporting standards and processes that clearly define the goals and guiding principles around the use of social media. The organization has taken input from all relevant stakeholders (business, Information Technology, Compliance, Legal, Human Resources, etc.) while defining the guiding principles for social media usage. The organization has assessed the adequacy of the social media policy with respect to regulatory and industry guidance, and has assigned accountability for updating the policy in light of changes in such guidance or recent market events.	• Confirm that a formal social media policy is in place Determine if the organization has taken inputs from all relevant stakeholders while defining the goals and guiding principles around the use of social media • Evaluate if the social media policy generally conforms with the standards set forth in this guideline and determine that the organization periodically evaluates the adequacy of the social media policy with respect to current industry/regulatory guidance

Risks to be Managed	Types of Controls to Manage Risks	Potential Audit Work Steps
A. Governance		
Board Structure and Leadership i. Lack of appropriate tone and effective communication set by leadership with regard to social media ii. Inappropriate decision-making and delegation of authorities for social media iii. Governance structure does not match the nature, scale, complexity, and risk content of the social media activities	The organization has clearly defined and established effective communication channels among the following groups to facilitate discussion around the use of social media: a. The board and management b. Management and the rest of the organization (individual corporate functions and business units) There is a clear allocation of roles and responsibilities, management structure, reporting lines, supervision, and accountability. Senior management periodically reviews and approves the overall appropriateness and efficiency of the governance structure, including suitability of reporting lines, definition of roles and responsibilities, and adequacy of oversight.	• Understand the social media governance structure of the organization and determine if there are any gaps • Obtain and inspect documentation evidencing defined roles and responsibilities in the organization • Obtain evidence showing adequate oversight and review of the organization's governance structure

Risks to be Managed	Types of Controls to Manage Risks	Potential Audit Work Steps
A. Governance		
Reputation and Stakeholder Relations i. Failure to understand and meet shareholder expectations regarding social media ii. Failure to understand social media trends related to the organization's workforce, customers, and other stakeholders	The organization has established processes to understand social media trends related to the organization's workforce, customers, and other stakeholder risks.	• Interview appropriate personnel to understand whether a social media current state assessment was performed • Obtain the current state assessment documents and inspect them for appropriateness
Corporate Responsibility and Sustainability (CR&S) i. Failure to meet social responsibility obligations over social media Inadequate disclosure of CR&S activities on social media	The organization implemented a governance framework that aligns with its corporate and social responsibility obligations over social media, including the following: a. Incorporating social media as part of its corporate responsibility; and b. Adequate disclosure of corporate responsibility and sustainability activities on social media.	• Understanding the organization's corporate and social responsibility obligations over social media • Obtain and review governance framework to inspect that it adequately includes the corporate and social responsibility obligations over social media.

Risks to be Managed	Types of Controls to Manage Risks	Potential Audit Work Steps
A. Governance		
Risk Oversight and Supervision i. Inadequate board oversight over social media risk management activities ii. Ineffective frameworks to facilitate an organization's enterprise social media risk management process iii. Inadequate or inappropriate social media risk appetite and tolerances iv. Inadequate public disclosures	The organization's board or a designated/representative body has oversight over social media risk management activities. The organization uses an effective governance framework to facilitate the enterprise social media risk management process. For further guidance on governance framework, refer to COSO 2013 Internal Control — Integrated Framework, COSO 2013 Enterprise Risk Management — Integrated Framework, COBIT5 and ISO/IEC 38500. The organization has defined and documented processes for risk oversight and supervision of social media and includes the following: a. Social media risk appetite and tolerances b. Risk intelligent decision-making process c. Appropriate public disclosures as per laws and regulations and statutory obligations	• Interview appropriate personnel to gain an understanding if a social media risk management process is identified by the organization • Obtain information/inspect if the risk assessment process is complete • Obtain evidence showing the oversight of the risk management process • Obtain evidence of public disclosures and review for adequacy

Risks to be Managed	Types of Controls to Manage Risks	Potential Audit Work Steps
B. Strategy and Planning		
Geopolitical, Economic, and Demand Landscape i. Lack of awareness of social media norms and policies for different geographies ii. Failure to realize how industry changes and changing economic conditions can affect social media (strategy/geopolitical) iii. Failure to anticipate changing customer trends, preferences, and requirements	The organization has policies, procedures, and guidelines around privacy laws, censorship, data restrictions, cultural differences, etc., applicable for different geographies, which are designed to improve the awareness levels among its employees, contractors, business partners, and third parties The organization has adequate capability to collect and analyze data from social networking platforms on customer preferences and other requirements (e.g., cultural, geopolitical, competition and influential factors, change in currency values, privacy issues, etc.) on a periodic basis, either internally or by engaging external agencies	• Obtain and inspect the social media policy document and confirm that the policies are complete and that they cover all jurisdictions in which the organization does business • Understand whether the organization collects and analyzes data affecting the geopolitical, economic and demand landscape • If the organization engages an external organization to perform the aforementioned analytics, obtain the SLAs and analysis reports and confirm they are adequate and complete

Risks to be Managed	Types of Controls to Manage Risks	Potential Audit Work Steps
B. Strategy and Planning		
Laws, Regulations, and Policies i. Adverse legal/regulatory changes on social media ii. Noncompliance with country/jurisdiction-specific laws and regulations iii. Failure to create an actionable and effective social media policy, in line with existing laws, regulations, and business operations	The organization has a legal/regulatory cell that has an established process to continuously monitor multijurisdictional legal/regulatory changes. The legal cell also networks with geography-specific legal/regulatory authorities to stay on top of the changing compliance landscape and processes associated with dealing with discrepancies, if need be. Procedures are followed by the organization to help ensure the social media policies are actionable, provide adequate directions (i.e., technological, applicable laws, legal, statutory, regulatory and compliance requirements, etc.), and are adhered to.	• Understand whether the social media program complies with applicable legal and regulatory requirements • Understand the process relating to how social media policies are periodically reviewed and kept current, and the parties/departments responsible for doing so • Obtain and inspect the evidence of compliance

Risks to be Managed	Types of Controls to Manage Risks	Potential Audit Work Steps
B. Strategy and Planning		
Business Model and Technology Adoption i. Inability to redefine the organization's business model to incorporate social media and reliance on inappropriate assumptions ii. Ineffective choice and implementation of Web 2.0 tools in the social media strategy iii. Failure to recognize the potential of various social media technologies and advances iv. Ineffective adoption (by management or employees), usage, and inappropriate budget allocation for implemented technology	Relevant attributes, such as target marketplace, consumer behavior, demand, macroeconomics, and government policies and legislation, are considered when accommodating the social media program into the business model. There are procedures in place to ensure the right choice of Web2.0 tools are selected and implemented to enable the social media strategy and landscape. The chosen technology platform is flexible enough to accommodate evolving changes, and IT processes are strengthened enough to track, identify, and decommission obsolete social media technologies and underlying infrastructure. The organization has a process to evaluate the platform's ability to integrate with existing technology. The organization's IT budget allocations are in line with its social media strategy.	• Gain an understanding of the social media tool(s) in place and determine that the tools can be adequately integrated with the organization's existing technology infrastructure. • Obtain the documentation showing the list of applications installed/in use; if the application permits login, observe the running of application • Understand whether there is a process to identify, assess and monitor the risks of using third party social media providers, including appropriateness of oversight and governance controls. • Understand whether a budget planning activity for social media is identified by the organization, and if executive management has established a budget for social media implementation and technology

Risks to be Managed	Types of Controls to Manage Risks	Potential Audit Work Steps
B. Strategy and Planning		
Social Media Strategy i. Failure to create a social media strategy ii. Misalignment of the social media strategy with corporate strategy and industry needs iii. Inability to monitor effectiveness of the social media investments	The organization has a defined and documented social media strategy, covering the applicable landscape that aligns with corporate strategy and incorporating available technology. Procedures and guidelines are followed by the organization to calculate ROI accurately against social media efforts.	• Obtain evidence that overall strategic objectives are defined and approved • Gain understanding of the social media strategies in place and their alignment with corporate strategy • Obtain the strategy documentation and identify how the ROIs are calculated against various social media activities performed

Risks to be Managed	Types of Controls to Manage Risks	Potential Audit Work Steps
B. Strategy and Planning		
Outsourcing i. Inability to create a strategy and define objectives for outsourced social media activities ii. Failure to monitor and measure effectiveness of all outsourced activities on social media iii. Failure to monitor business monitors or perform a legal review of the outsourcing contract	The organization has a risk-based vendor governance structure in place that reports to the board of directors and is responsible for defining outsourcing strategy and objectives for social media activities. The outsourcing strategy and underlying policies provide directions on vendor risk profiling (i.e., due diligence) to monitor business partners; vendor selection criteria; Service Level Agreement (SLA) requirements based on socio economic factors, vendor behavior management, and trend analysis; validating SLAs with the legal cell; and compliance with SLA requirements for effectiveness.	• Gain an understanding of formal arrangements/service agreements with vendors and whether their social media capabilities are aligned with the organization's business and risk objectives • Obtain evidence showing governance around the evaluation of the vendors' risk profiles and its effectiveness • Obtain the audit report of the vendor and confirm if SLA requirements have been met • Interview appropriate personnel to understand whether periodic audits of vendors happen, to help ensure that vendors have met/can meet SLA requirements based on defined factors

Risks to be Managed	Types of Controls to Manage Risks	Potential Audit Work Steps
B. Strategy and Planning		
Digital Crisis Management (DCM) i. Ineffective DCM communication, training, and testing strategy via social media ii. Failure to have a DCM plan that incorporates social media	The current Business Continuity Management framework adequately covers Digital Crisis Management to address reputation risks. The social media landscape is part of existing Disaster Recovery planning, and the RTO (Recovery Time Objective) and RPO (Recovery Point Objective) are met by alternate facilities and/or infrastructure.	• Understand whether a BC/DR program related to digital/social media crises is in place, including provisions for regular and periodic testing • Inspect the oversight activities around the BC/DR program • Confirm whether BC/DR testing has been done and results documented at least annually. Confirm whether a gap analysis has been performed between the results and the social media BC/DR objectives • Confirm whether the test results were reviewed by senior management and if any action items or follow-up measures were carried out

Risks to be Managed	Types of Controls to Manage Risks	Potential Audit Work Steps
C. Ethics and Compliance		
Code of Ethics and Compliance Culture i. Failure to implement a well-structured code of ethics with regard to social media usage and train employees on the ethical and honest use of social media sites ii. Failure to monitor and control unauthorized activities on social media iii. Failure to create a sound culture in which compliance-related matters and issues regarding social media are treated with rigor and objectivity iv. Failure to provide personnel with tools and resources needed to attain ongoing compliance	There are documented rules and guidelines on ethics and basic etiquette regarding social media usage. Employees are trained and offered guidance on the code of ethics for social media usage. There is a mechanism to monitor data posted by employees on social media. The organization takes steps to enforce compliance policies and take appropriate disciplinary action.	• Obtain Rules and Guidelines documents on ethics and basic etiquette regarding social media usage and confirm whether these rules and guidelines are being followed • Confirm if the actual training requirements on the code of ethics for social media usage are met • Assess the mechanism for monitoring data posted by employees on social media and confirm whether the mechanism is being followed to monitor and control data • Assess the conflict resolution mechanism (rules of engagement) to control unexpected behavior in social media and confirm whether the procedures are being followed • Understand how the organization enforces compliance policies and applies appropriate disciplinary action and confirm whether the procedures are being followed

Risks to be Managed	Types of Controls to Manage Risks	Potential Audit Work Steps
C. Ethics and Compliance		
Monitoring, Reporting, and Investigations i. Failure to conduct routine compliance audits for social media ii. Failure to identify, report, and document key ethics-related trends iii. Lack of defined protocols to address allegations iv. Inadequate establishment of preventive and detective controls	Regular audits take place to assess compliance with established rules and guidelines pertaining to social media usage. Adequate resources are allocated to perform regular compliance monitoring and auditing. There are adequate triggers on safeguards (e.g., minimum number of "vote down" or "report abuse" tags on a post) to identify and report breach of ethics issues. There is a logging mechanism that tracks and documents all reported violations for a defined period of time or until reset. The organization has in place adequate resources to monitor social media activity and report ethical issues effectively. The reporting also includes escalating/reporting to external stakeholders if certain conditions are met/breached.	• Obtain reports on audits conducted to assess compliance with established rules and guidelines pertaining to social media usage and confirm whether audit recommendations have been implemented • Obtain reports on resources allocated to perform regular compliance monitoring and auditing and confirm whether the resources allocated for compliance activities are adequate • Obtain reports on how the organization continuously monitors ethics and compliance for social media usage and confirm whether employees are aware of this process • Obtain documentation to confirm whether triggers are used on safeguards to identify and report breach of ethics issues • Obtain procedural document to identify established escalation procedure and line of authorities to address and inquire into allegations and confirm whether the procedures are being followed • Interview authoritative body/person to confirm whether the reporting procedures are being followed

Risks to be Managed	Types of Controls to Manage Risks	Potential Audit Work Steps
C. Ethics and Compliance		
Corrective Action, Supervision, and Discipline i. Failure to correct any mistake or inappropriate content on social media promptly ii. Failure to communicate consequences of unethical behavior and noncompliance iii. Lack of accountability and measurement over the use of social media iv. Failure to establish and maintain supervisory controls v. Failure to evaluate the risk of employees making company or client references on personal social media accounts	Steps are taken by designated personnel to undo or correct noncompliant posts or behavior in social media within a defined and targeted timeframe. Penalties are in place for abuse or noncompliance of social media usage policies and procedures, and are strictly and uniformly communicated and enforced in an unbiased manner.	• Obtain procedural documentation regarding penalties in place for abuse of or noncompliance with social media usage policies and procedures and confirm whether penalties are imposed where necessary. Confirm if the social media usage policy provides guidance around the do's and don'ts of making company or client references on personal social media accounts and if disciplinary actions due to noncompliance are sufficiently mentioned in the policy. • Confirm if disciplinary actions due to non-compliance are adequately communicated to employees • Interview responsible authority to determine the action items around noncompliant posts and confirm if there has been any such instance before

Risks to be Managed	Types of Controls to Manage Risks	Potential Audit Work Steps
C. Ethics and Compliance		
Ethics Training and Communications i. Inadequate training program for ethics and compliance on social media ii. Inability to establish ongoing ethics and compliance communications for social media	Mandatory training programs are in place for employees on ethics and compliance in social media usage. There is a mechanism (such as learning credits, Continuing Professional Education hours, etc.) to track completion of said training by an employee. There is an option for employees to provide anonymous feedback and reporting, and the complaints and feedback are promptly acknowledged and acted upon by a representative authority in a time bound manner.	• Obtain reports as to whether mandatory training programs are conducted for employees on ethics and compliance in social media usage and confirm that trainings offered are complete. Also, confirm whether a mechanism to track completion of said training by an employee exists. • Obtain documents on guidelines and rules of ethics and compliance in social media usage and confirm that such guidelines and rules are adequately communicated to employees

Risks to be Managed	Types of Controls to Manage Risks	Potential Audit Work Steps
D. Operations		
Social Media Management Team **i.** Failure to hire qualified talent for managing social media **ii.** Failure to set goals and objectives for the social media management team	Minimum qualifications, skill sets, and experience are specified in hiring social media manager(s)/ administrator(s)/moderator(s) The candidates hired for the social management team are trained and briefed by the team on their goals and objectives and the organization's expectations.	• Obtain records of resources allocated for social media management and confirm whether the qualifications, skill sets, and experience requirements are met • Obtain evidence on resource training and whether briefing on goals and objectives have taken place

Risks to be Managed	Types of Controls to Manage Risks	Potential Audit Work Steps
D. Operations		
Knowledge and Content Management i. Inability to mitigate rapid or unplanned knowledge loss over social media **ii.** Inability to classify and integrate knowledge across various social media platforms **iii.** Failure to update content periodically on all social media networks	The organization has controls as a failsafe (may be a policy, performance metrics, a standard, a backup system, etc.) to mitigate unplanned loss of knowledge and information over social media. There is a knowledge management strategy governing capture, documentation, and transfer of knowledge through adequate technological support (tools, software, and database). There is a system in place to capture, classify, and integrate knowledge generated or stored across various social media platforms. There is a system (of people, procedures, and constraints) put in place to manage content mix on social media networks. There is a mechanism to help ensure that the content is regularly and consistently updated on all social media networks.	• Obtain evidence and inspect if controls are in place to mitigate unplanned loss of knowledge and information over social media • Obtain documents stating the knowledge management strategy governing knowledge capture, documentation, and transfer adopted by the organization and citing evidence to confirm whether the strategy is being effectively implemented • Obtain documentation regarding the mechanism to help ensure content is regularly and consistently updated on social media networks and confirm whether the mechanism is being effectively implemented

Risks to be Managed	Types of Controls to Manage Risks	Potential Audit Work Steps
D. Operations		
Internal and External Communications i. Failure to set objectives for social media as a part of the organization's internal communications ii. Failure to have a branding and reputation management plan for social media iii. Failure to deal with negative conversation on social media in a timely and effective manner	The organization has incorporated social media as a part of its internal communication strategy through a defined set of objectives. The organization has leveraged various organizational sites and communities for its internal communication. The organization uses Search Engine Optimization (SEO) techniques to prominently showcase and be listed at the top of major ranking engines. Adequate personnel, time, tools, and resources are invested to monitor social media coverage of the company's brand (e.g., share of voice).	• Obtain evidence to confirm whether the organization uses social media for internal communications and if the desired set of objectives is met • Obtain evidence on whether the organization uses SEO techniques to be prominently showcased and listed at the top of major ranking engines • Obtain documentation on the brand management and reputation management plans the organization deploys to ensure their presence in social media and confirm whether adequate resources are allocated

Risks to be Managed	Types of Controls to Manage Risks	Potential Audit Work Steps
D. Operations		
Integrated Marketing Systems i. Inability to integrate social media into the organization's overall marketing strategy ii. Failure to monitor, measure, and analyze the performance of the social media marketing plan iii. Failure to set clear objectives for social media research and marketing strategies	The social media plan and strategies are an integral part of the organization's overall marketing strategy, with defined Key Performance Indicators (KPIs). There are processes and procedures to monitor, measure, and analyze the performance of social media marketing plan. There is a systematic, planned, and documented methodology to conducting research in marketing decisions on the social media platform.	• Interview top management to confirm whether the social media strategy is an integral part of the overall marketing strategy and confirm whether KPIs are defined • Obtain procedural documentation to understand the process to monitor, measure, and analyze the performance of the social media marketing plan • Obtain evidence on the methodology adopted to conduct research on the social media platform and confirm whether there are no discrepancies in the implemented procedures

Risks to be Managed	Types of Controls to Manage Risks	Potential Audit Work Steps
D. Operations		
Public Relations i. Failure to be responsive on social media ii. Failure to have an active customer interaction and support mechanism on social media iii. Failure to have an effective and easy feedback mechanism for business partners, stakeholders, and customers in the social media space iv. Inability to prevent an unhappy or dissatisfied consumer from turning into an influencer through negative comments	The organization uses tools to actively listen, using feed aggregators, analytical listening dashboards, sentiment analysis software, etc., to determine what their stakeholders are saying about them on social media sites. The organization actively and responsively engages with the stakeholders (social media presents an opportunity to interact even at a one-to-one level with customers) and addresses their concerns and questions (talking to the audience). There are documented guidelines and policies on handling complaints, responding, query resolution, and escalation of the social media conversation.	• Obtain evidence to confirm the tools used to actively monitor stakeholder activity regarding the organization on social media sites • Confirm whether there is a standard response procedure to engage and respond to stakeholder concerns • Obtain documented guidelines and policies on query resolution and handling complaints on social media and confirm whether allocated resources are assigned

Risks to be Managed	Types of Controls to Manage Risks	Potential Audit Work Steps
D. Operations		
Intellectual Property and Copyright/Trademark Infringement i. Inability to prevent impersonation and trademark infringement ii. Failure to have strong policies regarding intellectual property rights in the social media policy	The organization has established, implemented, and maintained processes and controls to protect its intellectual property by: a. Preventing trade secrets from being revealed or used without consent b. Preventing employees from publishing at a third-party site without the authorization of the owner/author c. Educating employees against posting proprietary or trade secrets through social media The organization has established, implemented, and maintained processes and controls on social media usage to protect against the copyright/trademark infringement including but not limited to: a. Impersonation and trademark infringement b. Username squatting or impersonation of the organization or its employees	• Obtain policy documentation regarding the organization's social media policy to address intellectual property rights and copyright/trademark infringement and confirm against evidence if the policies are being followed • Obtain documentation to understand steps adopted to ensure protection of trade secrets and prevention of leakage • Obtain policy documentation that restricts publishing of organization data by employees on third-party sites • Obtain records to confirm whether employees are being educated against posting proprietary or trade secrets through social media Obtain evidence on how the organization deals with username squatting or impersonation of the organization or its employees and understand what actions the organization takes to rectify such activity • Determine what methodologies/tools are used by the organization to systematically detect exposure to the social media risks herein, and respond with mitigating action. Determine if such methodologies are effective in detecting potential exposures.

Risks to be Managed	Types of Controls to Manage Risks	Potential Audit Work Steps
D. Operations		
Human Resource Management i. Inappropriate use of social media for onboarding, networking, mentoring, and coaching post recruitment ii. Failure to integrate the effective use of social media as a tool in the management of HR related activities iii. Failure to establish leading practices regarding social media to improve employee productivity	There are policy and procedures in place to ensure that the HR department appropriately uses social media as a pre/onboarding, networking, mentoring and first/pre-screening tool, to engage with candidates (e.g., disclosing pay packages in public forums, using sensitive information in pre-screening exercises etc.). There are policy and procedures and leading practices guidelines in place to help ensure usage of social media does not affect employee's productivity (e.g., breaks permitting only certain time periods of online social activity).	• Obtain evidence to understand if the organization uses social media as an active medium to assess potential candidates • Obtain policy documentations to understand the guidelines and leading practices put in place to help ensure employee's productivity is not hampered by the usage of social media • Confirm whether the organization has policies in place to extend social media training to employees

Risks to be Managed	Types of Controls to Manage Risks	Potential Audit Work Steps
D. Operations		
Innovation, Research, and Development i. Insufficient use of social networking sites to build business intelligence ii. Failure to build strong policies around the use of crowd sourcing iii. Failure to use social media as a virtual platform to get opinions and polls on products and services iv. Inadequate clarity of goals and objectives for a product launch on social media	The social media platform is used as a portal for further innovation by calling for ideas, suggestions, and feedback proactively. There are well-defined and strong policies governing the use of crowd sourcing, directed at gaining new ideas, thoughts, and perspectives. The organization uses social media as a platform to conduct polls and collect opinions on products and services, track consumer's interests, and test products and services relevant to consumers' interests. Social media is a part of communication and advertising platform used during a new product launch, with clear goals and objectives.	• Obtain evidence to understand if social media platforms are used for idea generation for innovations • Obtain policy documentation to confirm there are strong policies governing use of crowd sourcing for idea and data gathering • Determine whether the organization uses social media to conduct polls, collect opinions, and test products/services • Obtain evidence of the organization's use of social media to communicate and advertise new products/services

Risks to be Managed	Types of Controls to Manage Risks	Potential Audit Work Steps
E. Technology and Infrastructure		
Disaster Recovery Management i. Inability to recover data related to social media program ii. Disruption of business communication through social media iii. Lack of standardized change management process revolving around social media	Existing Disaster Recovery Planning (DRP) program adequately covers social media platforms across geographies, and RTO and RPO objectives are met by building redundancy into critical technology platforms during implementation. Technologies/tools are adapted by the organization to monitor and resolve a social media crisis, including those that affect business communications through social media. The organization conducts frequent disaster recovery drills on social media technologies/tools to assess its ability to face a digital crisis.	• Obtain documentation to confirm whether there is a DRP program in place that adequately covers social media platforms and their respective RTOs and RPOs across geographies • Understand the technologies/tools adopted by the organization to monitor and resolve a social media crisis • Obtain records to confirm whether the organization conducts frequent disaster recovery drills on social media tools/technologies to check if the DRP program is up-to-date

Risks to be Managed	Types of Controls to Manage Risks	Potential Audit Work Steps
E. Technology and Infrastructure		
Technology Contracting, Outsourcing, and Licensing i. Improper bidding, selection, and contracting through social media ii. Poor security and privacy controls of outsourced data iii. Inability to manage multiple providers servicing different social media platforms	The organization has a standardized process for outsourcing, contracting, and bidding and selection. Adequate security and privacy controls are in place for outsourced data in the areas of cross border data transfer, data retention, breach notification & incident response management, user access management, data disclosure, monitoring etc. There are clear and documented procedures to define and communicate the scope of work and clauses in SLAs to external service providers.	• Obtain evidence to determine whether the organization has a standardized process for outsourcing, contracting, and bidding and selection and confirm this against documented records and contracts • Understand security and privacy controls put in place for outsourced data and how they are implemented • Obtain procedural documentation that defines and communicates the scope of work and clauses in SLAs to external service providers and confirm whether these clauses are communicated via contracts to external service providers • Obtain documentation on established protocols to handle and manage multiple vendors servicing different social media platforms

Risks to be Managed	Types of Controls to Manage Risks	Potential Audit Work Steps
E. Technology and Infrastructure		
Identity and Access Management i. Failure to control access to key social media initiatives ii. Failure to periodically review user access and change authorization accordingly	The organization periodically reviews user access rights and perform audits on change authorization requests. The organization has defined security levels for information based on its classification. Access provisioning is in accordance with "principle of least privilege" and based on a need to know. The organization frequently reviews security (access) violations and performs access re-certifications on a periodic basis.	• Obtain evidence on how the organization carries out periodic reviews and audits regarding user access rights and change authorization requests • Gain an understanding of defined security levels for social media classification and access • Obtain evidence as to whether the organization frequently reviews security (access) violations and performs access re-certifications on a periodic basis

Risks to be Managed	Types of Controls to Manage Risks	Potential Audit Work Steps
E. Technology and Infrastructure		
Social Media Security i. Lack of physical or logical security ii. Failure to ensure integration of security tools iii. Inability to screen applications on employees' phones iv. Failure to prevent users from introducing malware from social network sites on the corporate network	The organization has logical security controls to protect the confidentiality, integrity, and availability of information exchanged through social media. The organization frequently conducts independent infrastructure/ application security tests on the platforms supporting social media content.	• Gain an understanding of the and logical security controls that have been put in place to protect the confidentiality, integrity, and availability of information exchanged through social media • Obtain records confirming whether the organization conducts independent infrastructure/application security tests on the platforms supporting social media content on a frequent basis • Evaluate the controls in place to prevent users from downloading and installing non-company-approved applications

Risks to be Managed	Types of Controls to Manage Risks	Potential Audit Work Steps
E. Technology and Infrastructure		
Privacy and Data Protection i. Unauthorized access to personally identifiable information ii. Failure to set and enforce privacy policies across the organization iii. Failure to audit the social media provider and review its privacy policy iv. Lack of review and approval of content prior to sharing v. Failure to implement authentication controls vi. Failure to safeguard all personally identifiable information in the organization's possession	The organization has policies and procedures to prevent unauthorized disclosure and access to personally identifiable information (PII) data. The organization has a consistent information/data classification strategy that clearly identifies an information owner and is commensurate with information protection requirements. The organization has an information protection strategy encompassing security and privacy policies that are established, implemented, and maintained in accordance with appropriate laws, regulations, and leading industry practices. The organization conducts risk and privacy impact assessments to evaluate the adequacy of privacy policies, procedures, and guidelines of social media providers prior to engaging them for their services. The organization has policies and procedures to monitor or restrict access to private information on social media platforms.	• Obtain documentation to understand the policies and procedures in place to prevent unauthorized disclosure and access to PII data • Determine whether the organization has a consistent information/data classification and protection strategy. • Confirm whether there is an information owner defined in the strategy and that the strategy is commensurate with information protection requirements • Obtain policy documentation to confirm whether there are security and privacy policies established, implemented, and maintained in accordance with appropriate laws, regulations, and leading industry practices • Obtain assessment reports to confirm risk and privacy impact assessments conducted to evaluate adequacy of privacy policies and guidelines • Obtain evidence to understand policies and procedures to monitor or restrict access to private information on social media platforms

Risks to be Managed	Types of Controls to Manage Risks	Potential Audit Work Steps
E. Technology and Infrastructure		
Security and Analytics Infrastructure i. Inability to secure the organization's social media infrastructure and critical information assets from internal and external threats ii. Failure to protect the social media resources from malicious threats, unauthorized use, or unintentional or intentional misuse iii. Failure to identify the metrics that will measure and drive social media program objectives iv. Failure to have a social media dashboard to check the performance of social media on all metrics, for executive reporting and oversight	The organization has processes and controls to protect the underlying network infrastructure for social media programs, for e.g., controls around user access provisioning/de-provisioning, sensitive access, user access reviews, password configurations, logging and monitoring of all the infrastructure elements supporting the social media platforms and the various analytics platforms. The organization has safeguards to protect social media resources from malicious threats, unauthorized use, or unintentional or intentional misuse. The organization performs monitoring and reporting on KPIs using a social media dashboard.	• Gain an understanding of the processes and controls to protect the social media infrastructure and critical information assets • Obtain evidence as to whether safeguards exist to protect social media resources from malicious threats, unauthorized use, or unintentional or intentional misuse • Obtain records to confirm whether the organization periodically monitors trends and analytics regarding organization of social media initiatives • Understand the use of social media dashboards to monitor and report key metrics and performance indicators

III. Glossary

III. GLOSSARY

The definitions in this section shall apply to the terms used in the guideline. Where terms are not defined in this section or within another chapter, they shall be defined using their ordinarily accepted meanings within the context in which they are used.

Aggregator	A website or software application that amasses information from multiple sources, for example news sites, search engines, or social media
Application Programing Interface (API)	An API is a documented interface that allows one software application to interact with another application. An example of this is the Twitter API.
Backup (Data)	A process by which data, electronic or paper-based, is copied in some form so as to be available and used if the original data from which it originated is lost, destroyed or corrupted.
Blog	Blog is a word that was created from two words: "web log." Blogs are usually maintained by an individual (in this case, an employee) or an organization with regular entries of commentary, descriptions of events, or other material such as graphics or video. Entries are commonly displayed in reverse-chronological order. Blogs can enable sharing opinions and knowledge in a public forum, and then allow followers to add a comment or ask a question. Blogs can be set up to automatically display all of followers' comments, or to monitor their posts and only publish the comments or questions that may add value to the original post.
Business Continuity	The ability of an organization to provide service and support for its customers and to maintain its viability before, during, and after a business continuity event.
Business Continuity Management	A holistic management process that identifies potential impacts that threaten an organization and provides a framework for building resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value creating activities. The management of recovery or continuity in the event of a disaster. Also the management of the overall program through training, rehearsals, and reviews, to ensure the plan stay current and up to date.
Comment	A comment is a response that is often provided as an answer or reaction to a blog post or message on a social network. Comments are a primary form of two-way communication on the social web.
Content	Content is used here to describe text, pictures, video and any other meaningful material that is on the Internet.
Content Management System	A software suite with multiple functionalities, allowing for the ability to create static Web pages, blogs, wikis, document stores, etc.
Crowdsourcing	The process of obtaining needed services, ideas, or content by soliciting contributions from a large group of people, and especially from an online community

Discussion Boards	A discussion board begins with a specific topic, question, issue or problem, and then users are encouraged to contribute their perspectives, as well as comment on others' prior contributions. Discussion boards can be open to all who wish to use or limited to a select sub-group of potential users.
FFIEC	The Federal Financial Institutions Examination Council, or FFIEC, is a formal interagency body of the United States government empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions by the Board of Governors of the Federal Reserve System (FRB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC), and the Consumer Financial Protection Bureau (CFPB) and to make recommendations to promote uniformity in the supervision of financial institutions.
Forums	Also known as a message board, a forum is an online discussion site. It is the modern equivalent of a traditional bulletin board.
Information Security	The securing or safeguarding of all sensitive information, electronic or otherwise, which is owned by an organization.
Information System	An information system is a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
Micro-blogs	A micro-blog is a blog, just on a much smaller scale. Micro-blogs are frequently limited to only 140 characters to allow compatible interaction with mobile phone texting capabilities. Twitter is one of the most well-known micro-blogging services. This popularity has led social networking tools, like Facebook, to embed micro-blogging capabilities via their "status update" feature.
Online Communities	Online communities are groups of people communicating mainly through the Internet. They may simply have a shared interest to talk about or more formally learn from each other and find solutions as a Community of Practice. Online communities may use email lists or forums, where content is centralized. While communities can emerge organically, in organizations some community-building is necessary if there are specific goals to achieve.
PCI DSS	The Payment Card Industry Data Security Standard provides an actionable framework for developing a robust payment card data security process - including prevention, detection and appropriate reaction to security incidents
Personally Identifiable Information	Personally Identifiable Information (PII) is information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context such a date of birth, addresses, passport numbers etc.
Recovery Point Objective (RPO)	The point in time to which data is restored and/or systems are recovered after an outage.
Recovery Time	The period of time within which systems, applications, or functions

Objective (RTO)	must be recovered after an outage (e.g. one business day). RTO's are often used as the basis for the development of recovery strategies, and as a determinant as to whether or not to implement the recovery strategies during a disaster situation.
Risk	Potential for exposure to loss which can be determined by using either qualitative or quantitative measures.
Risk Controls	All methods of reducing the frequency and/or severity of losses including exposure avoidance, loss prevention, loss reduction, segregation of exposure units and non-insurance transfer of risk
RSS Feed	RSS Feed - RSS (Really Simple Syndication) is a family of web feed formats used to publish frequently updated content such as blogs and videos in a standardized format. Content publishers can syndicate a feed, which allows users to subscribe to the content and read it when they please, and from a location other than the website
Sarbanes-Oxley Act	The Sarbanes–Oxley Act of 2002 is a United States federal law that set new or enhanced standards for all U.S. public company boards, management and public accounting firms, to protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws, and for other purposes.
Sentiment	Sentiment is normally referred to as the attitude of user comments related to a brand online. Some social media monitoring tools measure sentiment.
Sentiment Analysis	Sentiment analysis attempts to determine the point of view or attitude of a speaker or writer. This is an important aspect in social media monitoring in order to extract the data that is truly most valuable.
Social Business	Social Media and Social Software leveraged in support of the broader needs of the organization, either together in an all-encompassing strategy where both are integrated and optimized holistically or separately when either is used in support of an organizational outcome. Social Business has increasingly become the more broadly used term referencing the strategies and tactics an organization uses to adapt to, and benefit from, a market that has been transformed by Social Media.
Social Media Monitoring	Social media monitoring is the ability to use programs that can check the web for any mentions of your organization. This can include online articles, blog posts, tweets and Facebook comments as part of the package. In addition to the monitoring they can give you charts and graphs to tell you how you are perceived by the audience.
Social Media Optimization	Social Media Optimization is a set of practices for generating publicity through social media, online communities and social networks. The focus is on driving traffic from sources other than search engines, though improved search ranking is also a benefit of successful SMO.
Social Network Analysis	Social Network Analysis is the mapping and measuring of relationships and flows between people, groups, organizations, computers or other information/knowledge processing entities. The nodes in the network are the people and groups while the links show relationships or flows between the nodes. SNA provides both a visual and a mathematical

	analysis of human relationships.
Social Networking	Social networking tools began as a way to keep in touch with friends and family. Websites like MySpace and Facebook were originally intended to help build and sustain a network with people who share your interests. Social networking has now become an important business tool. You can use it to connect with professional colleagues both inside and outside organizations.
Social Software	The software and technologies that connect people inside organizations of all sizes that optimize workforce collaboration, communication and creativity. What makes it social and more powerful is when that software provides an awareness of the connections we have, and the connections we need, to produce maximum value - and encourages those connections to be made. In many cases, it connects the organization with external social media and external social media with the organization, without regard for traditional organizational boundaries.
Vital Records	Records essential to the continued functioning or reconstitution of an organization during and after an emergency and also those records essential to protecting the legal and financial rights of that organization and of the individuals directly affected by its activities.
Web 2.0	Web 2.0 refers to the second generation of the Web, which enables people with no specialized technical knowledge to create their own websites to self-publish, create and upload audio and video files, share photos and information and complete a variety of other tasks. It is a platform for self-expression, education and advocacy that "regular people" can use on their own without having to go to an expert to do it for them in contrast to the less interactive publishing sites of Web 1.0. Some of the best-known Web 2.0 websites include Wikipedia, MySpace, Digg, Flickr and YouTube.
Web Analytics	The measurement, analysis and reporting of Web data and trends. Web analytics can be used for many purposed, including search engine optimization, market segmentation and targeting, understanding usage patterns, etc.
Wikis	A wiki is a collaborative tool that allows multiple people to contribute, read, edit and discuss online content – even at the same time. Wikis can also track the history of all prior edits and changes, as well as who made those changes, and allows for the quick undo of any incorrect or inappropriate edits. The best known wiki on the web is Wikipedia, built using contributions from volunteer authors and editors.

IV. REFERENCE / HELPFUL LINKS

FINRA Regulatory Notice 10-06 – Guidance on Blogs and Social Networking Web Sites, January 2010
(http://www.finra.org/web/groups/industry/@ip/@reg/@notice/documents/notices/p120779.pdf)

FINRA Regulatory Notice 11-39 – Guidance on Social Networking Websites and Business Communications, August 2011
(http://www.finra.org/web/groups/industry/@ip/@reg/@notice/documents/notices/p124186.pdf)

SEC Says Social Media OK for Company Announcements if Investors Are Alerted, April 2013
(http://www.sec.gov/News/PressRelease/Detail/PressRelease/1365171513574#.UmpZEvndePs)

FINRA Target Examination Letters - Spot-Check of Social Media Communications, June 2013
(http://www.finra.org/Industry/Regulation/Guidance/TargetedExaminationLetters/P282569)

FFIEC Social Media: Consumer Compliance Risk Management Guidance, January 2013
(http://www.ffiec.gov/press/Doc/FFIEC%20social%20media%20guidelines%20FR%20Notice.pdf)

FTC .com Disclosures – How to make effective disclosures in Digital advertising, March 2013
(http://www.ftc.gov/os/2013/03/130312dotcomdisclosures.pdf)