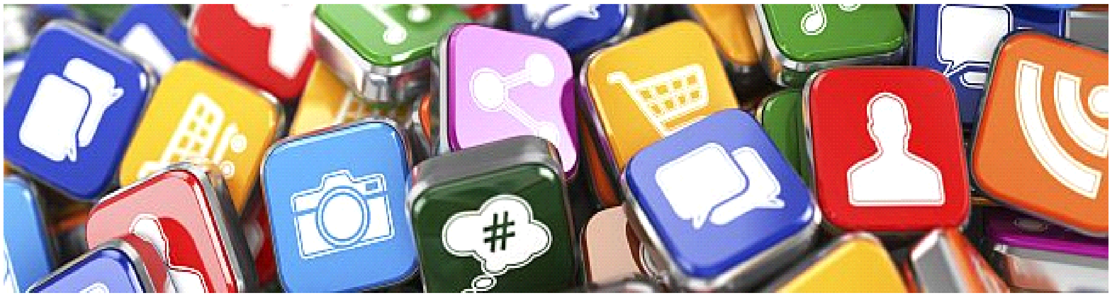
Chartered Institute of Internal Auditors

21 September 2020

Social media

Chartered Institute of Internal Auditors



The use of social media has grown substantially and it is important that organisations define their approach to its use, monitoring and interaction. All organisations, whether private or public, can have a social media presence or be discussed on social media.

Internal audit may be asked to provide assurance over existing controls or consultancy services to improve how an organisation interacts with social media.

The guide aims to provide some initial considerations and ideas to help auditors think about their role, objectives and work programmes.

What is social media?

Platforms such as Facebook, Twitter, YouTube, Instagram and LinkedIn have created online communities where people can share as much or as little personal information as they want with other members. Any website that invites you to interact with the site and with other visitors falls into the definition of social media. Have you seen the IIA's forum?

Social media is relevant not only for individuals, but business as well. It can be used as a method for business advertising as well as tracking and logging data for the benefit of a business to use.

Current trends

In January 2015 We Are Social published a compendium of global digital statistics called Digital, Social and Mobile in 2015. These statistics highlight the rapid growth and extensive use of social media. Changes over the last 12 months are shown in brackets.

1. Total population: 7.210 billion (+1.6%/+115 million)
2. Active internet users: 3.101 billion (+21%/+525 million)
3. Active social media accounts: 2.078 billion (+12%/+222 million)
4. Unique mobile users: 3.649 billion (+5%/+185 million)
5. Active mobile social accounts: 1.685 billion (+23%/+313 million)

Why is social media important to organisations?

Social media offers a number of opportunities to an organisation and can play an important part in marketing and customer engagement.

Below are some examples of strategies private and public organisations have initiated via one or more social media platforms:

1. Increased brand circulation and awareness

Paid advertising, competitions, celebrity and public endorsements via Twitter and online blogs

2. Maintaining competitive advantage

Engagement with key demographics through targeted marketing campaigns and product testing

3. Stakeholder engagement/communication

Political manifestos/campaigns, product teaser releases

4. Real time customer relationship management

Customer service, technical assistance and complaints handling

5. Recruitment

Direct and proactive recruitment through established networks and employee networks

How well an organisation manages its virtual presence and social media content has a direct impact on the public's perception of an organisation's management and reputation.

As with any public address, speech or statement an organisation should carefully consider the content, context and tone of the communication against a global audience.

Organisations also need to consider the permanency of content on the Internet. It is becoming increasingly clear that the 'internet never forgets' and even content that is thought to be deleted will be accessible in some form somewhere.

The board should develop a set of objectives surrounding its use and monitoring of social media.

These objectives will form the basis of the social media strategy and should clearly identify the current and future maturity regarding the use of social media.

It is important to note that some organisations may not need or want to strive towards full maturity, but if taking such a decision should define an approach that is aligned to the business model and competitive environment.

The law and the role of regulators

There is no specific regulation of social media within the UK and Ireland, so social media usage must be considered with the existing employment, data protection and defamation laws. Actions have been taken in relation to tweets for defamation: tweeting a menacing message resulted in criminal prosecution and the posting of photographs resulted in contempt of court.

Compliance with sales and promotional rules (eg advertising standards/broadcasting) must be adhered to along with entities listed in the UK adhering to Disclosure and Transparency Rules.

Risks

The risks associated with an organisation’s social media strategy are unique and should be identified and assessed in line with an established risk management model. However, in broad terms, the risks can often be grouped under the following headings:

Reputational risk

Social media sites are awash with comments and statements that have had negative effect on an organisation’s reputation either through direct or indirect association.

Legal or regulatory risks

Whilst no specific law governs the use of social media platforms organisations can, as with print media, be libel for slanderous or disparaging content. It is yet to be tested through the courts where, if any, distinction will be made between libel content made by individual employees and those made by their employer.

Asset security risks

It is well documented that in modern organisations the weakest point of systems and processes is the human element.

The prevalence of social media is connecting people in greater numbers, across greater distances than ever before; in this respect one of the best ways to look at social media is as a conversation in a pub with a lot of people listening and willing to share the conversation with or without your consent.

Social media is actively used by professional criminals to defraud individuals and organisations often by manipulating the social aspect to gain trust and access to confidential or sensitive information.

Potential risks and responses

1. Organisations are unaware of their social presence

- No corporate engagement.
- Unreactive/ad-hoc and inconsistent responses.
- Fragmented/best endeavours approach on local objectives.
- Lost opportunities to reach new markets and customers.

Possible impact

Loss of customers due to limited communication and engagement offered by the organisation leading to financial losses through missed sales opportunities and lack of overall competitive advantage.

Possible responses

Strategic:

- Defined organisational social media strategy and objectives in place.
- Social media risks are recorded in risk register.
- Monitoring reports are provided to senior management and the board.

Tactical:

- Regular review by senior management.
- Ownership, roles and responsibilities are clearly defined.
- Clear policies, procedures and employee expectations that are clearly communicated.
- Legal and regulatory are involved in the development of policies.
- Development of key performance indicators.
- Performance monitoring is undertaken.
- Access levels defined.
- Review processes in place prior to publication.

2. Damage to brand and reputation

- Unfavourable or confidential information released.
- Poor corporate image portrayed by employees.
- Defamation of own or competitor brand.
- The speed, spread, and impact of interactions.

Possible impact

New or loyal customers may no longer wish to be associated with the brand perceived as damaged or toxic leading to a loss of sales, loss of stakeholder confidence and depression of share prices.

Possible responses

Strategic:

- Ownership, roles and responsibilities clearly defined.
- Social media risks are recorded on risk register.
- Monitoring reports are provided to senior management and the board.

Tactical:

- Clear policies, procedures and employee expectations that are clearly communicated.
- Legal and regulatory are involved in the development of policies.
- Training schedules in place.
- Formulating and communicating clear damage limitation/response processes.
- Review processes in place prior to publication.

Operational

- Training on policies and procedures with periodic follow-up.
- Monitoring and compliance controls in place.

3. Legal, regulatory and compliance violations

- Disclosure of confidential information.
- Ramifications for non-compliance with industry regulations.
- Libel or defamatory comments.
- Copyright infringement.

Possible impact

Content may breach national or international regulation or legislation resulting in financial loss through fines and penalties.

Subsequent losses may arise due to loss of contract, sales through litigation and trade restriction.

Possible responses

Strategic:

- Social media risks are recorded on risk register.

Tactical:

- Clear policies, procedures and employee expectations that are clearly communicated.
- Legal and regulatory are involved in the development of policies.
- Training schedules in place.
- Monitoring reports are provided to senior management and the board.
- Review processes in place prior to publication.

Operational:

- Training on policies and procedures with periodic follow-up.
- Frequent review of policies to ensure inclusion of evolving legislation.
- Compliance with Advertising Standards Authority (ASA) and other standards.
- Content monitoring.

4. Social media channels and content can open up breaches of security and privacy

- Identity theft and account hijacking.
- Communication logging.
- Technical exploits.
- Information leakage.
- Third party risk.

Possible impact

Social media presence may be compromised directly or hijacked leading to erroneous and unauthorised content that result in fines, loss of trade and reputational damage.

Additional losses may be incurred through business interruption, denial of service to customer and other associated losses.

Possible responses

Strategic:

- Information security policies in place – logical access, data transmission, etc.

Tactical:

- Organisational data retention policies.
- Defined ownership, accountabilities embedded within outsourcing contracts.
- Appropriate loss transfer policies and insurances.

5. Excessive use of social media in the workplace not business related

- Employee use of company assets.
- Use of personal assets during working hours.
- Association and affiliation of employee with organisation.

Possible impact

There is an increased risk of introducing viruses and malware where own devices are not subject to screening software before accessing internal networks.

Additional losses may occur due to reduced output and productivity resulting from excessive social media use.

Possible responses

Tactical:

- Clear policies, procedures and employee expectations that are clearly communicated.

Operational:

- Restricting or monitoring network access and traffic.

The role of the internal auditor

Internal audit can play a vital role in the successful development, implementation, and operation of a social media strategy dependent on an organisations' social media maturity and level of risk management.

Consultancy

Internal audit consultancy service during the development of an organisation's strategy provides a robust and disciplined application of risk management and internal control frameworks.

The consulting relationship can facilitate the understanding of the organisation or market positions and act as a fact finding endeavour, against which structured advice and guidance can be provided.

Internal audit should ensure that where consultancy is provided to management this coverage, depth and timescale of the provision is identified and agreed prior to the commencement of the arrangement.

Assurance

Strategic, operational and tactical reviews involved with the management of established social media policies and procedures will provide independent and objective assurance over the control environment.

Internal audit assignments can be carried out as a specific review of the use of social media, in areas of higher risk (e.g. customer services/complaint handling), or as part of a wider review of an organisation's control environment.

Illustrated below, using the Institute's risk maturity model, identifies when and how consultancy and assurance might be applied by internal audit.

Risk maturity model

1. Maturity naive

The organisation is unaware of its virtual presence, the opportunities and risks. There is no consideration or monitoring of social media comments or articles

Audit involvement

Consultancy

Potential audit approaches

- Assist in risk assessments.
- Conduct 'listening audits' to understand what is being said on social media.
- Peer/competitor social media analysis.

2. Maturity aware

The organisation understands the virtual environment and the role it plays. Some effort may be made to establish limited virtual presence mainly as a defensive exercise.

Audit involvement

Consultancy

Potential audit approaches

- Peer/competitor social media analysis to determine most aligned social media platform and approach.
- Assist and challenge senior management in the development of social media presence and strategy.

3. Maturity defined

The organisation has formalised the risks and opportunities surrounding their virtual presence and their responses to these risks. Generic social media policies and procedures may exist.

Audit involvement

Assurance

Potential audit approaches

- Review social media strategy, formal policies, and compliance monitoring activities and associated management information.
- Review adequacy of risk mitigation.

4. Maturity managed

The organisation has developed mechanisms to deliver social media objectives; there is clear ownership and accountability of content.

Audit involvement

Assurance

Potential audit approaches

- Review and challenge business objectives, underlying assumptions and management information generated.
- Review effectiveness of risk mitigation.

5. Maturity embedded

The organisation participates in social media in a proactive and strategic manner. There are clear strategies for reacting to, and promoting, social media content through an established and functional governance structure.

Audit involvement

Assurance

Potential audit approaches

- Review established governance, risk management and internal controls.

- Review social media objectives against wider organisation objectives and national/international operations.

Potential internal audit approach

Strategic

An audit focussing on social media strategy should provide assurance that the primary objectives of an organisation's approach and use of social media are aligned to the organisations overall strategy and social media maturity. The following questions could be used as a starting point of a social media strategy audit:

1. Does the organisation have a full appreciation of its social media presence?
2. Is there a social media strategy with clear aims, responsibilities and accountabilities?
3. Are social media objectives defined, understood and communicated?
4. Are risks associated with our social media identified, recorded and assigned ownership?
5. Are the risks assessed with realistic mitigation to contain within defined risk appetites?
6. What governance is in place to monitor social media activities and risks?
7. Are there information security policies in place?

Tactical

Audits focussing on the tactical management of social media should provide assurance that management have designed and operate sufficient monitoring and oversight controls to mitigate risks associated with social media. The following questions could be used as a starting point of a social media tactical audit:

1. Does the organisation have a defined social media policy and procedures?
2. Is there adequate training and development to support the policy and procedures?
3. What involvement does the legal/regulation function have in policy development?
4. Who is accountable for the social media policy, platform content and usage?
5. What mechanisms have been developed to respond to social media content?
6. Who can use the official social media platforms?
7. How is content and usage monitored and how often?
8. What key performance indicators have been developed and how are these used?
9. How is performance reported to senior managers and the board?

10. How are emerging issues and risks captured, assessed and responded to?

Operational

The focus of an operational audit should encompass the more day to day activities present in the management of an organisation’s social media presence. The following questions could be used as a starting point of a social media operational audit:

1. Who has access to the social media platforms and at what level?
2. What monitoring of social media platforms is undertaken to identify content relevant to the organisation?
3. Is there a defined engagement, response and escalation process for each platform or collectively?
4. What review processes are in place to review content prior to publication?
5. How do you ensure consistency of response to individual stakeholders and across platforms?
6. What types of training is provided to employees with access to the institution's social media platforms?
7. How do you know training is effective?

Testing

As a starting point here is a list of areas below to consider, this is by no means an exhaustive list but can used as a starting point to consider potential tests to undertake.

Strategic

Assessment of:

- Social Media maturity.
- Social media strategy including risk appetite and whether there are defined metrics against which progress is measured.
- The organisation and internal culture.

Tactical

Governance:

- That policies and procedures are consistent with objectives.
- How roles and responsibilities are assigned/rescinded.
- How risks are assessed and recorded.
- What monitoring and compliance controls are in place including integrity and fairness to consumers?
- Information disclosure policies and application.
- Data strategy, retention period, format, access, etc.

Assessment of:

- Training materials and application.
- The completeness of the organisation's register of laws and regulations applicable to social media activities.
- Conversation tone and content.
- Listening (what is being said).
- Third party tools and software and/or contracts are evaluated for operational and compliance impacts

Operational

Process including:

- Review and approval of content before publication.
- How the board/executive management stay informed of actual and proposed social media activities.
- Evaluate whether management distinguishes consumer complaints received through social media platforms from social media incidents.
- Information security reviews and data logs.
- Information classification e.g. public, confidential, internal.
- Incident management responsibilities and procedures.
- Complaint and incident situations that require escalation to legal, compliance, senior management, etc.

Take a course in social media

Explore the risks and opportunities of social media with our dedicated course on the subject. This course is open to all and presented by professional trainer, Stephen Maycock CFIIA CRMA.