Digital risks and the role of internal audit
The digital enterprise

Khalid Wasti, Director
Geoffrey Kovesdy, Senior Manager

Deloitte & Touche LLP
Digital risks

Corporate data and information are a vital enterprise asset that must be stored and protected.
Digital risks (cont.)

Are we in the cloud?
Where is our data and how do our employees, customers and vendors access it?

Convergence

Data Analytics

Social

Cyber

Cloud

Mobile
The emergence of cloud computing is a major permanent change to the information services market, is central to the evolution and transformation of IT services

- Cloud computing represents a major change in information technology architecture, sourcing and services delivery, by giving business on-demand access to elastic, shared computing capabilities.
- Cloud Computing is changing in how business purchase, deploy, and support IT services, and offers significant opportunities to expand and enhance their services to customers.
- Ongoing IT industry disruptions will result from the deployment of cloud computing as an alternate sources of supply for products and services.
- For enterprises in the information services business — as well as IT vendors, services providers, and their suppliers — cloud computing is the new basis of competition.
- Cloud Computing is a disruptive force comparable to emergence client/server architectures 25 years ago. Enterprises must act to manage risks and taking advantage of emerging services.
- Businesses that cannot establish a position in the market by leveraging cloud computing, may face increasing competitive pressure from challengers.

Enterprises that adopt cloud computing delivery models have the potential to fundamentally re-shape the broader business landscape.
### Representative cloud computing security risks

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Availability</strong></td>
<td><strong>Service Availability and Recoverability</strong>&lt;br&gt;• Cloud provider may not be able to match in-house IT service availability, recovery time objectives (RTO), and recovery point objectives (RPO)&lt;br&gt;• Over-Subscription Risk&lt;br&gt;• In the event of a disaster, other customers may receive higher priority in recovery activities&lt;br&gt;• As cloud providers shift from investment mode to capture market share to cost cutting mode to reach profitability, capacity may become constrained</td>
</tr>
<tr>
<td><strong>Privacy</strong></td>
<td><strong>Legal Uncertainties</strong>&lt;br&gt;• Multiple jurisdictions increase regulatory complexity&lt;br&gt;• Data sharing agreements may be required before moving data to the cloud&lt;br&gt;• Business associate agreements (HIPAA)&lt;br&gt;• Data controllers and third parties (EU DPD) Breach/Disclosure&lt;br&gt;• Centralized data stores are especially prone to security breaches&lt;br&gt;• Timely discovery and reporting of the breach by the cloud provider may be challenging</td>
</tr>
<tr>
<td><strong>Authentication</strong></td>
<td><strong>Federated Authentication</strong>&lt;br&gt;Organizations implement single sign on applications used by multiple business partners but the SSO also grants access to sensitive internal information due to authentication mashups.</td>
</tr>
<tr>
<td><strong>Operational Security</strong></td>
<td><strong>Key Management</strong>&lt;br&gt;Any activity related to key generation, exchange, storage, safeguarding, use, vetting, and replacement that results in disclosure will provide access to infrastructure and data.</td>
</tr>
<tr>
<td></td>
<td><strong>Vulnerability Management</strong>&lt;br&gt;One vulnerability has the potential to expose large number of corporations critical assets.</td>
</tr>
<tr>
<td></td>
<td><strong>Asset Management</strong>&lt;br&gt;Assets in the cloud are not properly managed and could leak critical company information or cause data exposures.</td>
</tr>
<tr>
<td></td>
<td><strong>Incident Response</strong>&lt;br&gt;Ownership, responsibilities, and actions during incident response are not defined.</td>
</tr>
</tbody>
</table>
# Cloud computing risk assessment approach

<table>
<thead>
<tr>
<th>Phase</th>
<th>Activities</th>
<th>Key Activities</th>
<th>Deliverables</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Phase I: Planning and scoping</strong></td>
<td><strong>Activities:</strong> • Identify key internal and external stakeholders: Marketing, Product Development, IT, Compliance, Legal, Risk, etc. • Obtain relevant documents, strategy, policies, governance structure, etc. • Identify areas of focus and understand the Cloud deployment and delivery services • Develop a project plan and time table including program piloting strategy</td>
<td><strong>Activities:</strong> • Leverage multiple authoritative risk sources, including Deloitte’s Cloud Risk Intelligence Map to derive a base set of cloud risk statements • Determine the control ownership based on the Cloud deployment model and delivery services</td>
<td><strong>Milestone:</strong> • Project Plan <strong>Deliverable:</strong> • Final report on recommendations and findings</td>
</tr>
<tr>
<td><strong>Phase II: Develop customized integrated risk &amp; control framework</strong></td>
<td><strong>Activities:</strong> • Asses existing relevant security policies, strategies, governance for both internal and external stakeholders to understand “current state” • Applied client’s impact/likelihood scale to risk statements • Evaluated existing controls to identify gaps within the “current state” • Validate gaps with relevant stakeholders</td>
<td><strong>Activities:</strong> • Prioritized risks based on impact, risk tolerance, and if there are risks that can be accepted by the customer • Discussed with the stakeholders to help them identify viable risk mitigation solution acceptable by both consumer and provider</td>
<td><strong>Milestone:</strong> • Customized Integrated Risk framework <strong>Milestone:</strong> • Cloud Computing Risk Heat Map <strong>Milestone:</strong> • Risk Remediation plan</td>
</tr>
<tr>
<td><strong>Phase III: Perform risk assessment</strong></td>
<td><strong>Activities:</strong></td>
<td><strong>Activities:</strong></td>
<td><strong>Activities:</strong></td>
</tr>
<tr>
<td><strong>Phase IV: Perform risk mitigation</strong></td>
<td><strong>Activities:</strong></td>
<td><strong>Activities:</strong></td>
<td><strong>Activities:</strong></td>
</tr>
<tr>
<td><strong>Phase V: Collaboration and reporting</strong></td>
<td><strong>Activities:</strong></td>
<td><strong>Activities:</strong></td>
<td><strong>Activities:</strong></td>
</tr>
</tbody>
</table>

**Cloud computing risk assessment approach diagram**
Digital risks (cont.)

Cyber
Are we prepared for attacks?
What data is at risk?

Social

Data Analytics

Mobile

Cloud
Are we in the cloud?
Where is our data and how do our employees, customers and vendors access it?

Convergence
## Cyber security capabilities assessment/risk analysis

<table>
<thead>
<tr>
<th>Objectives</th>
<th>Activities</th>
<th>Deliverables</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assess Company’s current Cyber Security capabilities at a high level</td>
<td>• Review Company’s existing documentation relating to Cyber Security</td>
<td>Results and observations from the capabilities assessment, including:</td>
</tr>
<tr>
<td>against Deloitte’s Cyber Security Capabilities Framework, the</td>
<td>capability domains</td>
<td>• An overall snapshot of Company’s current state in the identified</td>
</tr>
<tr>
<td>effectiveness of how these capabilities are deployed, and identify</td>
<td>• Conduct targeted interviews with Cyber Security domain subject</td>
<td>capability areas</td>
</tr>
<tr>
<td>gaps in coverage and associated cyber risks</td>
<td>matter specialists</td>
<td>• Identification of relevant cyber security risks and potential options</td>
</tr>
<tr>
<td></td>
<td>• Drafting and review of a capabilities report</td>
<td>for further diagnostics/deep dives</td>
</tr>
</tbody>
</table>
Cyber security capabilities assessment

Deloitte’s Cyber Security Capability Framework accelerates the assessment of cyber security controls and program maturity.

The framework assess the capabilities of people, processes, and technology across 12 cyber security domains:
Cyber security capability domains

<table>
<thead>
<tr>
<th></th>
<th>Capability</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td><strong>Emerging Threat Research</strong></td>
</tr>
<tr>
<td></td>
<td>Capabilities to improve the organization’s knowledge of the existing and emerging threat landscape associated with the nature of the business to provide an advanced capability to, not only detect potential threats against the organization, but to also begin to predict those threats based on external and internal changes.</td>
</tr>
<tr>
<td>2.</td>
<td><strong>Brand Protection</strong></td>
</tr>
<tr>
<td></td>
<td>Capabilities to protect the organization’s online brand by proactive monitoring and detection of brand and reputation attacks.</td>
</tr>
<tr>
<td>3.</td>
<td><strong>Online Fraud Protection</strong></td>
</tr>
<tr>
<td></td>
<td>Capabilities to combat online fraud in areas related to log visibility, correlation, enrichment, and external threat intelligence, including the leveraging of multiple sources of intelligence, derived from both internal and Internet-based sources, to transform data-sets associated with application transactions, customer interactions, and member behavior, into actionable intelligence capable of proactively reducing losses incurred from online fraud schemes.</td>
</tr>
<tr>
<td>4.</td>
<td><strong>Insider Threat Protection</strong></td>
</tr>
<tr>
<td></td>
<td>Capabilities to detect the presence of malicious insiders from a network, host, and/or application perspective and utilize this information to proactively protect the enterprise from malicious activity.</td>
</tr>
<tr>
<td>5.</td>
<td><strong>Penetration Testing</strong></td>
</tr>
<tr>
<td></td>
<td>Capabilities to perform penetration assessments of networks, systems, and applications, and the use of collected information to understand an adapt to the organization’s current and emerging threat environment and its exposure to accompanying risks.</td>
</tr>
<tr>
<td>6.</td>
<td><strong>Vulnerability Management</strong></td>
</tr>
<tr>
<td></td>
<td>Capabilities to provide regular, accurate, and broad coverage visibility into the current vulnerability state of an organization, and the use of this vulnerability data as a foundational element of other cyber security domains.</td>
</tr>
</tbody>
</table>
## Cyber security capability domains

<table>
<thead>
<tr>
<th></th>
<th>Capability Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td><strong>Patch Management</strong>&lt;br&gt;Capabilities to deliver patches on schedule, provide a validation checkpoint for the patching level of the environment, provide an inventory of a given system as it pertains to threats and vulnerabilities against it, and provide measurable patching metrics.</td>
</tr>
<tr>
<td>8</td>
<td><strong>Network and Malware Forensics</strong>&lt;br&gt;Capabilities to both reactively and proactively discovery details related to events regarding attack types, methodologies, and behavior, and apply this data to both signature based control systems as well as predictive systems capable of providing information that can be used to preempt cyber-criminal attacks.</td>
</tr>
<tr>
<td>9</td>
<td><strong>Incident Response</strong>&lt;br&gt;Capabilities for the tracking, response, measurement, and metrics collection of security incidents across the organization’s enterprise</td>
</tr>
<tr>
<td>10</td>
<td><strong>Log Collection and Analysis</strong>&lt;br&gt;Capabilities to proactively seek out gaps in data collection coverage, identify opportunities for improvement regarding what logging data provides, and optimize the technologies used to generate, collect, and correlate log event data and analysis.</td>
</tr>
<tr>
<td>11</td>
<td><strong>Cyber Threat Modeling</strong>&lt;br&gt;Capabilities to evolve controls, process, skill sets, and deployed technologies from a reactive posture to a predictive one by leveraging collected log data to locate threats, map information related to threats to likelihood and risk, update incident response plans, and optimize deployed technology controls.</td>
</tr>
<tr>
<td>12</td>
<td><strong>Solution Research and Development</strong>&lt;br&gt;Capabilities to evolve security controls in an effort to stay ahead of emerging threats, cyber-criminal techniques and behavior, and new technology acquisitions and business partner relationships.</td>
</tr>
</tbody>
</table>
We will assess at a high-level the company’s current state Cyber Security capabilities, including for the people, process, and technology areas. Risks will be identified for the company based on gaps in these capabilities.

### Illustative deliverables

<table>
<thead>
<tr>
<th>Area</th>
<th>Findings</th>
<th>Ref.</th>
<th>Recommendations</th>
<th>Ref.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>People</strong></td>
<td>The organization has some resources within the ISOC that can conduct penetration testing, but not on a routine basis due to operational constraints and multiple roles that those resources are fulfilling</td>
<td>2.6.4</td>
<td>The organization may find it of more value and cost benefit to utilize current resources to conduct internal penetration testing on a routine and dedicated basis since they do have individuals with the necessary skills to perform this duty.</td>
<td>2.6.4</td>
</tr>
<tr>
<td><strong>Process</strong></td>
<td>The organization has limited capability to conduct penetration testing in a staged environment or against new and emerging threats</td>
<td>2.6.5</td>
<td>The organization should expand its penetration testing capability to include more advance testing, more advanced social engineering, and develop greater control over the frequency of testing</td>
<td>2.6.5</td>
</tr>
<tr>
<td><strong>Technology</strong></td>
<td>The organization lacks standard tools to perform its own ad-hoc and on-the-spot penetration tests to confirm or support potential vulnerability assessment alerts and/or incident investigation findings.</td>
<td>2.6.6</td>
<td>Either through agreement with a 3rd Party Vendor, or through technology acquisition, develop the technology capability to perform out of cycle penetration testing.</td>
<td>2.6.6</td>
</tr>
</tbody>
</table>

#### Capability assessment scorecard

<table>
<thead>
<tr>
<th>Cyber Threat Intelligence Capabilities</th>
<th>People</th>
<th>Process</th>
<th>Technology</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber Threat Intelligence Gathering</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Emerging Threat Research</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Brand Protection Services</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Online Fraud Protection</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Insider Threat Detection</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Penetration Testing</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vulnerability Management</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Patch Management</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network &amp; Malware Forensics</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Incident Response</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Log Collection and Analysis</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cyber Threat Modeling</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Solution Research &amp; Development</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**KEY:** Mature = ●; Emerging = ○; Basic = □; None = □
Digital risks (cont.)

Cyber
Are we prepared for attacks? What data is at risk?

Social

Data Analytics

Mobile
Do we know what tools are accessing our data? Can we keep up with the changing devices?

Cloud
Are we in the cloud? Where is our data and how do our employees, customers and vendors access it?

Convergence
Overview

Mobile devices, including smart phones, tablets, e-readers, etc. have penetrated almost every facet of our lives. Mobile technologies have advanced to the point where individuals and organizations can finally take advantage of everything mobility has to offer.

• Employees, especially senior executives, are demanding greater choice, flexibility and capabilities as they rapidly adopt and extend their use of smart phones and tablets, and increasingly leverage these devices in their day-to-day work and personal lives
• Application enhancements extend the desktop to handheld devices and deliver more powerful tools to employees, potentially increasing productivity and improving bottom line performance
• Companies are looking to take advantage of mobile technologies to extend their current online business models, open up new channels, expand their reach into new and existing markets and create tighter partner and customer relationships

Mobile devices are valuable from a business perspective as they offer portability, usability and connectivity to the internet and corporate infrastructure, but they also present significant risk.
## Representative mobile security risks

The new mobile ecosystem is quite different than traditional computing. As employees increasingly use mobile devices to access critical corporate data and systems, risks have been introduced at the device, infrastructure and application levels:

| Operational Risks | • Existing security management solutions and processes may not scale or function when applied to mobile devices  
|                   | • Deployment control resides largely with the platform vendor, hardware manufacturer and carrier — upgrading the OS and patching applications may be outside the control of IT  
| Legal & Regulatory Risks | • Potential privacy issues due to personnel activity, device use, data exposure, etc.  
|                         | • Ethical and legal questions around monitoring, device wiping, securing devices and data upon employee termination for “bring your own” mobile devices  
|                         | • Regulatory requirements regarding e-discovery, monitoring, data archiving need to be considered  
| Technology & Data Protection Risks | • Due to their small size and regular use outside of the organization, mobile devices are more likely to be lost or stolen potentially leading to unauthorized access to sensitive information stored on the device.  
|                                      | • Applications are proliferating at astonishing rates; trust models and secure SDLC capabilities are not keeping pace.  
| Infrastructure & Device Risks | • Malware targeting mobile devices is rapidly maturing and increasing in volume. Additionally, mobile devices may provide an avenue of attack into the enterprise.  
|                              | • Users may be able to bypass corporate security controls, further weakening the security posture of the device and subjecting the company to increased risk. |
Our approach - assessment framework

We have identified seven (7) key security domains that will be factored in as part of our overall approach and we will use these key domains as our underlying framework when developing the audit program for mobile technology.

Mobile Application Security
- Secure development and security assessment/testing of enterprise mobile applications
- Secure delivery and management of enterprise-developed mobile applications
- Third party mobile application security requirements

Data Protection
- Permissible data storage (as defined by acceptable use policy)
- Encryption policies and controls
- Secure data transmission
- Separation of enterprise and personal data

Corporate Wireless Access
- Wireless network access policy for devices
- Access monitoring
- Authentication controls

Mobile Program Governance
- Mobile strategy
- Roles and responsibilities for mobile operations and security
- Mobile security policy and compliance
- Mobile use/acceptable use policy and compliance

Mobile Device Security & Configuration
- Device provisioning, tracking/inventory and decommissioning
- Secure device configuration requirements and standards (i.e. password requirements, remote lock/wipe, etc.)
- Device Patch management
- Anti-malware/Mobile OS Security

Mobile Infrastructure Security
- Mobile infrastructure architecture
- Mobile authentication/authorization architecture
- Logging and monitoring within mobility infrastructure

Incident Response
- Process and procedures for triaging, reporting and responding to incidents related to lost devices and/or stolen content
- Secure removal (‘wipe’)
## Representative mobile security audit scope

<table>
<thead>
<tr>
<th>Audit scope areas</th>
<th>Example key control areas</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobile Program Governance</td>
<td>• Mobile strategy</td>
</tr>
<tr>
<td></td>
<td>• Roles and responsibilities for mobile operations and security</td>
</tr>
<tr>
<td></td>
<td>• Mobile use/acceptable use policy</td>
</tr>
<tr>
<td>Mobile Device Security &amp;</td>
<td>• Device provisioning, tracking/inventory and decommissioning</td>
</tr>
<tr>
<td>Configuration</td>
<td>• Secure configuration requirements and standards</td>
</tr>
<tr>
<td></td>
<td>• Patch management</td>
</tr>
<tr>
<td></td>
<td>• Anti-virus/Anti-malware/Mobile OS Security</td>
</tr>
<tr>
<td>Mobile Infrastructure Security</td>
<td>• Mobile infrastructure architecture</td>
</tr>
<tr>
<td></td>
<td>• Mobile device configuration policy management</td>
</tr>
<tr>
<td>Mobile Application Security</td>
<td>• Third party mobile application security requirements</td>
</tr>
<tr>
<td></td>
<td>• Secure development of enterprise mobile applications</td>
</tr>
<tr>
<td></td>
<td>• Vulnerability assessment and penetration testing</td>
</tr>
<tr>
<td></td>
<td>• Secure delivery and installation of enterprise-developed mobile applications</td>
</tr>
<tr>
<td>Data Protection</td>
<td>• Permissible data storage (as defined by acceptable use policy)</td>
</tr>
<tr>
<td></td>
<td>• Encryption policies and controls</td>
</tr>
<tr>
<td></td>
<td>• Secure data transmission</td>
</tr>
<tr>
<td>Corporate Wireless Access</td>
<td>• Wireless network access policy</td>
</tr>
<tr>
<td></td>
<td>• Access monitoring</td>
</tr>
<tr>
<td></td>
<td>• Authentication controls</td>
</tr>
<tr>
<td>Incident Response</td>
<td>• Logging and monitoring within mobility infrastructure</td>
</tr>
<tr>
<td></td>
<td>• Process and procedures for reporting lost mobile devices</td>
</tr>
<tr>
<td></td>
<td>• Process and procedures for responding to a lost mobile device</td>
</tr>
<tr>
<td></td>
<td>• Secure removal (‘wipe’) of enterprise data and applications</td>
</tr>
</tbody>
</table>
Digital risks (cont.)

Social
Are we protecting our reputation? Do we know what is being said?

Cyber
Are we prepared for attacks? What data is at risk?

Data Analytics

Cloud
Are we in the cloud? Where is our data and how do our employees, customers and vendors access it?

Convergence

Mobile
Do we know what tools are accessing our data? Can we keep up with the changing devices?

Analytics

Social

How are organizations using social business to support their adoption of social media?

**Sales**
- Keeping close tabs on competitive offerings and vulnerabilities to emphasize their edge

**Service**
- Proactively managing issues while crowdsourcing issue resolution and escalation to quickly solve high priority issues

**Marketing**
- Using social data to engage their customers to share messaging and track the social sentiment

**Human Resource Management**
- Using social media to interactively engage job seekers to attract top talent, while supporting existing employees with peer-to-peer HR support

**Supply Chain**
- Engaging suppliers and contract manufacturers around priorities, exceptions, and “fire-drills”.

**Product Development**
- Dynamically developing and enhancing products gathering feedback from customers and employees
Social media

Representative Benefits

1. Generate Prospects and Leads (Sales)
   - Decrease time to market for new products
   - Increase marketing effectiveness
   - Develop new revenue opportunities
   - Leverage "interest" based marketing & advertising

2. Decrease Costs
   - Decrease R&D costs for new products by listening to your customers (and prospects)
   - Focus on inexpensive social media tools instead of using the traditional expensive marketing channels
   - Decrease customer support costs

3. Increase Loyalty
   - Increase customer insights and intelligence ("Voice of Customer")
   - Improve customer experience responsiveness
   - Improve customer education, expertise and service
   - Direct contact with the customer instead of indirect through the retail channels

4. Manage Brand Reputation
   - Increase brand awareness through social media
   - Protect brand and manage reputation
   - Benefit from spontaneous reactions from the community by connecting like-minded peers

Representative Challenges

1. Loss of Control
   - The voice of the customer is amplified
   - Companies no longer control the message or topic
   - Messages might include negative publicity

2. Inconsistent message
   - When engaging several employees in the social media world, their messages and responses may not be consistent and aligned with the strategy of the company

3. Confidential Information
   - The use of social media sites enables users to circumvent company controls, opening up the potential to violate communication policies
   - Education and training for employees is a component to managing loss of information

4. Productivity loss
   - Social media drives collaboration among co-workers but can also be a major distraction in the workplace
# Social media: Risks

<table>
<thead>
<tr>
<th>Potential risks</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Legal and regulatory compliance</strong></td>
</tr>
<tr>
<td>• Disclosure of confidential data (e.g., Personal Health Information, Personally Identifiable Information)</td>
</tr>
<tr>
<td>• Violation of copyright laws</td>
</tr>
<tr>
<td>• Protection of intellectual property rights, patents, and trademarks</td>
</tr>
<tr>
<td>• Regulatory noncompliance</td>
</tr>
<tr>
<td><strong>Security and privacy</strong></td>
</tr>
<tr>
<td>• Identity theft and social engineering</td>
</tr>
<tr>
<td>• Technical exploits: Malware, viruses/worms, Flash vulnerabilities, and XML injection</td>
</tr>
<tr>
<td>• Insufficient monitoring capabilities</td>
</tr>
<tr>
<td>• Data leakage</td>
</tr>
<tr>
<td><strong>Brand and reputation damage</strong></td>
</tr>
<tr>
<td>• Bad press</td>
</tr>
<tr>
<td>• Defamation, unfavorable or untrue posts</td>
</tr>
<tr>
<td>• Copyright infringement</td>
</tr>
<tr>
<td>• Insufficient monitoring and listening capabilities</td>
</tr>
<tr>
<td><strong>Social governance and strategy</strong></td>
</tr>
<tr>
<td>• Lack of policy</td>
</tr>
<tr>
<td>• Lack of risk oversight</td>
</tr>
<tr>
<td>• Misalignment of social strategy with strategic vision</td>
</tr>
<tr>
<td><strong>Employees</strong></td>
</tr>
<tr>
<td>• Inappropriate use of social media</td>
</tr>
<tr>
<td>• Distraction/productivity loss</td>
</tr>
<tr>
<td>• Inadequate training and awareness</td>
</tr>
</tbody>
</table>
A well-defined strategy and risk-based approach is needed to manage social media programs

- **Strategy** — The basis for aligning activities with standards and strategic objectives.
- **Risk Management** — Provides for structured management, mitigation, and continuous monitoring of risks.
- **Governance** — Sets the policy and process framework to realize opportunities and manage/mitigate risks.
- **Audit and Compliance** — Ensures adherence to relevant regulations, laws, standards, and internal policies and procedures.
- **Training, Education, and Awareness** — Ensures employees remain current on new and existing policies and procedures related to social media.
Regulations & guidelines

**FINRA:** Regulatory Notice 10-06, 11-39, 12-29: Guidance on social networking websites and business communications

**NLRB:** Approved policy prohibits “inappropriate postings”

**SEC:** First set of guidelines to help investment advisers comply with antifraud and recordkeeping mandates

**FDA:** Communications rules led to shutdown of many pharmaceutical social networking pages when they eliminated the option to turn off public comments

**FTC:** FTC rules regarding identity and affiliation disclosures, disclaimers, and endorsements

**Others:** Financial institutions’ social media content must abide by the same federal rules as other forms of advertising. Regulations include Reg B, DD and Z as well as the Gramm-Leach-Bliley Act.
Social media risk assessment approach

### Phase I: Planning and scoping

**Activities:**
- Identify key internal and external stakeholders: Marketing, Product Development, IT, Compliance, Legal, Risk, etc.
- Obtain relevant documents, strategy, policies, governance structure, etc.
- Define/agree on scope and search criteria
- Identify areas of focus
- Develop a project plan and time table including program piloting strategy

**Deliverables:**
- Project Plan

### Phase II: Social Listening

**Activities:**
- Define search terms: brands, keywords, topic points, comparison organizations
- Generate social media research reports through “listening” and “risk sensing” tools
- Review raw data and identify patterns, anomalies, and areas for additional focus

**Milestone:**
- Social media listening report and high level insights

### Phase III: Design and discovery

**Activities:**
- Obtain stakeholder feed of “current state” through:
  - Online surveys
  - Workshops
  - Publicly available or privately subscribed information
- Review existing social media and relevant security policies, strategies, governance
- Review user access to owned social sites
- Review regulatory requirements
- Develop risk assessment framework

**Milestone:**
- Questionnaires, surveys or workshops
- Templates

### Phase IV: Assess and analyze

**Activities:**
- Synthesize responses
- Aggregate the results using broad themes
- Identify prioritized emerging risks and potential impacts from assessment and sensing research
- Validate the observations with the stakeholders in one on one interviews

**Milestone:**
- Summary of preliminary findings
- Validation meetings

### Phase V: Collaboration and reporting

**Activities:**
- Collaborate with Deloitte subject matter experts and management to stratify emerging risks, potential impact
- Develop risk mitigation response strategies for risks
- Identify recommendations based on insights gained
- Summarize findings

**Deliverable:**
- Final report on recommendations and findings
Would you like to hear how other internal audit functions are evaluating social media risks?

Are you interested in learning more about how other internal audit functions are managing social media risks, as well as leading practices related to governance and control frameworks? If so, we invite you to complete our social media survey. Survey results will be released to participants* who request them.

To access this survey, please visit:
www.deloitte.com/us/socialsurvey

* Names and contact information of survey participants, as well as specific details provided, will be kept strictly confidential.
Digital risks (cont.)

Analytics
Using data to provide deep, relevant insight

Cyber
Are we prepared for attacks? What data is at risk?

Data
Analytics
Do we understand what all our data means? How do we keep track of everything

Social
Are we protecting our reputation? Do we know what is being said?

Mobile
Do we know what tools are accessing our data? Can we keep up with the changing devices?

Cloud
Are we in the cloud? Where is our data and how do our employees, customers and vendors access it?

Convergence
Overview — The intersection of compliance and business analytics

Five big trends are driving the adoption of new approaches to business analytics. Taken together they underscore an unforgiving demand for improved performance — and a wake-up call for more disciplined risk management.

**Data Volumes & Technology Capacity** — Global data volumes continue to grow exponentially. Luckily today’s analytical computing capacity and analytical tools can meet the challenge.

**Regulations** — Regulators are demanding deeper insight into risk, exposure, and public responsiveness from financial, health care, and many other sectors requiring integrated data across the enterprise.

**Profitable Growth** — The need to remain competitive compels investments in analytics infrastructure and tools to improve insight into financial, economic, environmental and market information. The goal? More informed and responsive decisions.

**New Signals** — Holistic signal detection from traditional internal and external structured and unstructured data plus voice, e-mails, social networks, sensor enabled facilities, products, instruments must be integrated and monitored for real time operational insight and decision-making.

**Hidden Insight** — The growing complexity of global business has raised the stakes at all levels of decision-making. Facing more information than humans can possibly process, decision makers need more powerful tools for uncovering hidden patterns that may go undetected.
Analytics benefits — What types of questions can analytics answer

- **Hindsight**
  - What happened?
  - How many, how often, where?

- **Insight**
  - Where is the problem?
  - What actions are needed?
  - Why is this happening?

- **Foresight**
  - What if these trends continue?
  - What will happen next?
  - What’s the best that can happen?
The digital enterprise

Convergence
Do we understand how all the digital technologies interact? What are the risks and are we managing them?

Data Analytics
Do we understand what all our data means? How do we keep track of everything?

Cyber
Are we prepared for attacks? What data is at risk?

Social
Are we protecting our reputation? Do we know what is being said?

Mobile
Do we know what tools are accessing our data? Can we keep up with the changing devices?

Cloud
Are we in the cloud? Where is our data and how do our employees, customers and vendors access it?
The building blocks for digital risk management are not radically new — an end-to-end lifecycle approach **for a digital risk management program can help organizations “get it right” with competitive benefits**
Effective digital risk management begins with an understanding of what digital assets you own, within what channels and markets you have a digital footprint, and what digital risks impact the “heart of the business”— core strategy, brand reputation, customer experience, etc.

Holistic approach to digital risk management

Governance structure
- Internal mechanisms to control ownership, review, approval, monitoring, reporting and improvement of digital assets and online activity

Policies and standards
- Establishing a pre-defined rule set, against which digital activity can be created, deployed, managed and retired

Processes
- Establishing new, and realigning existing, internal processes to comply with policies, security & privacy reviews, standards and procedures

Tools and techniques
- Leveraging appropriate tools and technologies to enforce control and ensure governance is actively maintained and monitored

Risk Management Components
- Who?
  - Stakeholder Groups/Interested Parties
- How?
  - Digital Channels
- Where?
  - Markets (Global, Regional, Single Country)

Digital Risk Register

Who?
- Stakeholder Groups/Interested Parties

How?
- Digital Channels

Where?
- Markets (Global, Regional, Single Country)
A risk intelligent approach

<table>
<thead>
<tr>
<th>Phase</th>
<th>Explore</th>
<th>Identify</th>
<th>Assess</th>
<th>Respond</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key Activities</td>
<td>• Understand the digital landscape</td>
<td>• Identify risks and risk interactions</td>
<td>• Identify key stakeholders and SMEs</td>
<td>• Prioritize recommendations and proposed initiatives</td>
</tr>
<tr>
<td></td>
<td>• Identify and interview relevant stakeholders</td>
<td>• Document observations</td>
<td>• Assess risks and rank for each area</td>
<td>• Consolidate initiatives into an overall roadmap identifying short term and strategic goals</td>
</tr>
<tr>
<td></td>
<td>• Review supporting documentation and artifacts</td>
<td>• Validate observations with stakeholders</td>
<td>• Determine areas of improvement</td>
<td>• Execute risk mitigation plans</td>
</tr>
<tr>
<td></td>
<td>• Perform external scans</td>
<td>• Research potential impact of risks</td>
<td>• Develop risk mitigation activities</td>
<td></td>
</tr>
</tbody>
</table>

| Outputs | | | | |
| --- | --- | --- | --- |
| • An understanding of your digital landscape | • An inventory of your digital risks | • A ranking of digital risks | • A risk intelligent response to the convergence of digital risks |
| • An understanding of the potential convergence risks | • A listing of preliminary recommendations | | |