Deloitte.

Risks Through the Convergence of Digital Technologies

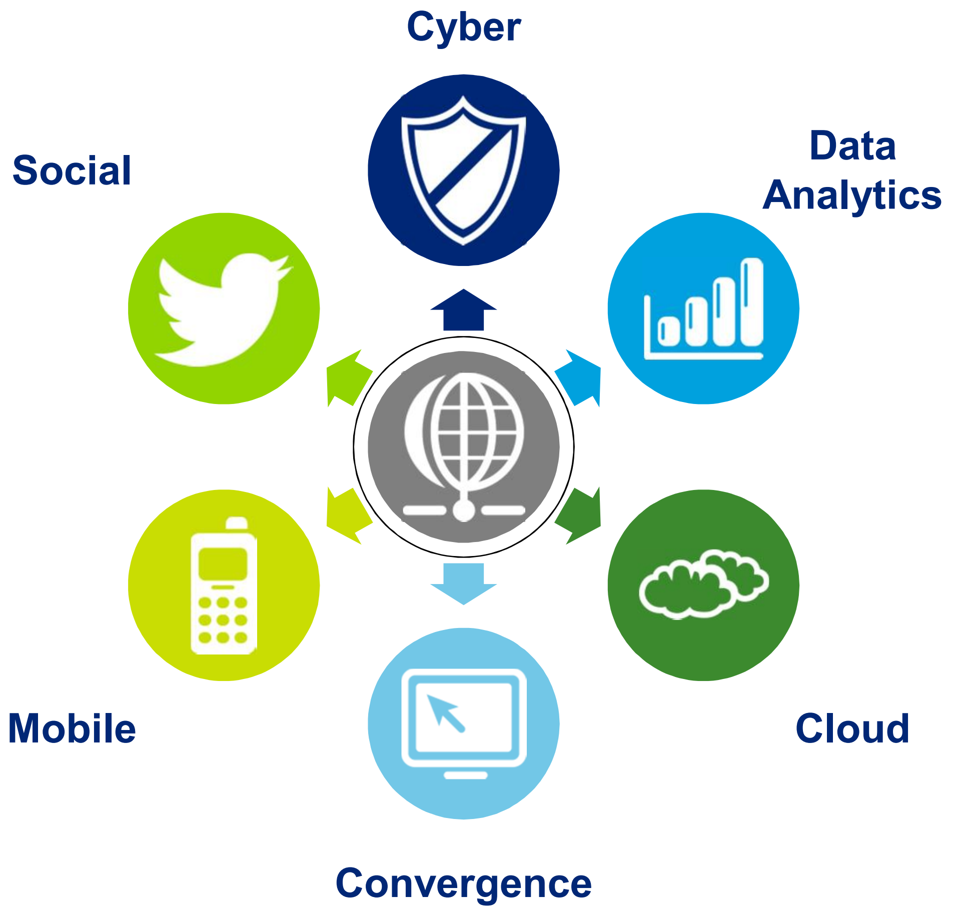
The Digital Enterprise

Khalid Wasti
Director, Deloitte & Touche LLP

Digital risks

Data in the Center

Corporate data and information are a vital enterprise asset that must be stored and protected.



Cyber

Social

Data Analytics

Mobile

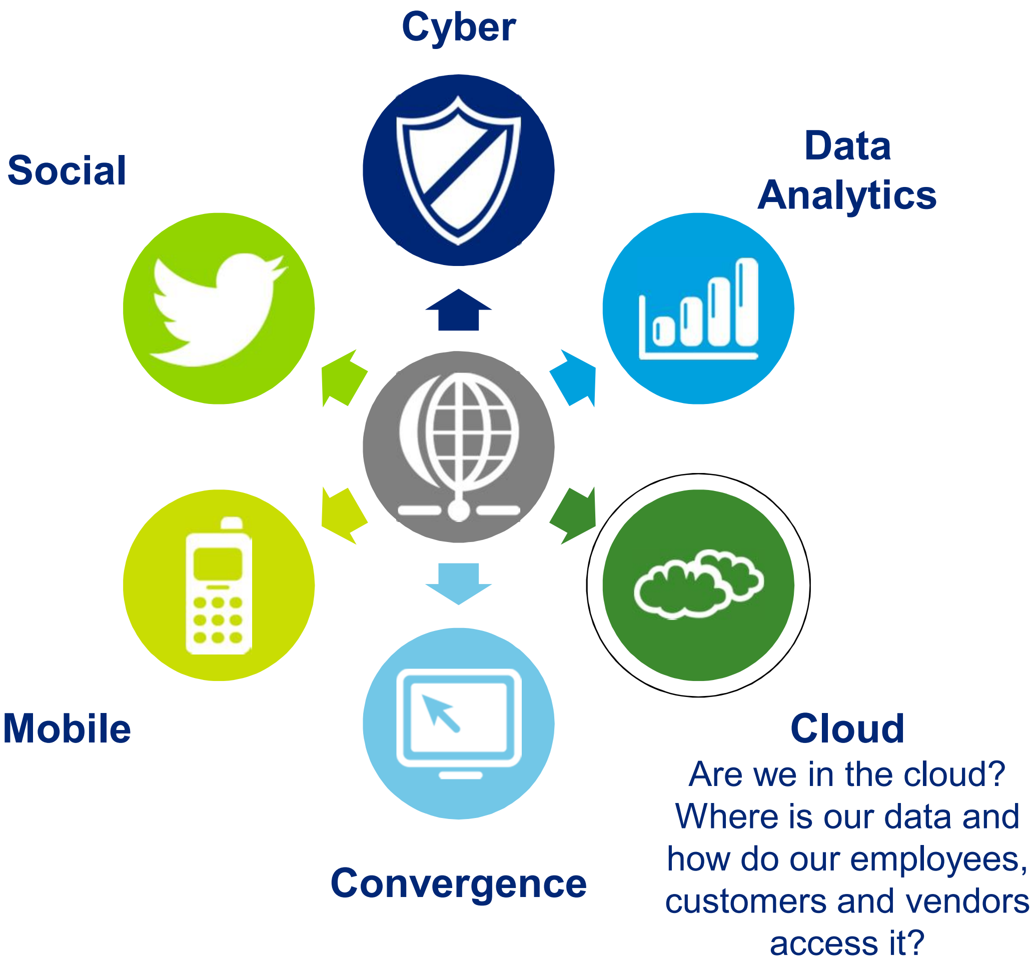
Cloud

Convergence

Digital risks (cont.)

Cloud

Changing how we leverage technology and pay for it



Cyber

Social

Data Analytics

Mobile

Convergence

Cloud

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

Overview

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.

Cloud Computing Security Risks

Availability

Service Availability and Recoverability

- Cloud provider may not be able to match in-house IT service availability, recovery time objectives (RTO), and recovery point objectives (RPO)

Over-Subscription Risk

- In the event of a disaster, other customers may receive higher priority in recovery activities
- As cloud providers shift from investment mode to capture market share to cost cutting mode to reach profitability, capacity may become constrained

Privacy

Legal Uncertainties

- Multiple jurisdictions increase regulatory complexity
- Data sharing agreements may be required before moving data to the cloud
  - Business associate agreements (HIPAA)
  - Data controllers and third parties (EU DPD)

Breach/Disclosure

- Centralized data stores are especially prone to security breaches
- Timely discovery and reporting of the breach by the cloud provider may be challenging

Authentication

Federated Authentication

- 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.

Key Management

- Any activity related to key generation, exchange, storage, safeguarding, use, vetting, and replacement that results in disclosure will provide access to infrastructure and data.

Operational Security

Vulnerability Management

One vulnerability has the potential to expose large number of corporations critical assets.

Asset Management

Assets in the cloud are not properly managed and could leak critical company information or cause data exposures.

Incident Response

Ownership, responsibilities, and actions during incident response are not defined.

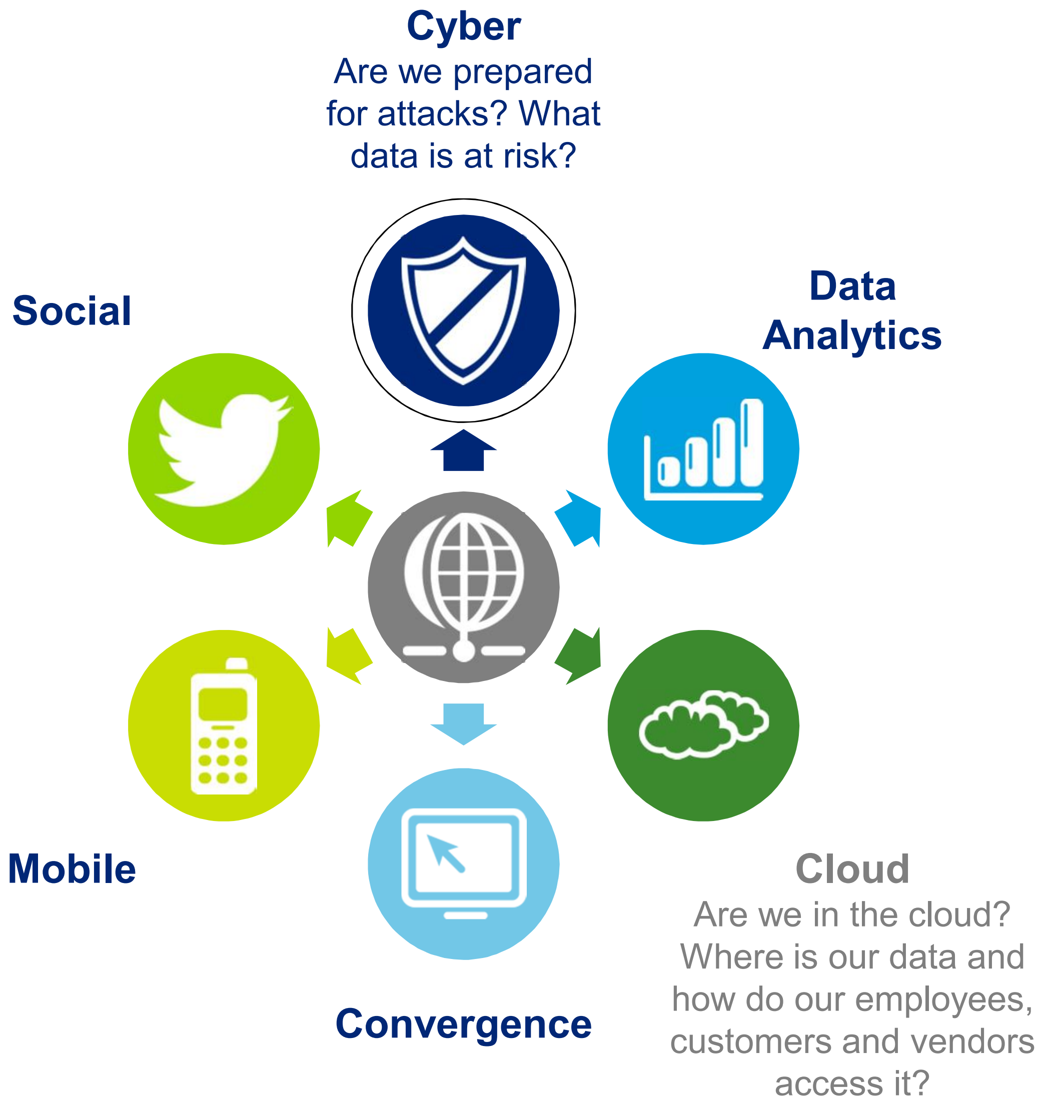
Cloud Computing Risk Assessment Approach

Phase	Phase I: Planning and scoping	Phase II: Develop customized integrated risk & control framework	Phase III: Perform risk assessment	Phase IV: Perform risk mitigation	Phase V: Collaboration and reporting
Key Activities	**Activities:** • 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	**Activities:** • 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	**Activities:** • 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	**Activities:** • 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	**Activities:** • Collaborate with Deloitte subject matter experts and management to stratify emerging risks, potential impact • Summarize findings
Deliverables	**Milestone:** • Project Plan	**Milestone:** • Customized Integrated Risk framework	**Milestone:** • Cloud Computing Risk Heat Map	**Milestone:** • Risk Remediation plan	**Deliverable:** • Final report on recommendations and findings

Digital risks (cont.)

Cyber Security

Providing for secure conversations



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

Social

Data Analytics

Mobile

Convergence

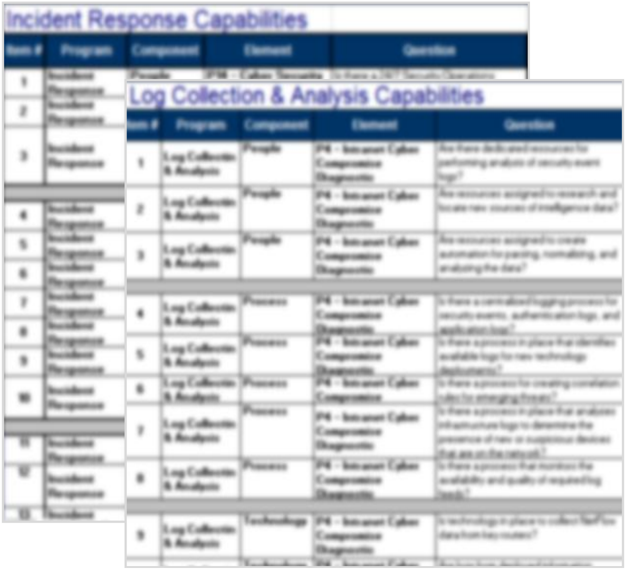
Cloud
Are we in the cloud? Where is our data and how do our employees, customers and vendors access it?

Cyber Security Capabilities Assessment / Risk Analysis

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

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:



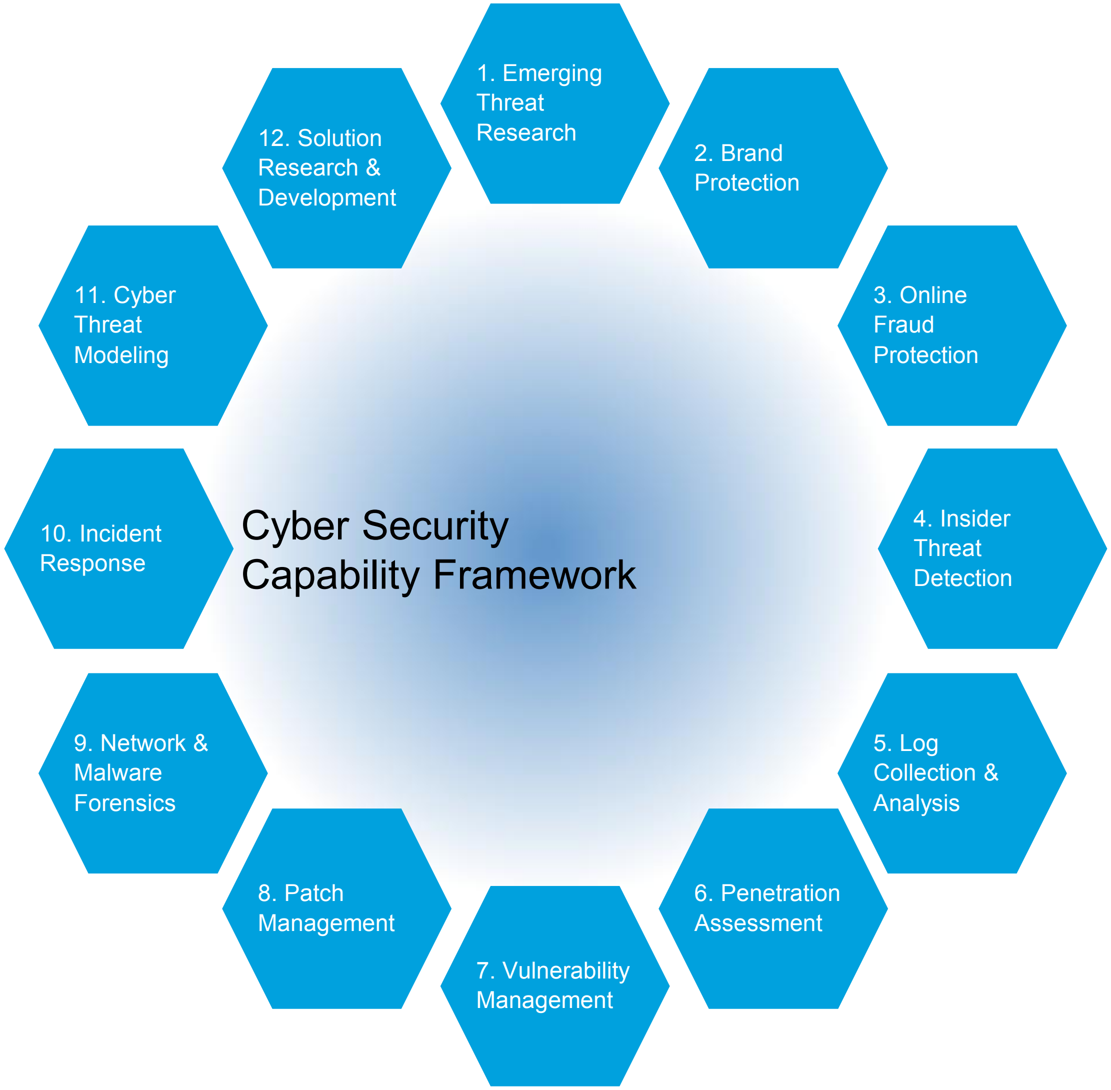
Incident Response Capabilities

Item #	Program	Component	Element	Question
1	Incident Response	People	IPM - Cyber Security	Is there a 24/7 Security Operations
2	Incident Response			
3	Incident Response			
4	Incident Response			
5	Incident Response			
6	Incident Response			
7	Incident Response			
8	Incident Response			
9	Incident Response			
10	Incident Response			
11	Incident Response			
12	Incident Response			
13	Incident			

Log Collection & Analysis Capabilities

Item #	Program	Component	Element	Question
1	Log Collection & Analysis	People	P4 - Intranet Cyber Compromise Diagnostic	Are there dedicated resources for performing analysis of security event logs?
2	Log Collection & Analysis	People	P4 - Intranet Cyber Compromise Diagnostic	Are resources assigned to research and locate new sources of intelligence data?
3	Log Collection & Analysis	People	P4 - Intranet Cyber Compromise Diagnostic	Are resources assigned to create automation for parsing, normalizing, and analyzing the data?
4	Log Collection & Analysis	Process	P4 - Intranet Cyber Compromise Diagnostic	Is there a centralized logging process for security events, authentication logs, and application logs?
5	Log Collection & Analysis	Process	P4 - Intranet Cyber Compromise Diagnostic	Is there a process in place that identifies available logs for new technology deployments?
6	Log Collection & Analysis	Process	P4 - Intranet Cyber Compromise	Is there a process for creating correlation rules for emerging threats?
7	Log Collection & Analysis	Process	P4 - Intranet Cyber Compromise Diagnostic	Is there a process in place that analyzes infrastructure logs to determine the presence of new or suspicious devices that are on the network?
8	Log Collection & Analysis	Process	P4 - Intranet Cyber Compromise Diagnostic	Is there a process that monitors the availability and quality of required log feeds?
9	Log Collection & Analysis	Technology	P4 - Intranet Cyber Compromise Diagnostic	Is technology in place to collect NetFlow data from key routers?

Cyber Security Capability Assessment Questionnaire



Cyber Security Capability Framework

1. Emerging Threat Research
2. Brand Protection
3. Online Fraud Protection
4. Insider Threat Detection
5. Log Collection & Analysis
6. Penetration Assessment
7. Vulnerability Management
8. Patch Management
9. Network & Malware Forensics
10. Incident Response
11. Cyber Threat Modeling
12. Solution Research & Development

Cyber Security Capability Domains

D&T's Cyber Threat Intelligence Capability Framework
1. Emerging Threat Research
2. Brand Protection
3. Online Fraud Protection
4. Insider Threat Detection
5. Log Collection & Analysis
6. Penetration Assessment
7. Vulnerability Management
8. Patch Management
9. Network & Malware Forensics
10. Incident Response
11. Cyber Threat Modeling
12. Solution Research & Development

1. Emerging Threat Research	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.
2. Brand Protection	Capabilities to protect the organization's online brand by proactive monitoring and detection of brand and reputation attacks.
3. Online Fraud Protection	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.
4. Insider Threat Protection	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.
5. Penetration Testing	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.
6. Vulnerability Management	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.

Cyber Security Capability Domains (cont'd)

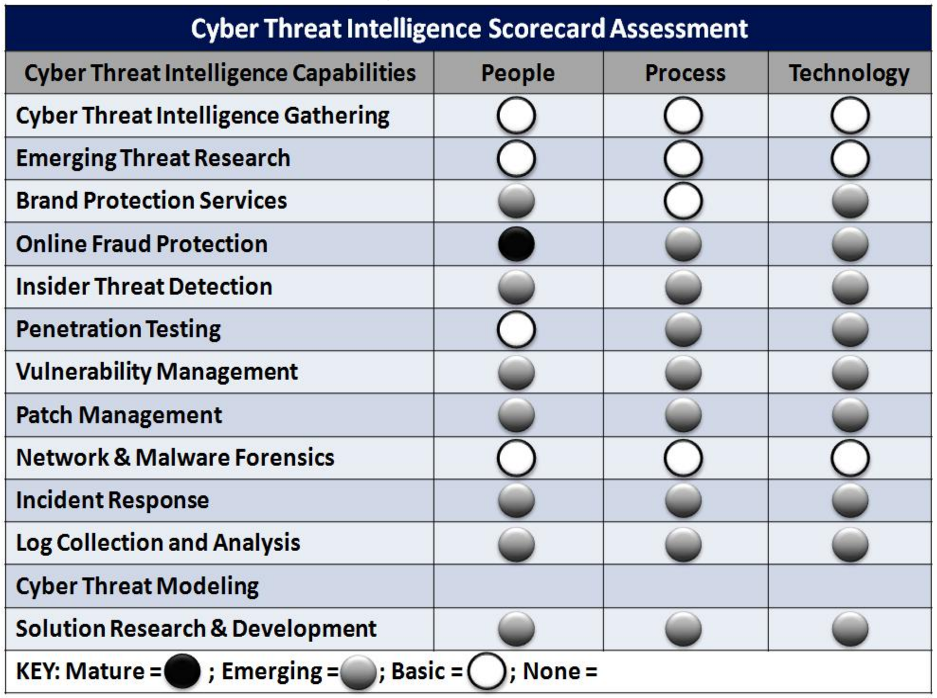
D&T's Cyber Threat Intelligence Capability Framework
1. Emerging Threat Research
2. Brand Protection
3. Online Fraud Protection
4. Insider Threat Detection
5. Log Collection & Analysis
6. Penetration Assessment
7. Vulnerability Management
8. Patch Management
9. Network & Malware Forensics
10. Incident Response
11. Cyber Threat Modeling
12. Solution Research & Development

7. Patch Management	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.
8. Network and Malware Forensics	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.
9. Incident Response	Capabilities for the tracking, response, measurement, and metrics collection of security incidents across the organization's enterprise
10. Log Collection and Analysis	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.
11. Cyber Threat Modeling	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.
12. Solution Research and Development	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.

Illustrative Deliverables

We will assess at a high-level Company’s current state Cyber Security capabilities, including for the **people, process, and technology areas** . Risks will be identified for Company based on gaps in these capabailities.

Capability Assessment Scorecard



Cyber Threat Intelligence Scorecard Assessment			
Cyber Threat Intelligence Capabilities	**People**	**Process**	**Technology**
Cyber Threat Intelligence Gathering	○	○	○
Emerging Threat Research	○	○	○
Brand Protection Services	◐	○	◐
Online Fraud Protection	●	◐	◐
Insider Threat Detection	◐	◐	◐
Penetration Testing	○	◐	◐
Vulnerability Management	◐	◐	◐
Patch Management	◐	◐	◐
Network & Malware Forensics	○	○	○
Incident Response	◐	◐	◐
Log Collection and Analysis	◐	◐	◐
Cyber Threat Modeling			
Solution Research & Development	◐	◐	◐
KEY: Mature = ● ; Emerging = ◐; Basic = ○; None =			

Capability Assessment Findings and Cyber Risks

Penetration Testing				
Area	**Findings**	Ref.	**Recommendations**	Ref.
People	▪ 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	2.6.4	▪ 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.	2.6.4
Process	▪ The organization has limited capability to conduct penetration testing in a staged environment or against new and emerging threats	2.6.5	▪ 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	2.6.5
Technology	▪ 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.	2.6.6	▪ Either through agreement with a 3rd Party Vendor, or through technology acquisition, develop the technology capability to perform out of cycle penetration testing.	2.6.6

Digital risks (cont.)

Mobile

Connecting with people wherever they are

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?

Convergence

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

Overview

Mobile devices, including smart phones, tablets, e-readers, etc. have penetrated 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 presents significant risk.

Mobile Security and Privacy 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

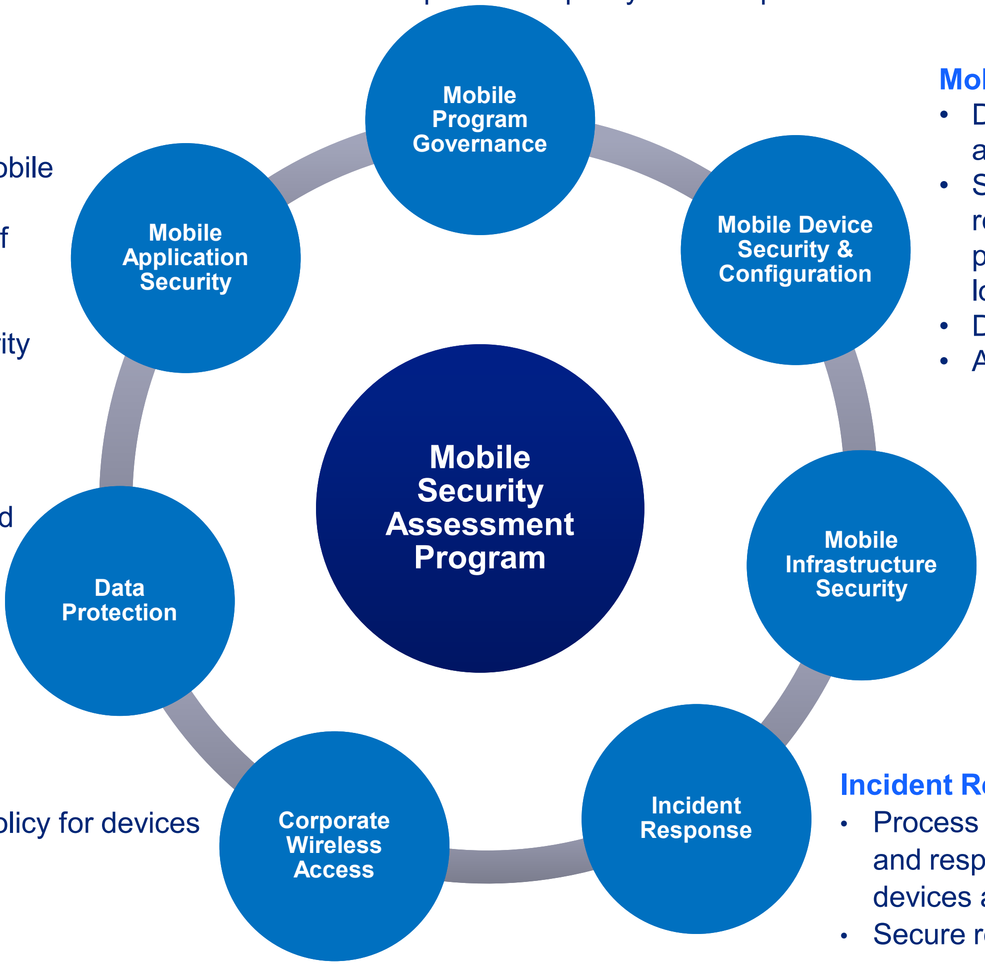
- Malware targeting mobile devices is rapidly maturing and increasing in volume. Additionally, mobile devices may provide an avenue of attack into the enterprise.
- Users may be able to bypass corporate security controls, further weakening the security posture of the device and subjecting the company 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 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 Program Governance
Mobile Device Security & Configuration
Mobile Infrastructure Security
Incident Response
Corporate Wireless Access
Data Protection
Mobile Application Security
Mobile Security Assessment Program

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

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

Data Protection

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

Mobile Infrastructure Security

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

Corporate Wireless Access

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

Incident Response

- Process and procedures for triaging, reporting and responding to incidents related to lost devices and/or stolen content
- Secure removal (‘wipe’)

Mobile Security Audit Scope

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

Digital risks (cont.)

Social

Allowing people to connect electronically in real time

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

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

Convergence

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

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 interactiv***ely 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

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

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

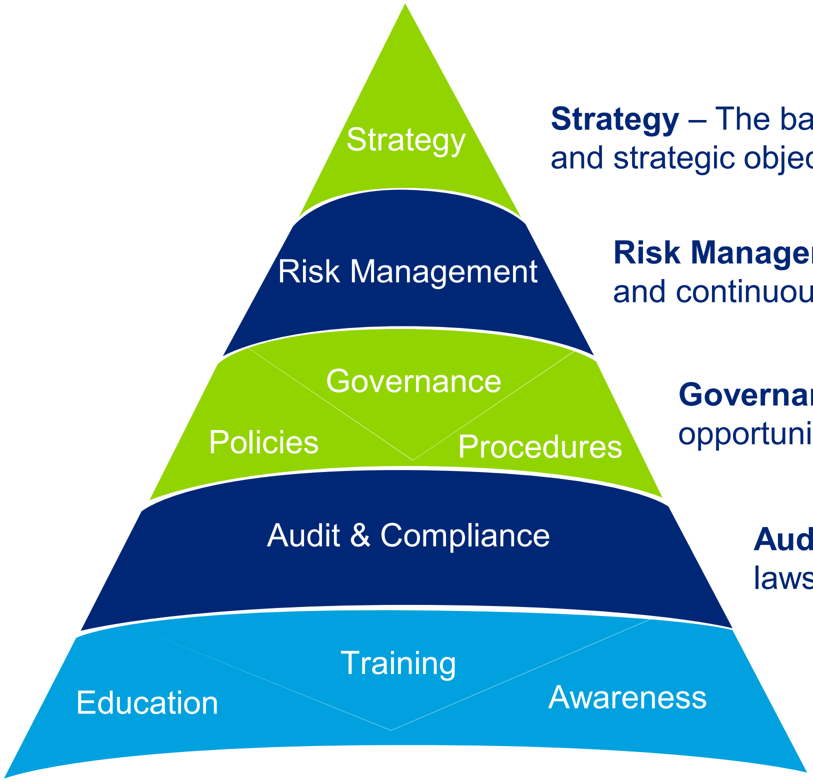
4 Productivity loss

- Social media drives collaboration among co-workers but can also be a major distraction in the work place

Social media: Risks

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

A well-defined strategy and risk-based approach is needed to manage social media programs



Social media governance

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.

Assessment Approach

Phase	Phase I: Planning and scoping	Phase II: Social Listening	Phase III: Design and discovery	Phase IV: Assess and analyze	Phase V: Collaboration and reporting
Key Activities	**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	**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	**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	**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	**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
Deliverables	**Milestone:** • Project Plan	**Milestone:** • Social media listening report and high level insights	**Milestone:** • Questionnaires, surveys or workshops • Templates	**Milestone:** • Summary of preliminary findings • Validation meetings	**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:

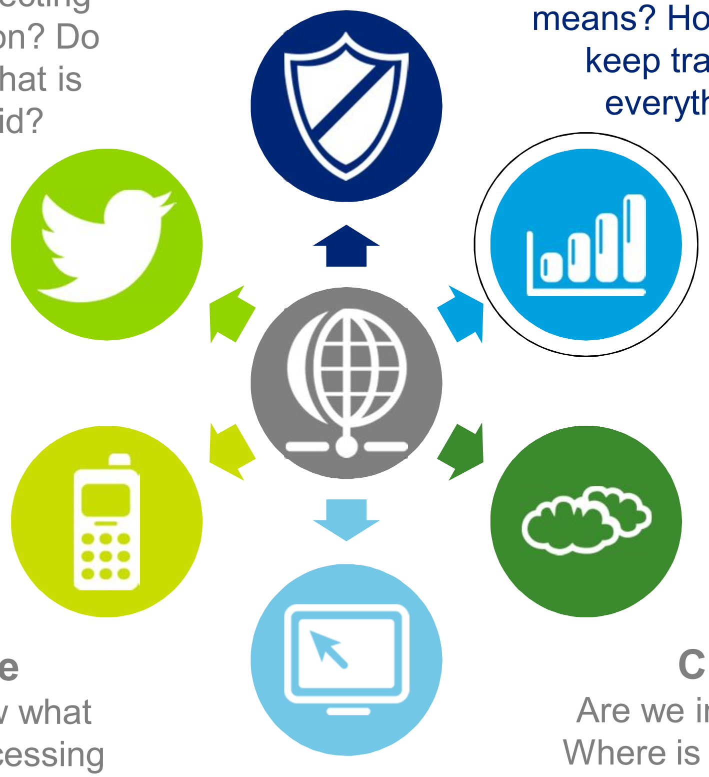
www.deloitte.com/us/socialsurvey

* 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?

Convergence

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

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.**

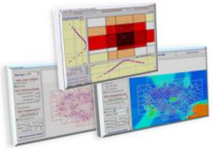
Data Volumes & Technology Capacity — Global data volumes continue to grow exponentially. Luckily today's analytical computing capacity and analytical tools can meet the challenge.

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.

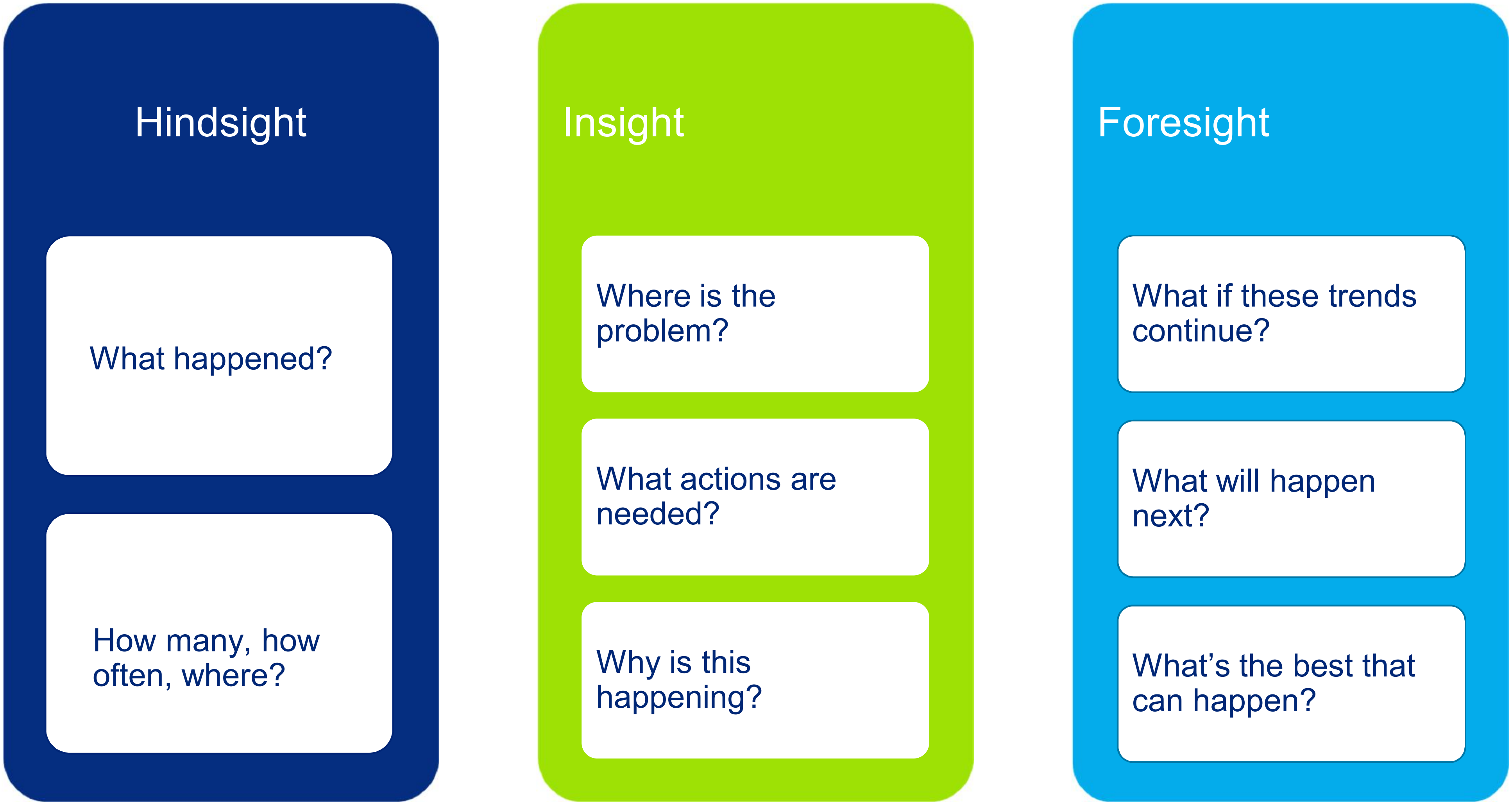
Wisdom of Crowds
Equipment
Facilities
Energy
Email
Documents
Signal
Analysis
Action
Excel
Operational
Systems
Economic
Geological
Climate
Threat
Social Web Analytics

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

New technologies embraced by businesses to keep pace with competition have evolved to become interrelated and are the core of the **Postdigital Enterprise**

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

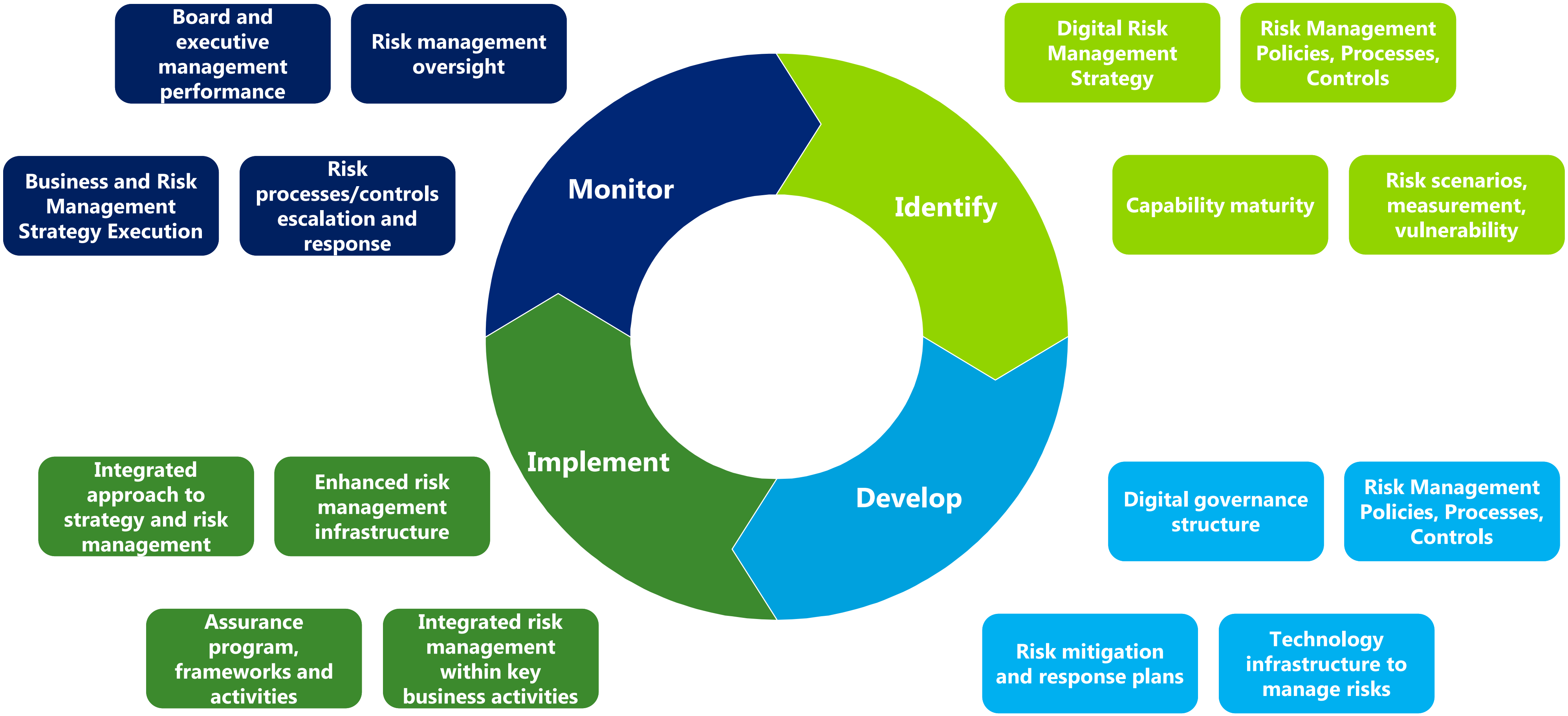
Mobile
Do we know what tools are accessing our data? Can we keep up with the changing devices?

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

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

Digital Risk Management Lifecycle

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 the greatest competitive benefits



Monitor

Board and executive management performance

Risk management oversight

Business and Risk Management Strategy Execution

Risk processes/controls escalation and response

Identify

Digital Risk Management Strategy

Risk Management Policies, Processes, Controls

Capability maturity

Risk scenarios, measurement, vulnerability

Develop

Digital governance structure

Risk Management Policies, Processes, Controls

Risk mitigation and response plans

Technology infrastructure to manage risks

Implement

Integrated approach to strategy and risk management

Enhanced risk management infrastructure

Assurance program, frameworks and activities

Integrated risk management within key business activities

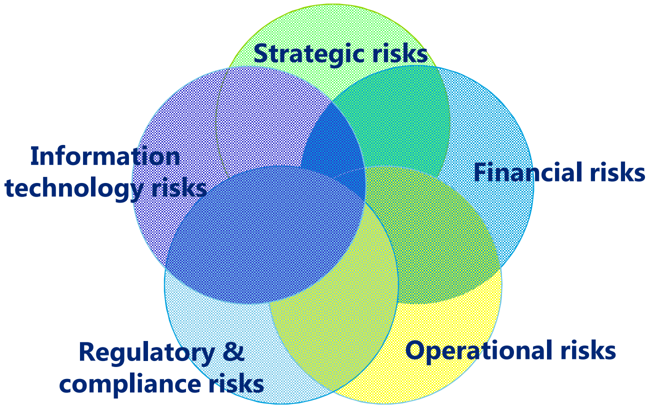
Holistic Approach to Digital Risk Management

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.

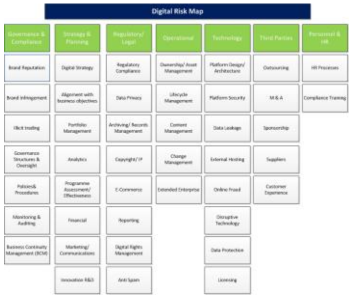
Who?
Stakeholder Groups / Interested Parties

How?
Digital Channels

Where?
Markets (Global, Regional, Single Country)



Digital Risk Register



Digital Risk Map

Governance & Compliance	Strategy & Planning	Regulatory/ Legal	Operational	Technology	Third Parties	Personnel & HR
Brand Reputation	Digital Strategy	Regulatory Compliance	Ownership/ Asset Management	Platform Design/ Architecture	Outsourcing	HR Processes
Brand Infringement	Alignment with business objectives	Data Privacy	Lifecycle Management	Platform Security	M & A	Compliance Training
Illicit trading	Portfolio Management	Archiving/ Records Management	Content Management	Data Leakage	Sponsorship	
Governance Structures & Oversight	Analytics	Copyright/ IP	Change Management	External Hosting	Suppliers	
Policies& Procedures	Programme Assessment/ Effectiveness	E-Commerce	Extended Enterprise	Online Fraud	Customer Experience	
Monitoring & Auditing	Financial	Reporting		Disruptive Technology		
Business Continuity Management (BCM)	Marketing/ Communications	Digital Rights Management		Data Protection		
	Innovation R&D	Anti Spam		Licensing		

Risk Management Components

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

A risk intelligent approach

Phase	Explore	Identify	Assess	Respond
Key Activities	• Understand the digital landscape • Identify and interview relevant stakeholders • Review supporting documentation and artifacts • Perform external scans	• Identify risks and risk interactions • Document observations • Validate observations with stakeholders • Research potential impact of risks	• Identify key staketholders and SMEs • Assess risks and rank for each area • Determine areas of improvement • Develop risk mitigation activities	• Prioritize recommendations and proposed initiatives • Consolidate initiatives into an overall roadmap identifying short term and strategic goals • Execute risk mitigation plans
Outputs	• An understanding of your digital landscape	• An inventory of your digital risks • An understanding of the potential convergence risks	• A ranking of digital risks • A listing of preliminary recommendations	• A risk intelligent response to the convergence of digital risks

Contacts

Khalid Wasti
Director
Deloitte & Touche LLP
+1 212 436 5156
kwasti@deloitte.com

LinkedIn: www.linkedin.com/pub/khalid-wasti/9/1a/537

This publication contains general information only and is based on the experiences and research of Deloitte practitioners. Deloitte is not, by means of this publication, rendering business, financial, investment, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte, its affiliates, and related entities shall not be responsible for any loss sustained by any person who relies on this publication.

About Deloitte
Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.