Deloitte.

Cybersecurity

The role of Internal Audit

Cyber risk—High on the agenda

Audit committees and board members are seeing cybersecurity as a top risk, underscored by recent headlines and increased government and regulatory focus

Recent **U.S. Securities and Exchange Commission (SEC)** guidance regarding **disclosure obligations** relating to cybersecurity risks and incidents…..

"Registrants should address **cybersecurity risks and cyber incidents** in their Management's Discussion and Analysis of Financial Condition and Results of Operations (MD&A), Risk Factors, Description of Business, Legal Proceedings and Financial Statement Disclosures." *SEC Division of Corporate Finance Disclosure Guidance: Topic No. 2 - Cybersecurity*

Ever-growing concerns about cyber-attacks affecting the nation's critical infrastructure prompted the signing of the **Executive Order (EO) 13636, Improving Critical Infrastructure Cybersecurity.**

The Executive Order highlights the focus on an improved **cybersecurity framework** and the rapid changes of **regulatory agency expectations and oversight**

One of the foundational drivers behind the update and release of the **2013 COSO Framework** was the need to address how organizations **use and rely on evolving technology** for internal control purposes

Cyber risk—Drivers

The forces driving growth and efficiency may create a broad attack surface

Technology becomes more pervasive

- Internet, cloud, mobile, and social are mainstream platforms inherently oriented for sharing
- Employees want continuous, real-time access to their information

Changing business models

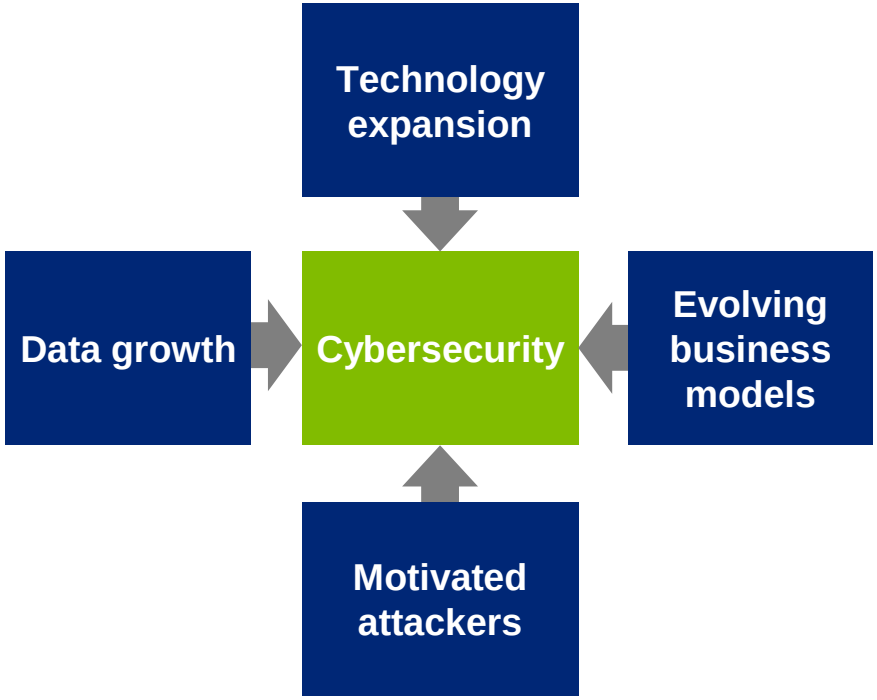
- Service models have evolved—outsourcing, offshoring, contracting, and remote workforce

More data to protect

- Increased volume of customers' personal, account, and credit card data, as well as employee's personal identifiable information and also company trade secrets
- The need to comply with privacy requirements across a wide array of jurisdictions

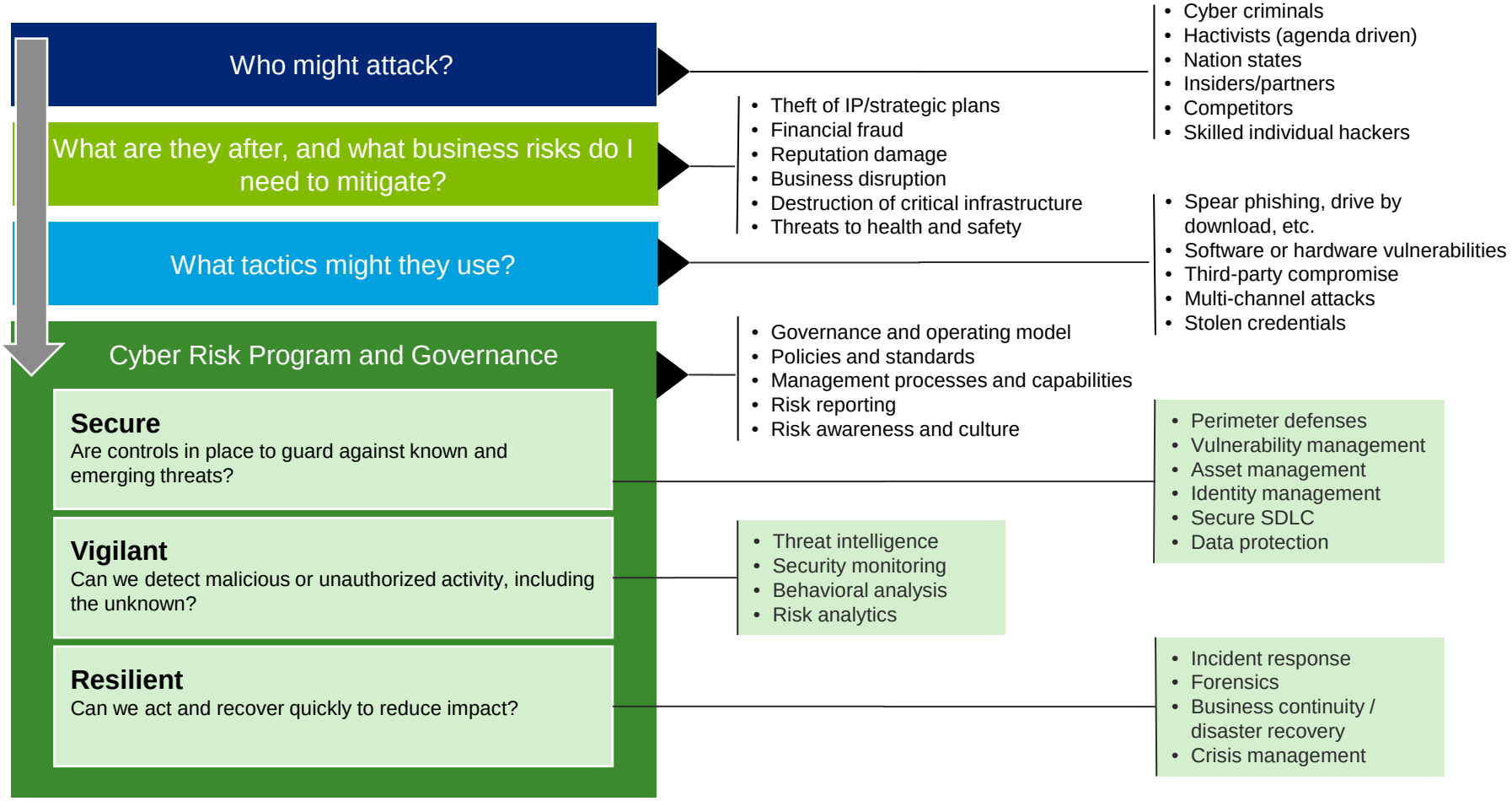
Threat actors with varying motives

- Hackers to nation states
- Continuously innovating and subverting common controls
- Often beyond the reach of a country's law enforcement



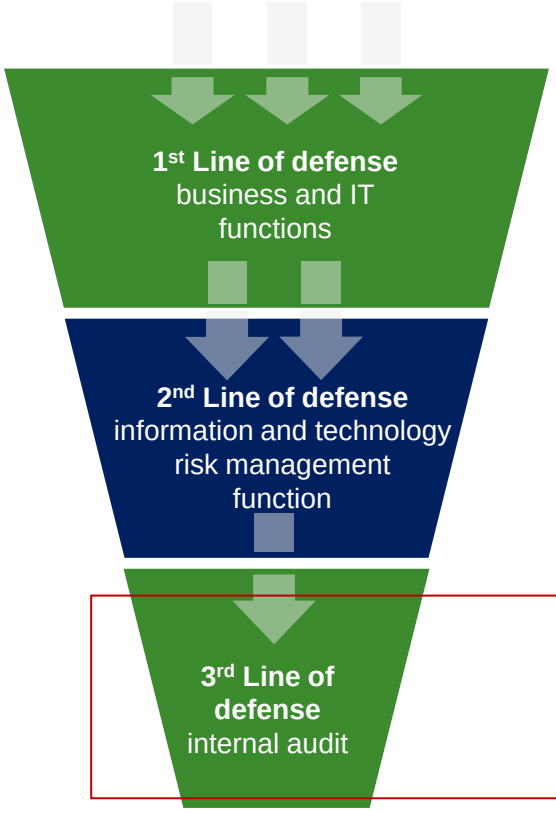
Cyber risk—Appetite

Management should develop an understanding of who might attack, why, and how



Cyber risk—Roles and responsibilities

Effective risk management is the product of multiple layers of risk defense. Internal Audit should support the board's need to understand the effectiveness of cybersecurity controls.



Roles and responsibilities
• Incorporate risk-informed decision making into day-to-day operations and fully integrate risk management into operational processes • Define risk appetite and escalate risks outside of tolerance • Mitigate risks, as appropriate
• Establish governance and oversight • Set risk baselines, policies, and standards • Implement tools and processes • Monitor and call for action, as appropriate • Provide oversight, consultation, checks and balances, and enterprise-level policies and standards
• Independently review program effectiveness • Provide confirmation to the board on risk management effectiveness • Meet requirements of SEC disclosure obligations focused on cybersecurity risks

Given recent high profile cyber attacks and data losses, and the SEC's and other regulators' expectations, it is critical for Internal Audit to understand cyber risks and be prepared to address the questions and concerns expressed by the audit committee and the board

Cyber risk—Deloitte cybersecurity framework*

An assessment of the organization's cybersecurity should evaluate specific capabilities across multiple domains

Secure

Cybersecurity risk and compliance management

- Compliance monitoring
- Issue and corrective action planning
- Regulatory and exam management
- Risk and compliance assessment and mgmt.
- Integrated requirements and control framework

Secure development life cycle

- Secure build and testing
- Secure coding guidelines
- Application role design/access
- Security design/architecture
- Security/risk requirements

Security program and talent management

- Security direction and strategy
- Security budget and finance management
- Policy and standards management
- Exception management
- Talent strategy

Third-party management

- Evaluation and selection
- Contract and service initiation
- Ongoing monitoring
- Service termination

Information and asset management

- Information and asset classification and inventory
- Information records management
- Physical and environment security controls
- Physical media handling

Identity and access management

- Account provisioning
- Privileged user management
- Access certification
- Access management and governance

Vigilant

Threat and vulnerability management

- Incident response and forensics
- Application security testing
- Threat modeling and intelligence
- Security event monitoring and logging
- Penetration testing
- Vulnerability management

Data management and protection

- Data classification and inventory
- Breach notification and management
- Data loss prevention
- Data security strategy
- Data encryption and obfuscation
- Records and mobile device management

Risk analytics

- Information gathering and analysis around:
  - User, account, entity
  - Events/incidents
  - Fraud and anti-money laundering
  - Operational loss

Resilient

Crisis management and resiliency

- Recover strategy, plans & procedures
- Testing & exercising
- Business impact analysis
- Business continuity planning
- Disaster recovery planning

Security operations

- Change management
- Configuration management
- Network defense
- Security operations management
- Security architecture

Security awareness and training

- Security training
- Security awareness
- Third-party responsibilities

* The Deloitte cybersecurity framework is aligned with industry standards and maps to NIST, ISO, COSO, and ITIL.

Cyber risk—Deloitte cybersecurity framework*

Certain cybersecurity domains may be partially covered by existing IT audits, however many capabilities have historically not been reviewed by internal audit

Secure

Cybersecurity risk and compliance management

- Compliance monitoring
- Issue and corrective action planning
- Regulatory and exam management
- Risk and compliance assessment and mgmt.
- Integrated requirements and control framework

Secure development life cycle

- Secure build and testing
- Secure coding guidelines
- Application role design/access
- Security design/architecture
- Security/risk requirements

Security program and talent management

- Security direction and strategy
- Security budget and finance management
- Policy and standards management
- Exception management
- Talent strategy

Third-party management

- Evaluation and selection
- Contract and service initiation
- Ongoing monitoring
- Service termination

Information and asset management

- Information and asset classification and inventory
- Information records management
- Physical and environment security controls
- Physical media handling

Identity and access management

- Account provisioning
- Privileged user management
- Access certification
- Access management and governance

Vigilant

Threat and vulnerability management

- Incident response and forensics
- Application security testing
- Threat modeling and intelligence
- Security event monitoring and logging
- Penetration testing
- Vulnerability management

Data management and protection

- Data classification and inventory
- Breach notification and management
- Data loss prevention
- Data security strategy
- Data encryption and obfuscation
- Records and mobile device management

Risk analytics

- Information gathering and analysis around:
  - User, account, entity
  - Events/incidents
  - Fraud and anti-money laundering
  - Operational loss

Resilient

Crisis management and resiliency

- Recover strategy, plans & procedures
- Testing & exercising
- Business impact analysis
- Business continuity planning
- Disaster recovery planning

Security operations

- Change management
- Configuration management
- Network defense
- Security operations management
- Security architecture

Security awareness and training

- Security training
- Security awareness
- Third-party responsibilities

* The Deloitte cybersecurity framework is aligned with industry standards and maps to NIST, ISO, COSO, and ITIL.

SOX (financially relevant systems only) | **Penetration and vulnerability testing** | **BCP/DRP Testing**

Cyber risk—Assessment approach

An internal audit assessment of cybersecurity should cover all domains and relevant capabilities, and involve subject matter specialists when appropriate

Phase	Phase I: Planning and scoping	Phase II: Understand current state	Phase III: Risk assessment	Phase IV: Gap assessment and recommendations
Key activities	**Activities:** • Identify specific internal and external stakeholders: IT, Compliance, Legal, Risk, etc. • Understand organization mission and objectives • Identify industry requirements and regulatory landscape • Perform industry and sector risk profiling (i.e., review industry reports, news, trends, risk vectors) • Identify in-scope systems and assets • Identify vendors and third-party involvement	**Activities:** • Conduct interviews and workshops to understand the current profile • Perform walkthroughs of in-scope systems and processes to understand existing controls • Understand the use of third-parties, including reviews of applicable reports • Review relevant policies and procedures, including security environment, strategic plans, and governance for both internal and external stakeholders • Review self assessments • Review prior audits	**Activities:** • Document list of potential risks across all in-scope capabilities • Collaborate with subject matter specialists and management to stratify emerging risks, and document potential impact • Evaluate likelihood and impact of risks • Prioritize risks based upon organization's objectives, capabilities, and risk appetite • Review and validate the risk assessment results with management and identify criticality	**Activities:** • Document capability assessment results and develop assessment scorecard • Review assessment results with specific stakeholders • Identify gaps and evaluate potential severity • Map to maturity analysis • Document recommendations • Develop multiyear cybersecurity/IT audit plan
Deliverables	**Deliverable:** • Assessment objectives and scope • Capability assessment scorecard framework	**Deliverable:** • Understanding of environment and current state	**Deliverable:** • Prioritized risk ranking • Capability assessment findings	**Deliverables:** • Maturity analysis • Assessment scorecard • Remediation recommendations • Cybersecurity audit plan

Cyber risk—Assessment maturity analysis

Maintaining and enhancing security capabilities can help mitigate cyber threats and help the organization to arrive at its desired level of maturity

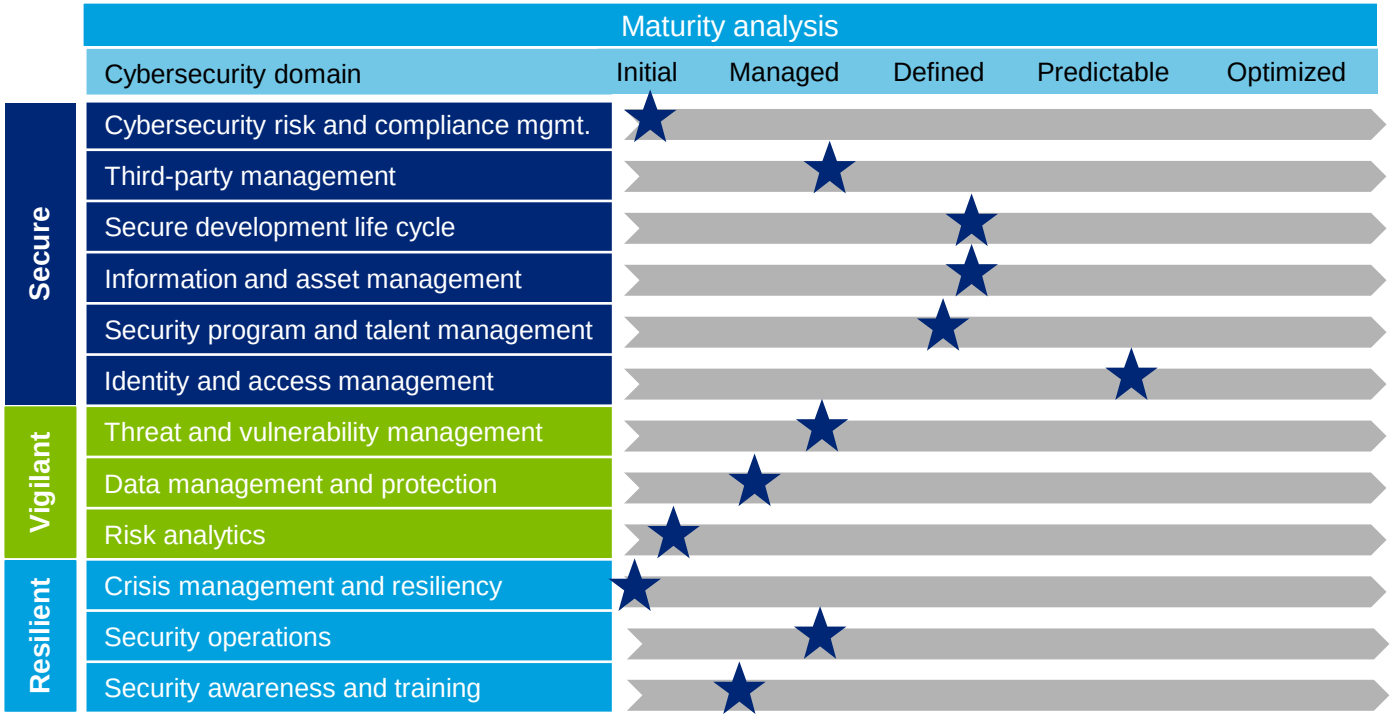
Stage 1: Initial
- Recognized the issue
- Ad-hoc/case by case
- Partially achieved goals
- No training, communication, or standardization

Stage 2: Managed
- Process is managed
- Responsibility defined
- Defined procedures with deviations
- Process reviews

Stage 3: Defined
- Defined process
- Communicated procedures
- Performance data collected
- Integrated with other processes
- Compliance oversight

Stage 4: Predictable
- Defined quantitative performance thresholds and control limits
- Constant improvement
- Automation and tools implemented
- Managed to business objectives

Stage 5: Optimized
- Continuously improved
- Improvement objectives defined
- Integrated with IT
- Automated workflow
- Improvements from new technology



Current state CMMI maturity*

*The industry recognized *Capability Maturity Model Integration (CMMI) can be used as the model for the assessment. Each domain consists of specific capabilities which are assessed and averaged to calculate an overall domain maturity.*

Cyber risk—Assessment scorecard

A scorecard can support the overall maturity assessment, with detailed cyber risks for people, process, and technology. Findings should be documented and recommendations identified for all gaps.

	Assessment Scorecard			
	Cybersecurity domain	People	Process	Technology
Secure	Cybersecurity risk and compliance mgmt.			
Secure	Third-party management			
Secure	Secure development life cycle			
Secure	Information and asset management			
Secure	Security program and talent management			
Secure	Identity and access management			
Vigilant	Threat and vulnerability management	4	2	1
Vigilant	Data management and protection			
Vigilant	Risk analytics			
Resilient	Crisis management and resiliency			
Resilient	Security operations			
Resilient	Security awareness and training			

1: Initial → 2: Managed → 3: Defined → 4: Predictable → 5: Optimized

Capability assessment findings and recommendations

Threat and vulnerability management—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 third-party vendor, or through technology acquisition, develop the technology capability to perform out of cycle penetration testing.	2.6.6

Cyber risk— Representative internal audit plan

A cybersecurity assessment can drive a risk-based IT internal audit plan. Audit frequency should correspond to the level of risk identified, and applicable regulatory requirements/expectations.

Internal Audit	FY 2015	FY 2016	FY 2017	Notes (representative)
SOX IT General Computer Controls	X	X	X	Annual requirement but only covers financially significant systems and applications
External Penetration and Vulnerability Testing	X	X	X	Cover a portion of IP addresses each year
Internal Vulnerability Testing		X		Lower risk due to physical access controls
Business Continuity Plan/Disaster Recovery Plan	X		X	Coordinate with annual 1st and 2nd line of defense testing
Data Protection and Information Security		X		Lower risk due to …
Third-party Management			X	Lower risk due to …
Risk Analytics	X	X	X	Annual testing to cycle through risk areas, and continuous monitoring
Crisis Management	X		X	Cyber war gaming scenario planned
Social Media	X			Social media policy and awareness program
Data Loss Protection (DLP)		X		Shared drive scan for SSN / Credit Card #

Cyber risk—Deloitte IT internal audit

Leading cybersecurity risk management services—specifically suited to collaborate with you

The right resources at the right time

- Deloitte has provided IT audit services for the past 30 years and IT audit training to the profession for more than 15 years. Our professionals bring uncommon insights and a differentiated approach to IT auditing, and we are committed to remaining an industry leader.
- We have distinct advantages through:
  - Access to a global team of IA professionals, including IT subject matter specialists in a variety of technologies and risk areas
  - A responsive team of cyber risk specialists with wide-ranging capabilities virtually anywhere in the world, prepared to advise as circumstances arise or as business needs change
  - A differentiated IT IA approach that has been honed over the years in some of the most demanding environments in the world, with tools and methodologies that help accelerate IT audit
  - Access to leading practices and the latest IT thought leadership on audit trends and issues

#1 provider of cyber risk management solutions

- The only organization with the breadth, depth, and insight to help complex organizations become secure, vigilant, and resilient
- 1000+ cyber risk management projects in the US alone in 2014 executed cross industry
- 11,000 risk management and security professionals globally across the Deloitte Touche Tohmatsu Limited network of member firms

Contributing to the betterment of cyber risk management practices

- Assisted National Institute of Standards and Technology in developing their cybersecurity framework in response to the 2013 Executive Order for Improving Critical Infrastructure Cybersecurity
- Third-party observer of the Quantum Dawn 2 Cyber Attack Simulation, conducted by the Securities Industry and Financial Markets Association in July 2013
- Working with government agencies on advanced threat solutions

- Named as a Kennedy Vanguard Leader in cyber security consulting: “[Deloitte] continually develops, tests, and launches methodologies that reflect a deep understanding of clients’ cyber security and help the firm… set the bar.”

  Source: Kennedy Consulting Research & Advisory; Cyber Security Consulting 2013; Kennedy Consulting Research & Advisory estimates © 2013 Kennedy Information, LLC. Rreproduced under license.

- “Deloitte’s ability to execute rated the highest of all the participants”

  Forrester Research, “Forrester Wave™: Information Security Consulting Services Q1 2013”, Ed Ferrara and Andrew Rose, February 1, 2013

Contacts

Deloitte.

Official Professional Services Sponsor

Professional Services means audit, tax, consulting and financial advisory services.