Western Intergovernmental Audit Forum

Critical Questions for Technological Changes

Reviewing controls for data protection

Crown jewels approach to data protection

What data is important to the organization?

What are the risks to that data?

What is being done to mitigate those risks?

Focus protective measures and assessments on the crown jewels

Are you using a cybersecurity framework?

- Leverage frameworks to provide coverage when conducting assessment
- Go beyond the checklist approach asking open ended questions

Examples:

NIST: National Institute of Standards and Technology

ISO: International Organization for Standardization

COSO: Committee of Sponsoring Organizations of the Treadway Commission

ITIL: Information Technology Infrastructure Library

CIS CSC: Center for Internet Security Critical Security Controls

FFIEC: Federal Financial Institutions Examination Council

Cyber internal audit – a comprehensive framework

Cybersecurity Governance

- Cybersecurity strategy
- Organizational model
- Steering committee structure
- Tone at the top
- Regulatory and legal landscape
- Key indicators

Secure

Program management

- Policies, standards, baselines, guidelines, and procedures
- Talent and budget management
- Asset management
- Change management
- Program metrics & reporting
- Risk and compliance management

Data protection

- Data classification
- Records management
- Data quality management
- Data loss prevention
- Data encryption
- Data privacy
- Defensible destruction

Identity and access management

- Account provisioning
- Account de-provisioning
- Privileged user management
- Access certification
- Access management and governance
- Generic account management
- Multi-factor authentication (MFA)

Infrastructure security

- Hardening standards
- Security design/architecture
- Configuration management
- Network defense
- Security operations management
- Endpoint protection

Software security

- Secure build and testing
- Secure coding guidelines
- Application role design/access
- Development lifecycle
- Patch management

Cloud security

- Cloud strategy
- Cloud risk identification
- Cloud provider inventory
- Minimum controls baseline
- Cloud controls compliance

Third-party management

- Evaluation and selection
- Risk-based tiering
- Contract and service initiation
- Ongoing monitoring
- Service termination

Workforce management

- Onboarding & off boarding
- Physical security
- Phishing exercises
- Security training and awareness
- Privileged user certification

Vigilant

Threat and vulnerability management

- Threat modeling and intelligence
- Penetration testing
- Vulnerability management
- Emerging threats identification
- Brand protection
- Cyber threat information sharing

Monitoring

- Security operations center (SOC)
- Security information and event management (SIEM)
- Cyber risk analytics
- User entity behavior analytics
- Continuous monitoring program

Resilient

Crisis management

- Response planning
- Red team exercises
- Tabletop exercises
- Incident response and forensics
- Crisis communication plan
- Third-party responsibilities

Enterprise resiliency

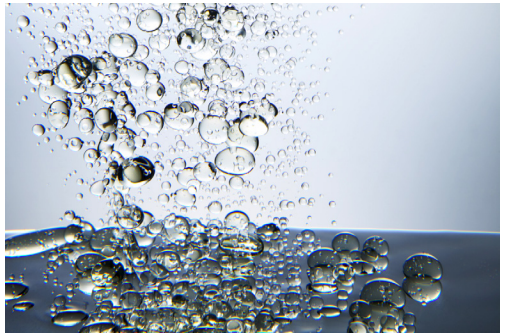
- Business impact analysis (BIA)
- Business continuity planning (BCP)
- Disaster recovery planning (DRP)
- Cyber incident insurance

*The Deloitte Risk & Financial Advisory cyber internal audit framework is aligned with industry standards and maps to NIST, ISO, COSO, ITIL, and CIS CSC. Alternative frameworks may be used.

Controls for data protection

Data exists in three states

- Data at rest
- Data in motion
- Data in use



Are controls based on the value of the data?

Are you encrypting data in the three states?

What controls are in place to protect data in all three states?

How do we ensuring the ownership of data?

Have data classes been defined?

Is data assigned to the defined classes?

Has a data owner been assigned to all data (not just structured data)?

Are minimum protective requirements for each data class defined?

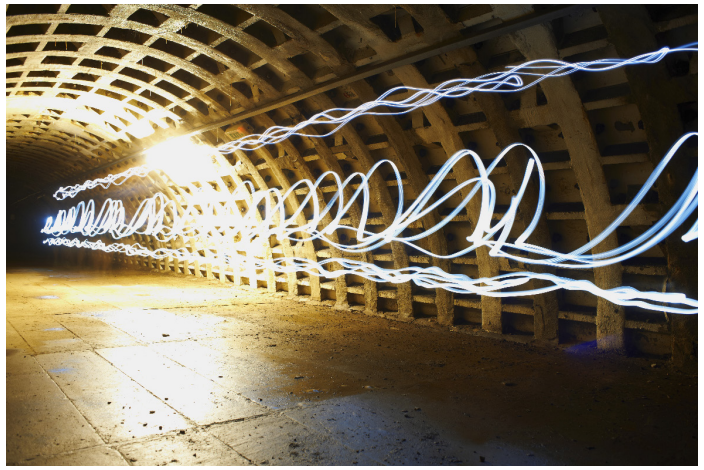
Questions when data transfers from one platform to another

Transfers during normal use:

- Is data in motion encrypted in transit?
- What method is used to authenticate incoming data?
- Do you have a data flow diagram?

Transfers as part of a one time migration:

- Are protective controls in place on par with Production?
- Does access adhere to principle of least privileged?



Contract language questions for IT purchases

Is it a product or a service?

Will the vendor see/touch sensitive data?

What are the SLA’s (service level agreements)?

Is data privacy / security mentioned if it's a service?

Is record retention defined?

Implementation of new tools, data management and cloud services and security.

Cloud:

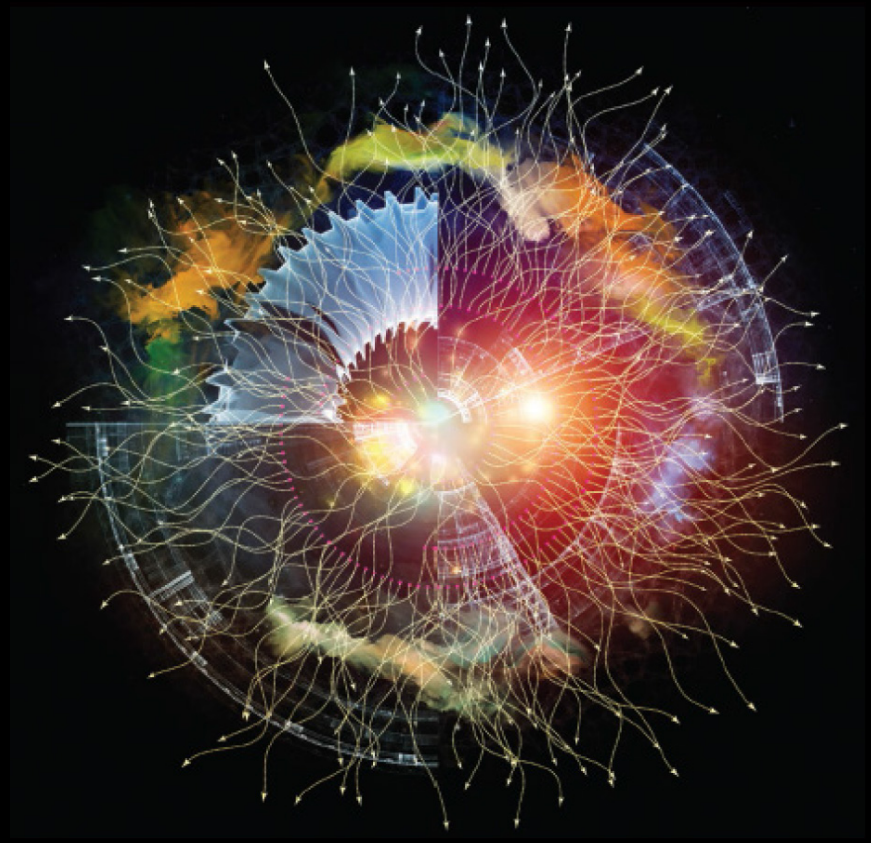
- Has a list of sanctioned cloud applications been determined?
- Has unsanctioned use of cloud applications been reviewed?
- Is a CASB (cloud access security broker) tool in place?

Tools:

- Has a security review of the tool been completed?
- Has access been limited to least privileged?

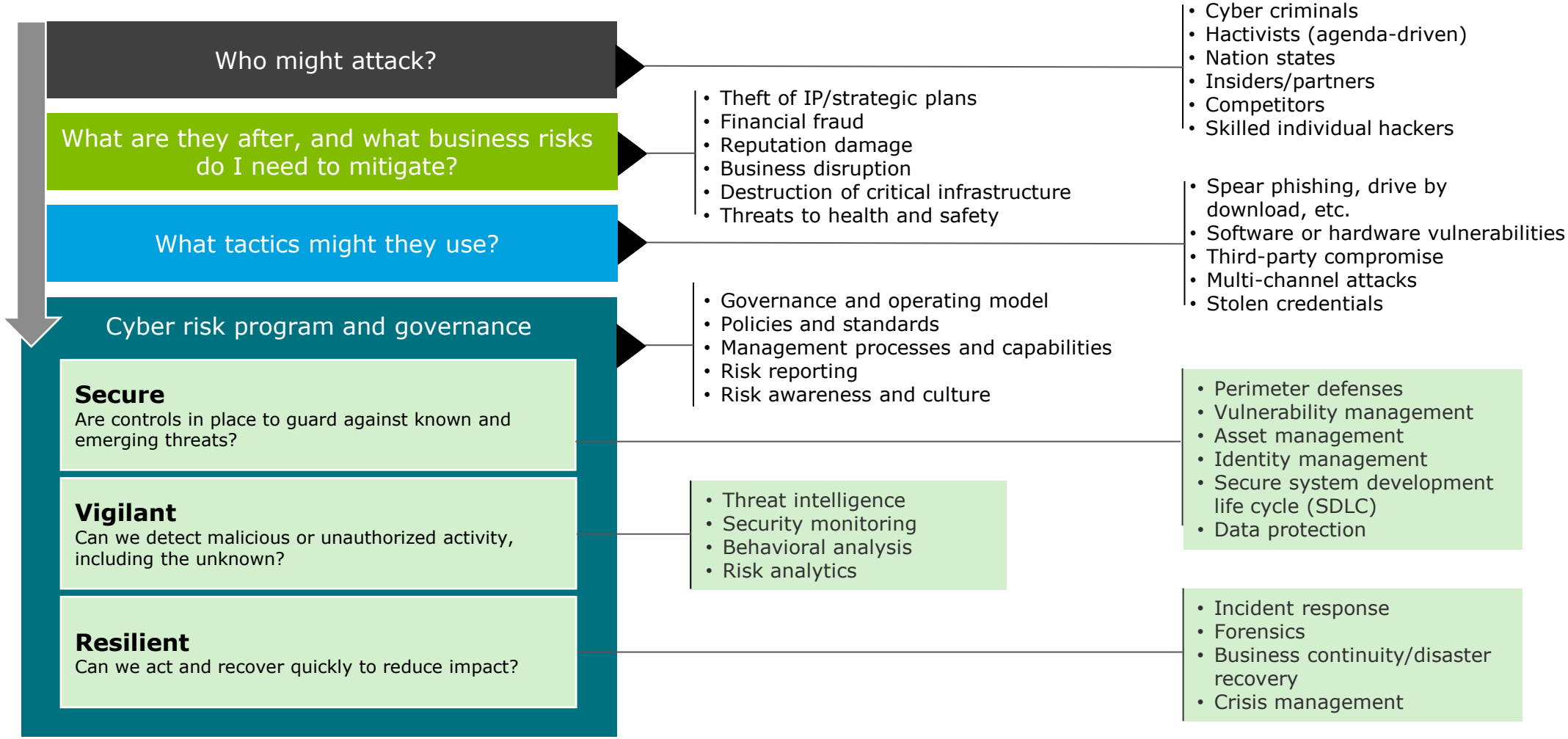
Putting the questions together

The audit program reference material



Focus on identifying your crown jewels

Who might attack them, why they want them, and how they might do it



What can Internal Audit do to support the company's cyber & IT risk management program and objectives?

Its Cyber/IT IA approach should be:

- An ongoing, risk-based program
- Built on a tested cyber/IT framework
- Delivered in both assurance and advisory methods
- Executed on a continuous and risk-based assurance cycle

The IA function should have:

- A solid understanding of the full scope of cyber risks
- An independent viewpoint, supported by the appropriate procedures performed
- A broad-based cybersecurity third line of defense model

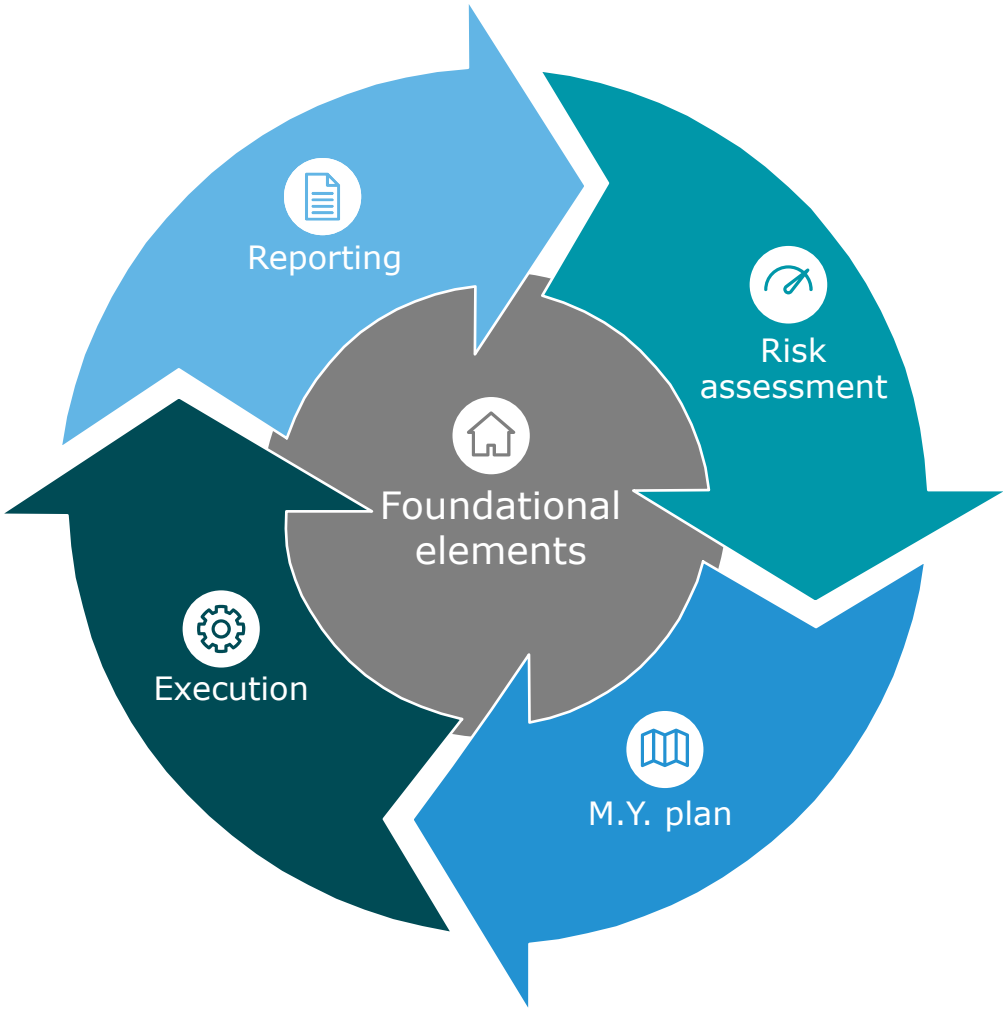
The cyber and IT internal audit program approach

Risk assessment is a comprehensive method for assessing cyber risk, is appropriate for the organization, and is scored

M.Y. plan is a **m**ulti-**y**ear, risk-based assurance cycle which targets domain-specific issues with adequate scoping and sizing

Execution occurs with effective deployment of people, process and tools to provide insights

Reporting is continuous, accurate, scorecard-based, and adequate for multiple stakeholders



Cyber internal audit – a comprehensive framework

Cybersecurity Governance

- Cybersecurity strategy
- Organizational model
- Steering committee structure
- Tone at the top
- Regulatory and legal landscape
- Key indicators

Secure

Program management

- Policies, standards, baselines, guidelines, and procedures
- Talent and budget management
- Asset management
- Change management
- Program metrics & reporting
- Risk and compliance management

Data protection

- Data classification
- Records management
- Data quality management
- Data loss prevention
- Data encryption
- Data privacy
- Defensible destruction

Identity and access management

- Account provisioning
- Account de-provisioning
- Privileged user management
- Access certification
- Access management and governance
- Generic account management
- Multi-factor authentication (MFA)

Infrastructure security

- Hardening standards
- Security design/architecture
- Configuration management
- Network defense
- Security operations management
- Endpoint protection

Software security

- Secure build and testing
- Secure coding guidelines
- Application role design/access
- Development lifecycle
- Patch management

Cloud security

- Cloud strategy
- Cloud risk identification
- Cloud provider inventory
- Minimum controls baseline
- Cloud controls compliance

Third-party management

- Evaluation and selection
- Risk-based tiering
- Contract and service initiation
- Ongoing monitoring
- Service termination

Workforce management

- Onboarding & off boarding
- Physical security
- Phishing exercises
- Security training and awareness
- Privileged user certification

Vigilant

Threat and vulnerability management

- Threat modeling and intelligence
- Penetration testing
- Vulnerability management
- Emerging threats identification
- Brand protection
- Cyber threat information sharing

Monitoring

- Security operations center (SOC)
- Security information and event management (SIEM)
- Cyber risk analytics
- User entity behavior analytics
- Continuous monitoring program

Resilient

Crisis management

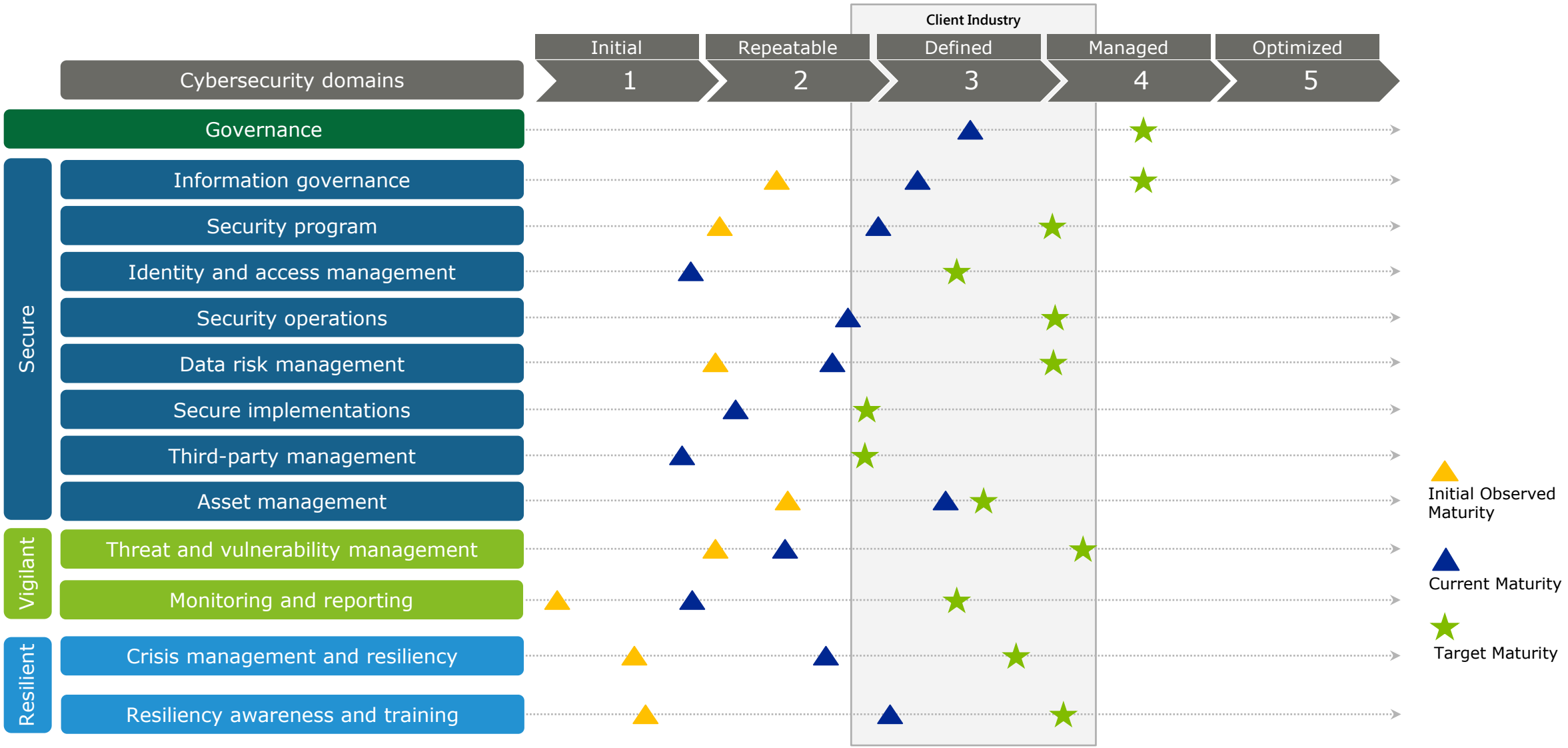
- Response planning
- Red team exercises
- Tabletop exercises
- Incident response and forensics
- Crisis communication plan
- Third-party responsibilities

Enterprise resiliency

- Business impact analysis (BIA)
- Business continuity planning (BCP)
- Disaster recovery planning (DRP)
- Cyber incident insurance

*The Deloitte Risk & Financial Advisory cyber internal audit framework is aligned with industry standards and maps to NIST, ISO, COSO, ITIL, and CIS CSC. Alternative frameworks may be used.

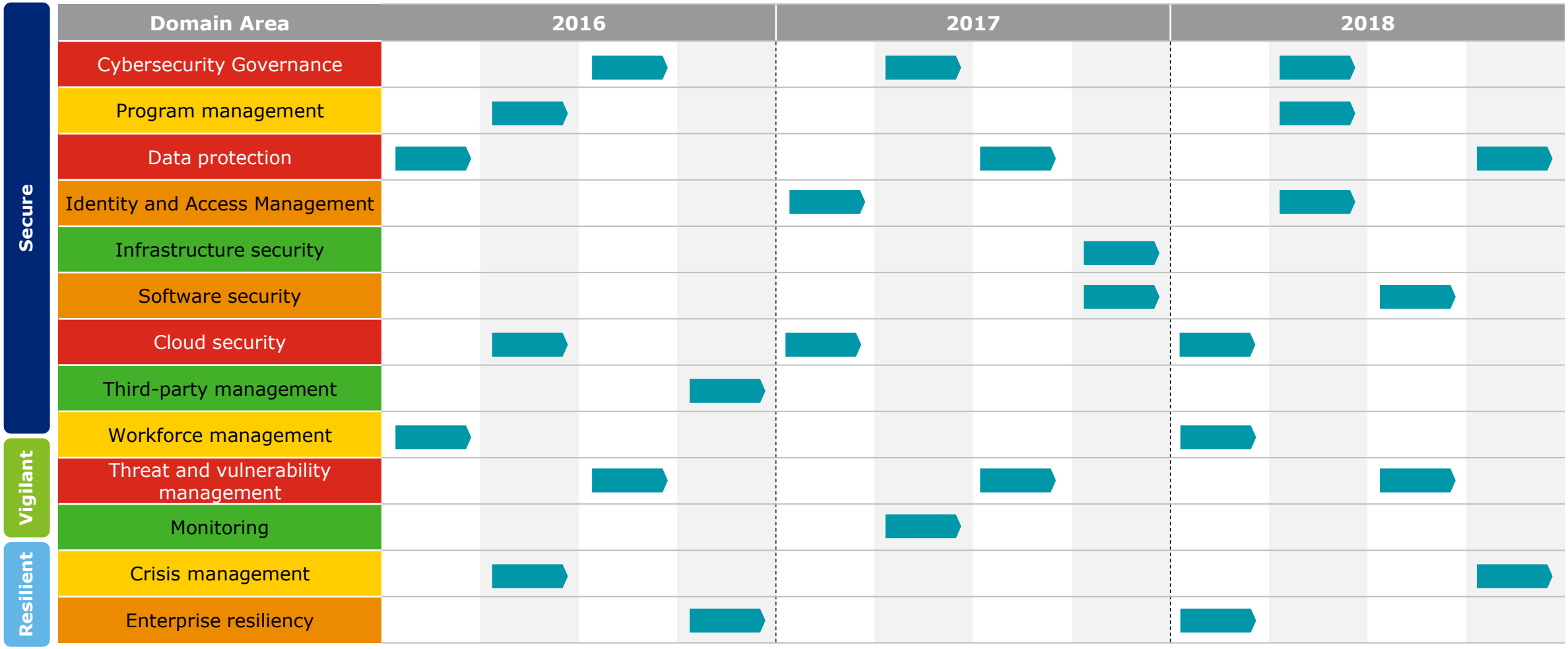
An example of a cyber maturity model assessment



Driving a multi-year cyber internal audit plan

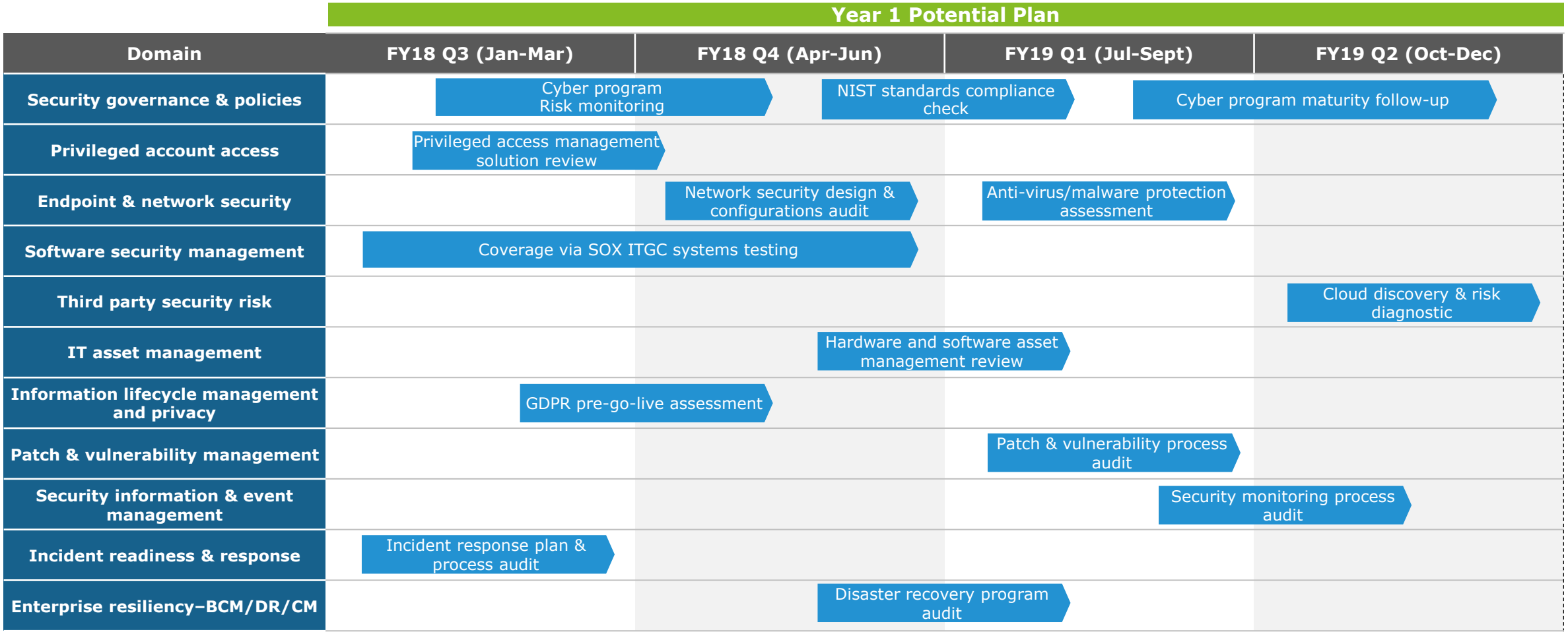
Develop a plan and re-assess it quarterly to maintain relevance and refine it as threats and regulatory requirements change

Illustrative and tailored example



Build an agile and risk-based cyber and IT IA plan for the organization

Illustrative and tailored example

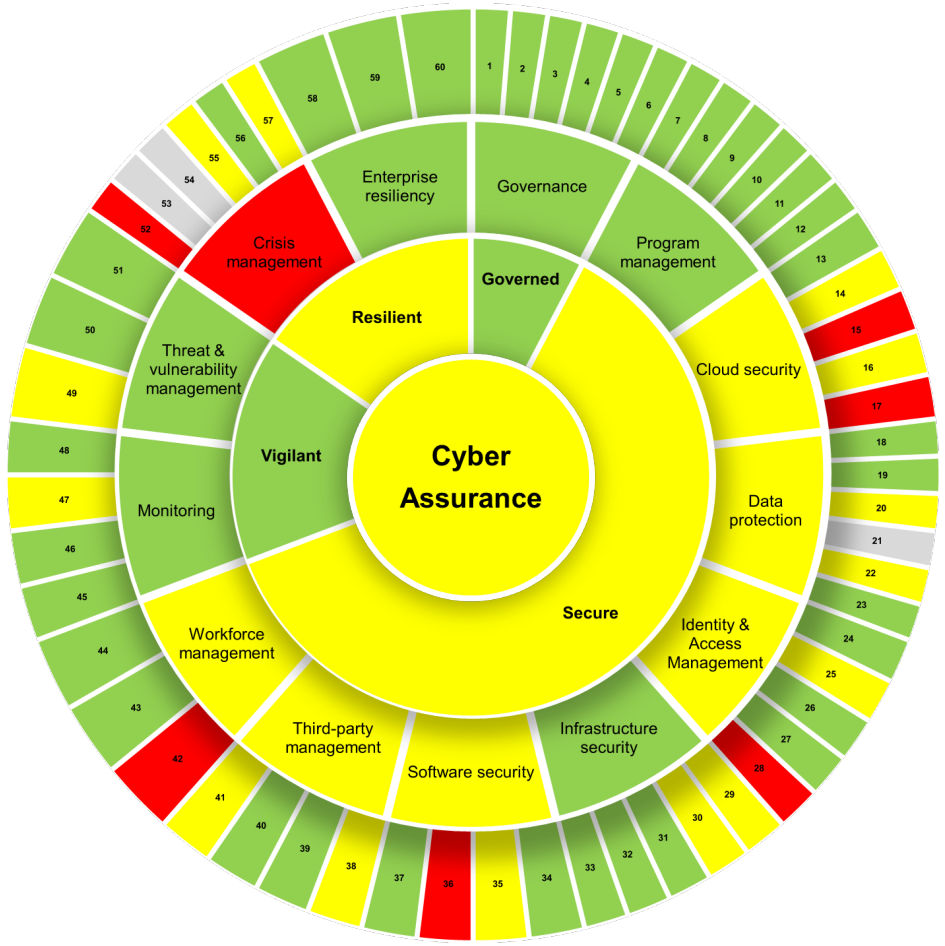


Reporting cyber and IT internal audit insights is different at different levels

- Allows stakeholders to communicate effectively
- Provides "at-a-glance" status update
- Customized for each group of stakeholders
- Tailored to individual company cyber frameworks

Board & C-Suite

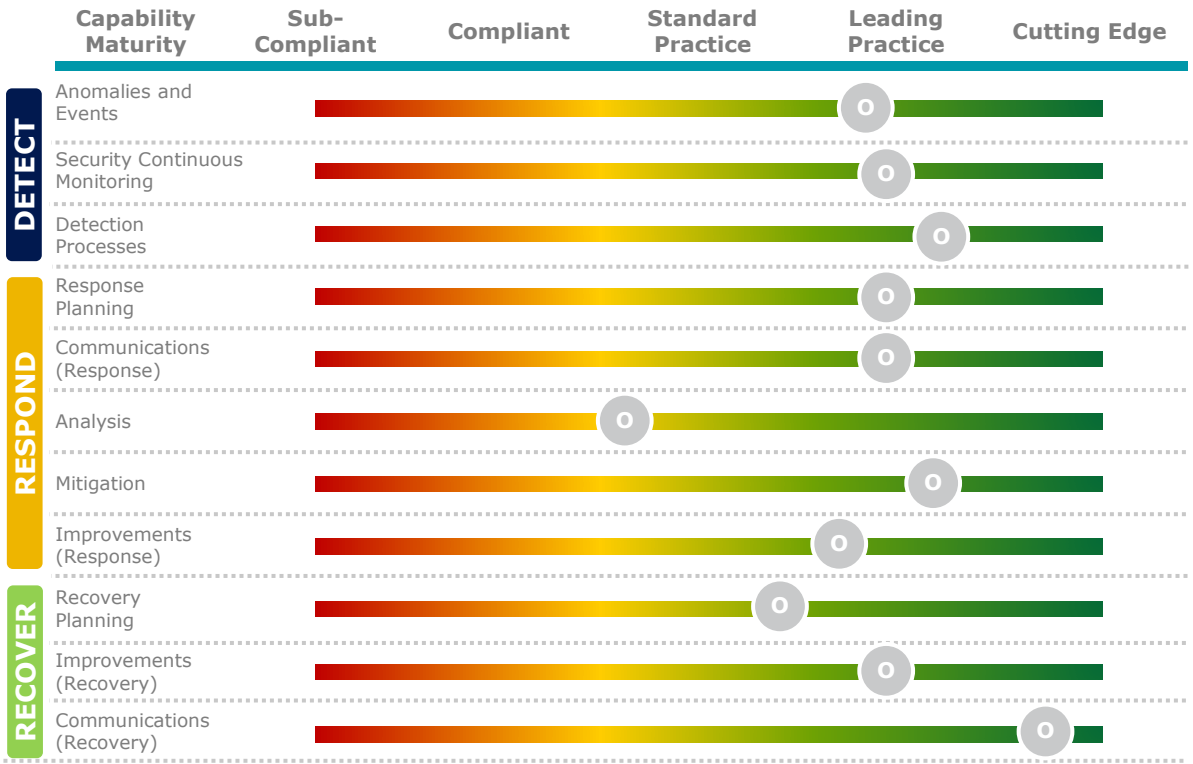
IT Steering Committee



IT Working Groups

Another example of tailored reporting of cyber IA assessment summary results

Current State Maturities



Maturity Definitions

Compliant

- The overall approach to managing cyber security and risk management is not strategic and often reactive
- Program focus is primarily on implementing isolated protective technologies
- Little or basic monitoring and recovery capabilities

Standard Practice

- Organization takes a consistent approach to cyber security governance and risk management in some parts of the enterprise
- Processes and controls are implemented in silos to prevent and monitor for cyber attacks
- Recovery from attacks is inconsistent and usually takes several days

Leading Practice

- Organization adopts a strategic and threat aligned approach to cyber security and risk management
- Advanced technologies and controls are deployed consistently to protect and detect attacks
- Recovery processes and capabilities are effective and enable recovery from most attacks in a few days

Cutting Edge

- Organization takes an innovative and research based approach to cyber security
- The organization often deploys customized controls and technologies to its ~~their~~ environment
- Ability to recover from most attacks and breaches in a matter of hours

Questions?

Chris Pattillo
Deloitte Advisory Manager
cpattillo@Deloitte.com

Deloitte.

This presentation contains general information only and Deloitte is not, by means of this presentation, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This presentation 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 shall not be responsible for any loss sustained by any person who relies on this presentation.