Deloitte.

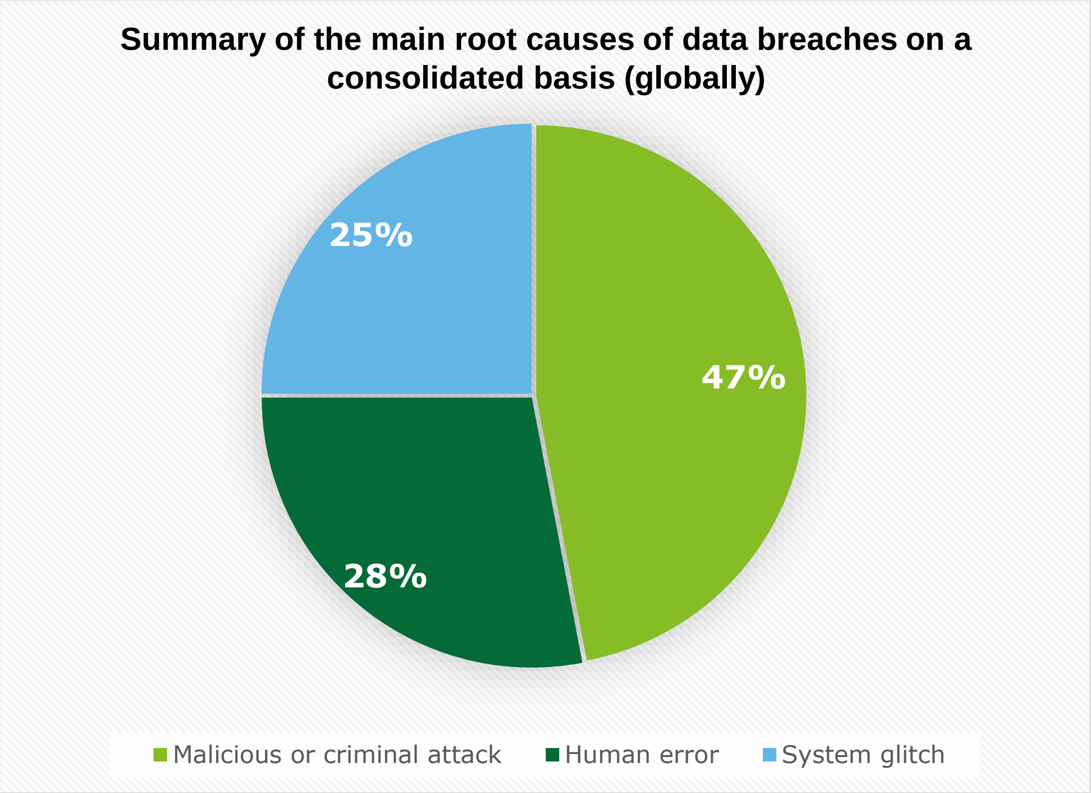
SOC for Cybersecurity

An overview of the AICPA's cybersecurity attestation reporting framework

December 2018

Data breaches are not stopping despite significant investments both globally and in the U.S.

Total spent on Cyber Security in 2017[1]	Likelihood of a recurring material data breach (within 2 years)	Average cost per compromised record	Cost of lost business (US)	Average time to identify a breach
$89.1 Billion	***27.7%***	***$141***	***$4.13 Million***	***191 Days***



Summary of the main root causes of data breaches on a consolidated basis (globally)

- ✓ The number of cyber-related attacks and breaches continues to grow
- ✓ The average cost of cybercrime incurred by companies across major industries continues to grow
- ✓ New and emerging risks are introduced daily
- ✓ A variety of recent legislation related to cybersecurity reporting and disclosures

Sources:

1. Gartner Press Release, Gartner Forecasts Worldwide Security Spending Will Reach $96 Billion in 2018, Up 8 Percent from 2017, December 2017 https://www.gartner.com/newsroom/id/3836563

2. Ponemon Institute and IBM Security, 2017 Cost of Data Breach Study: Global Overview https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03130WWEN&

Recent remarks on cybersecurity

While our digital world brings about extraordinary benefits, it also presents us with significant risks. The following are just a handful of recent sound bytes that not only reinforce this but also call attention to how this is much more than a technology concern and one that extends to the culture and core values of an organization.

> *While companies and shareholders agree that cybersecurity is one of the most prominent corporate issues of our time, it is unclear why companies are not doing more to implement robust cybersecurity frameworks and to provide meaningful disclosures regarding the risks of data loss*
>
> **SEC Commissioner, Kara Stein**
> https://www.sec.gov/news/speech/speech-stein-021318

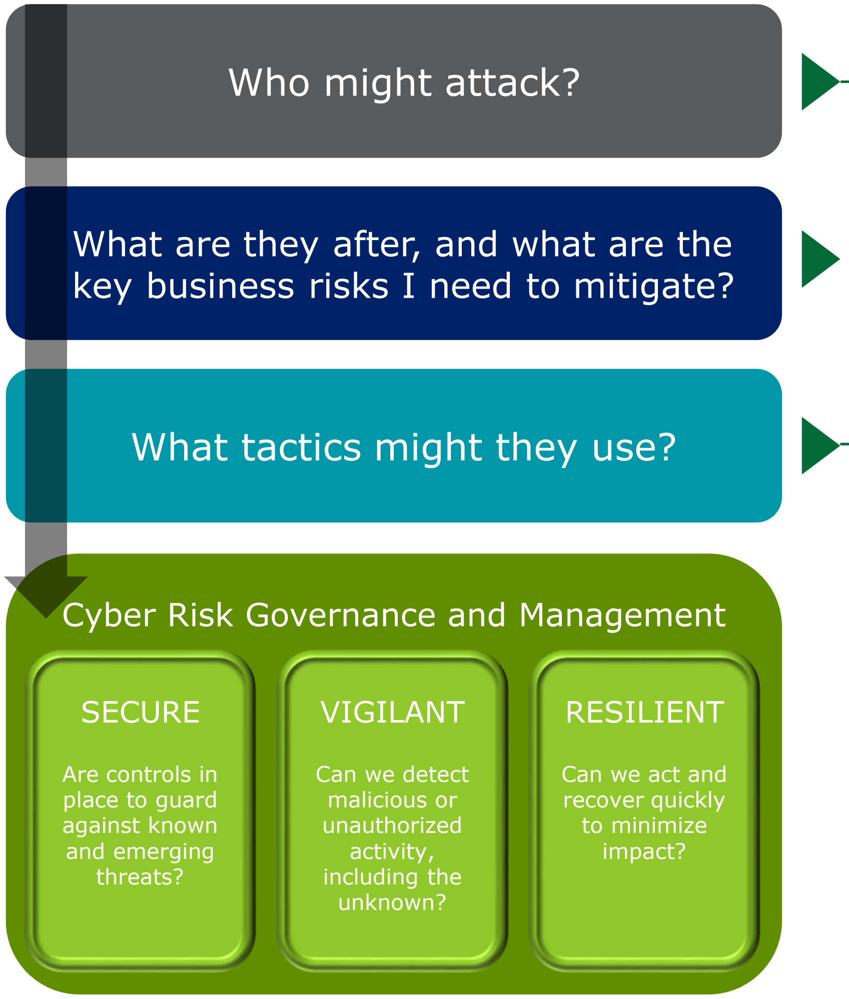
> *We encourage companies to adopt comprehensive policies and procedures related to cybersecurity and to assess their compliance regularly, including the sufficiency of their disclosure controls and procedures as they relate to cybersecurity disclosure.*
>
> **SEC's Statement and Guidance on Public Company Cybersecurity Disclosures (17 CFR Parts 229 and 249)**
> https://www.sec.gov/rules/interp/2018/33-10459.pdf

> *We need to arm corporate boards with a mechanism to thoughtfully assess management's assertions about the design and effectiveness of their organizations' cyber defenses.*
>
> **Former Deputy Secretary of the US Department of Treasury, Sarah Bloom Raskin**
> https://www.treasury.gov/press-center/press-releases/Pages/jl0685.aspx

> *Cybercrime is an enterprise-level risk that will require an interdisciplinary approach, significant investments of time and talent by senior leadership and board-level attention*
>
> **SEC Commissioner Robert Jackson**
> https://www.sec.gov/news/speech/speech-jackson-cybersecurity-2018-03-15

> *We believe the best way for industry to focus on the threat of cyber security is to have a consistent framework*
>
> **NYDFS Superintendent, Maria Vullo, at a 2017 NAIC meeting**
> https://www.insurancejournal.com/news/national/2017/04/10/447358.htm

Cyber threat landscape, vectors, and approaches



Who might attack?

What are they after, and what are the key business risks I need to mitigate?

What tactics might they use?

Cyber Risk Governance and Management

SECURE

Are controls in place to guard against known and emerging threats?

VIGILANT

Can we detect malicious or unauthorized activity, including the unknown?

RESILIENT

Can we act and recover quickly to minimize impact?

- Cyber criminals
- Hacktivists (agenda driven)
- Nation states
- Insiders / partners
- Competitors
- Skilled individual hacker

- Theft of intellectual property or strategic plans
- Financial fraud
- Reputation damage
- Business disruption
- Destruction of critical infrastructure
- Threats to health & safety

- Spear phishing, drive by download, etc.
- Software or hardware vulnerabilities
- Third-party compromise
- Multi-channel attacks
- Stolen credentials
- … and others

A framework for cybersecurity risk management

Industry leading practices and frameworks can be a valuable lens through which to evaluate an organization’s security posture, maturity, and areas of potential enhancement.

Inputs

Industry standards

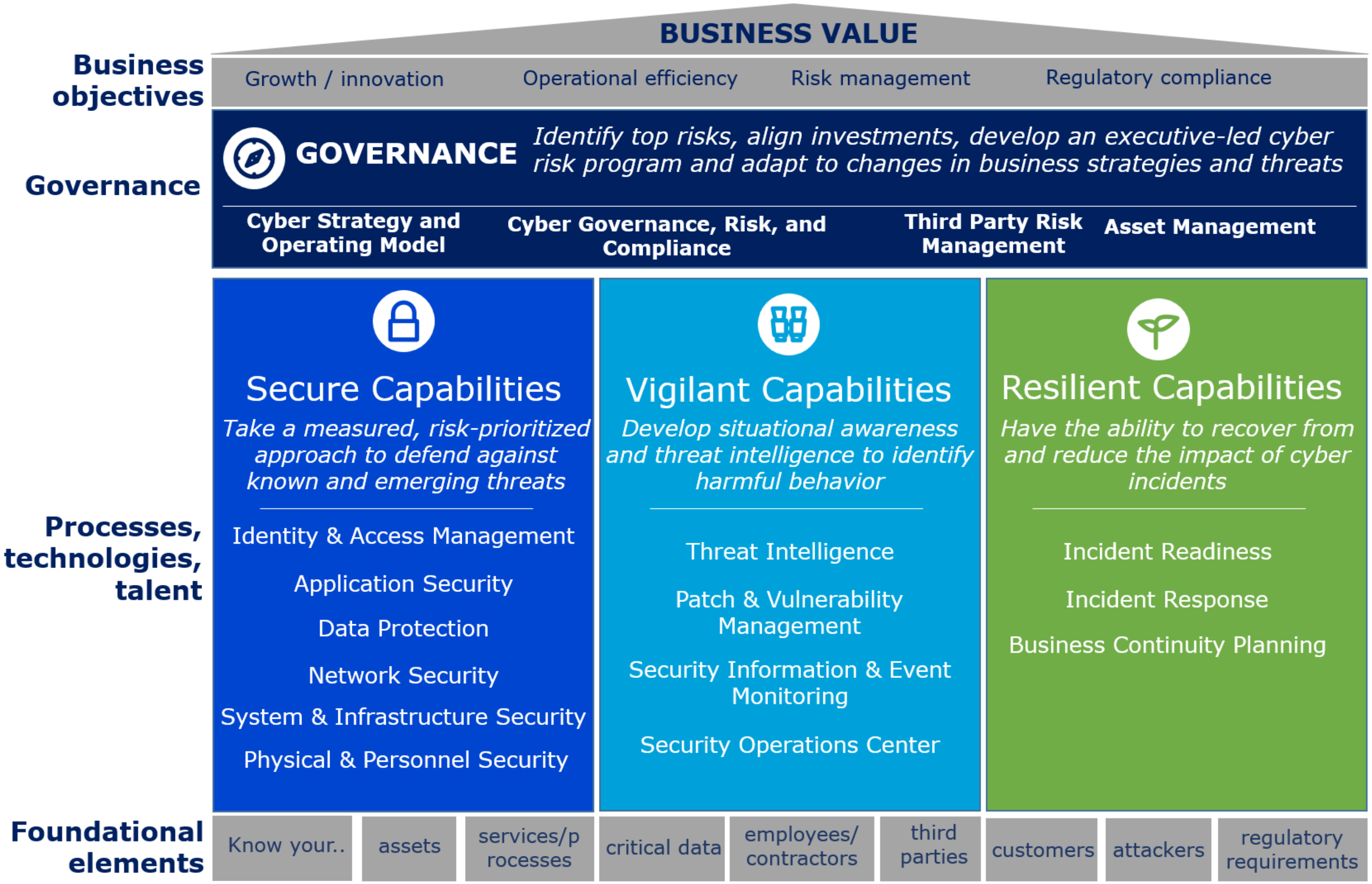
- ISO[4] 27001/2
- COBIT[5]
- NIST[6] cybersecurity framework
- Global privacy and data protection laws
- ITIL[7]

Leading practices

- Innovative cyber capabilities
- Practical knowledge by serving large clients
- Published industry research

Threat landscape

- Who might attack?
- What are they after?
- What tactics will they use?



BUSINESS VALUE

Business objectives: Growth / innovation · Operational efficiency · Risk management · Regulatory compliance

Governance

GOVERNANCE *Identify top risks, align investments, develop an executive-led cyber risk program and adapt to changes in business strategies and threats*

Cyber Strategy and Operating Model · **Cyber Governance, Risk, and Compliance** · **Third Party Risk Management** · **Asset Management**

Processes, technologies, talent

Secure Capabilities

Take a measured, risk-prioritized approach to defend against known and emerging threats

- Identity & Access Management
- Application Security
- Data Protection
- Network Security
- System & Infrastructure Security
- Physical & Personnel Security

Vigilant Capabilities

Develop situational awareness and threat intelligence to identify harmful behavior

- Threat Intelligence
- Patch & Vulnerability Management
- Security Information & Event Monitoring
- Security Operations Center

Resilient Capabilities

Have the ability to recover from and reduce the impact of cyber incidents

- Incident Readiness
- Incident Response
- Business Continuity Planning

Foundational elements: Know your.. · assets · services/processes · critical data · employees/ contractors · third parties · customers · attackers · regulatory requirements

[4] *International Organization for Standardization*

[5] Control Objectives for Information and Related Technologies

[6] *National Institute for Standards and Technology*

[7] *Formerly known as the Information Technology Infrastructure Library*

Recent regulatory and compliance drivers

Broad regulatory pressure to tighten controls and visibility around operational risk persists, including those associated with the effectiveness of cyber risk management programs, disclosures, third parties and fraud.

The New York State Department of Financial Services (“NYDFS”) issues finalized Cybersecurity Requirements (23 NYCRR 500) for financial services companies

The Office of Foreign Assets Control’s (“OFAC”) released sanctions regime to persons pursuing cyber-enabled activities

SWIFT issues Customer Security Controls Framework

The Federal Financial Institutions Examination Council (“FFIEC”) release of a cybersecurity tool called CAT—Cybersecurity Assessment Tool

The American Institute of Certified Public Accountants (“AICPA”) finalizes its cybersecurity risk management attestation reporting framework

The Securities and Exchange Commission (“SEC”) adopts interpretive guidance on public company cybersecurity disclosures and issues an investigative report on business email compromises

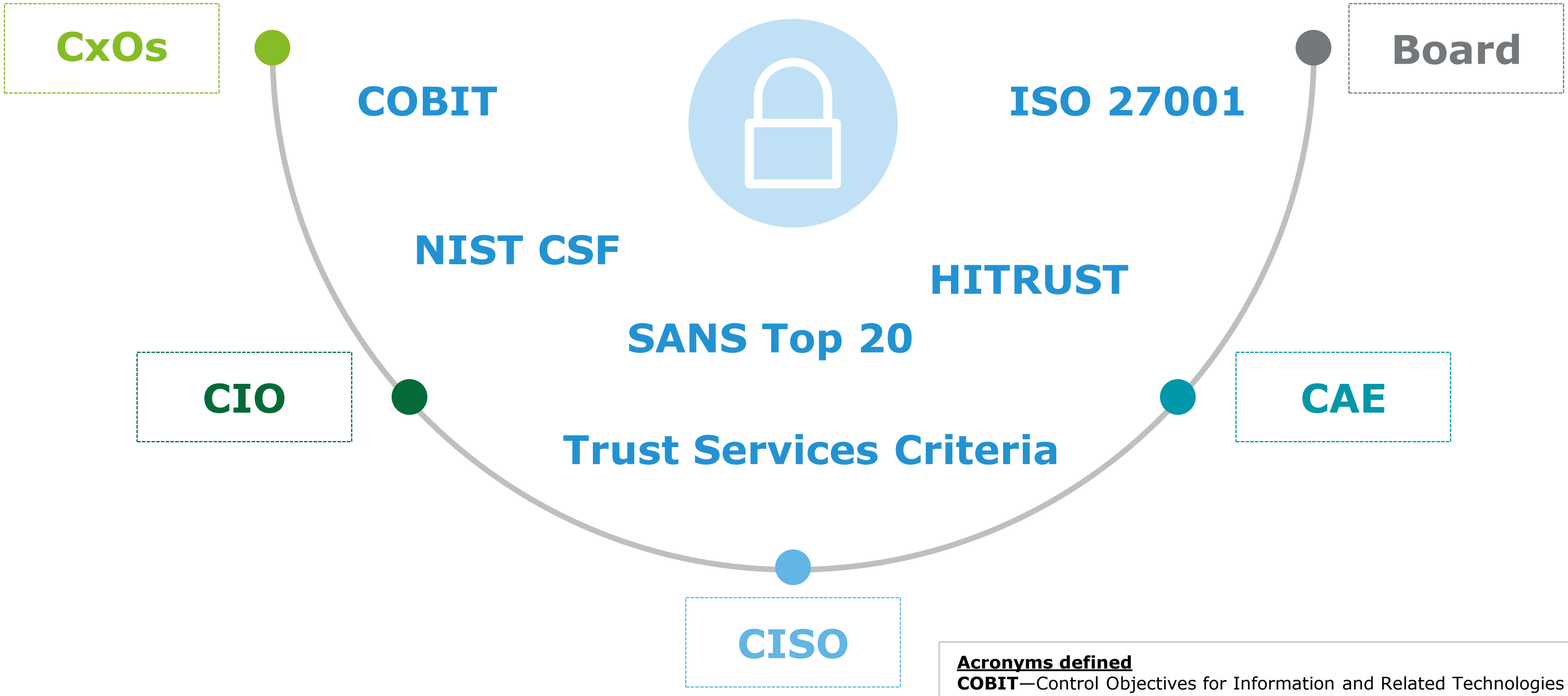
The Office of Compliance Inspections and Examinations (“OCIE”) Cybersecurity Examination Initiative to assess cybersecurity preparedness in the securities industry

The EU approves and adopts General Data Protection Regulation (“GDPR”) to harmonize data privacy laws across Europe

National Association of Insurance Commissioners (“NAIC”) adopts the Insurance Data Security Model Law

Measuring without a common yardstick can cause confusion

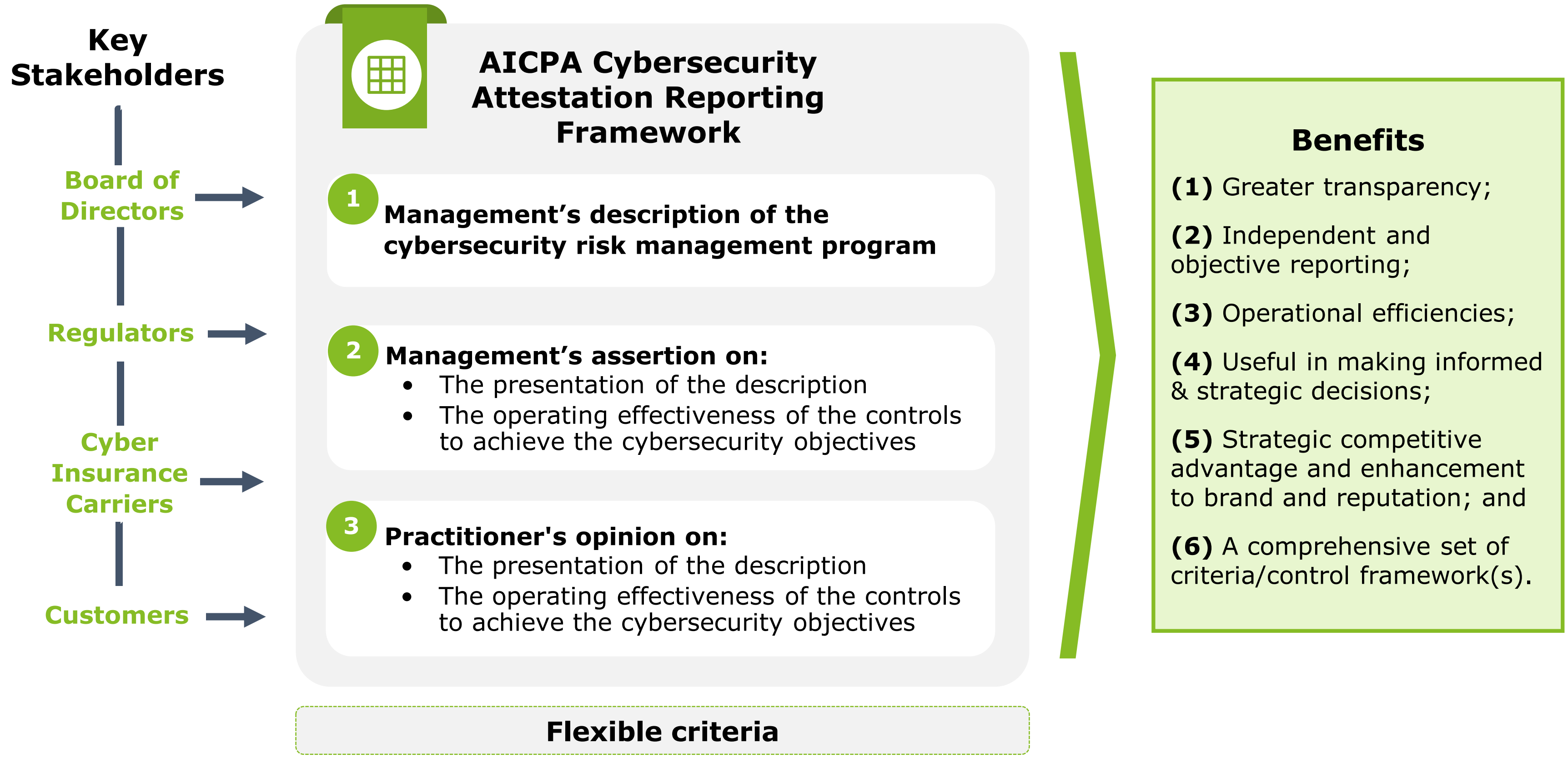
Having a mechanism that establishes a common underlying language for cybersecurity risk management reporting can help organizations more effectively evaluate their cyber programs and facilitate consistent and transparent communication both across the enterprise and to external stakeholder groups.



Acronyms defined
COBIT—Control Objectives for Information and Related Technologies
HITRUST – Health Information Trust Alliance
ISO—International Organization for Standardization
NIST CSF—National Institute of Standards and Technology Cybersecurity Framework
SANS - SysAdmin, Audit, Network and Security

AICPA’s cybersecurity attestation reporting framework

On April 24, 2017, the AICPA released its cybersecurity attestation reporting framework (SOC for Cybersecurity), which is intended to expand cyber risk reporting to address the marketplace need for uniformity and greater stakeholder transparency.



Key Stakeholders

- Board of Directors
- Regulators
- Cyber Insurance Carriers
- Customers

AICPA Cybersecurity Attestation Reporting Framework

1. **Management’s description of the cybersecurity risk management program**

2. **Management’s assertion on:**
   - The presentation of the description
   - The operating effectiveness of the controls to achieve the cybersecurity objectives

3. **Practitioner's opinion on:**
   - The presentation of the description
   - The operating effectiveness of the controls to achieve the cybersecurity objectives

Flexible criteria

Benefits

(1) Greater transparency;

(2) Independent and objective reporting;

(3) Operational efficiencies;

(4) Useful in making informed & strategic decisions;

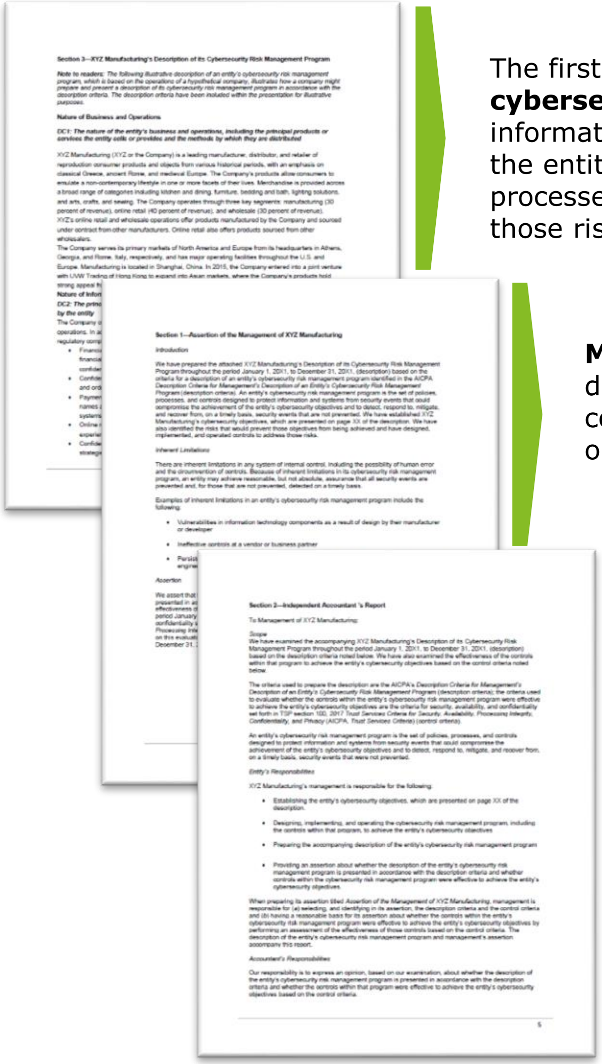
(5) Strategic competitive advantage and enhancement to brand and reputation; and

(6) A comprehensive set of criteria/control framework(s).

Source: *Description Criteria for Management’s Description of an Entity’s Cybersecurity Risk Management Program*
https://www.aicpa.org/InterestAreas/FRC/AssuranceAdvisoryServices/Pages/AICPACybersecurityInitiative.aspx

Contents of the report

Three sections make-up an entity's SOC for Cybersecurity report – (1) Management's description of its cybersecurity risk management program, (2) Management's assertion, and (3) the CPA firm's independent opinion.



Section 3—XYZ Manufacturing's Description of its Cybersecurity Risk Management Program

Note to readers: *The following illustrative description of an entity's cybersecurity risk management program, which is based on the operations of a hypothetical company, illustrates how a company might prepare and present a description of its cybersecurity risk management program in accordance with the description criteria. The description criteria have been included within the presentation for illustrative purposes.*

Nature of Business and Operations

DC1: The nature of the entity's business and operations, including the principal products or services the entity sells or provides and the methods by which they are distributed

XYZ Manufacturing (XYZ or the Company) is a leading manufacturer, distributor, and retailer of reproduction consumer products and objects from various historical periods, with an emphasis on classical Greece, ancient Rome, and medieval Europe. The Company's products allow consumers to emulate a non-contemporary lifestyle in one or more facets of their lives. Merchandise is provided across a broad range of categories including kitchen and dining, furniture, bedding and bath, lighting solutions, and arts, crafts, and sewing. The Company operates through three key segments: manufacturing (30 percent of revenue), online retail (40 percent of revenue), and wholesale (30 percent of revenue). XYZ's online retail and wholesale operations offer products manufactured by the Company and sourced under contract from other manufacturers. Online retail also offers products sourced from other wholesalers.

The Company serves its primary markets of North America and Europe from its headquarters in Athens, Georgia, and Rome, Italy, respectively, and has major operating facilities throughout the U.S. and Europe. Manufacturing is located in Shanghai, China. In 2015, the Company entered into a joint venture with UVW Trading of Hong Kong to expand into Asian markets, where the Company's products hold strong appeal fr

Nature of Infor

DC2: The princ
by the entity

The Company o
operations. In a
regulatory comp

- Financi
  financia
  confider
- Confide
  and ord
- Paymen
  names
  systems
- Online
  experie
- Confide
  strategi

Section 1—Assertion of the Management of XYZ Manufacturing

Introduction

We have prepared the attached XYZ Manufacturing's Description of its Cybersecurity Risk Management Program throughout the period January 1, 20X1, to December 31, 20X1, (description) based on the criteria for a description of an entity's cybersecurity risk management program identified in the AICPA *Description Criteria for Management's Description of an Entity's Cybersecurity Risk Management Program* (description criteria). An entity's cybersecurity risk management program is the set of policies, processes, and controls designed to protect information and systems from security events that could compromise the achievement of the entity's cybersecurity objectives and to detect, respond to, mitigate, and recover from, on a timely basis, security events that are not prevented. We have established XYZ Manufacturing's cybersecurity objectives, which are presented on page XX of the description. We have also identified the risks that would prevent those objectives from being achieved and have designed, implemented, and operated controls to address those risks.

Inherent Limitations

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of inherent limitations in its cybersecurity risk management program, an entity may achieve reasonable, but not absolute, assurance that all security events are prevented and, for those that are not prevented, detected on a timely basis.

Examples of inherent limitations in an entity's cybersecurity risk management program include the following:

- Vulnerabilities in information technology components as a result of design by their manufacturer or developer
- Ineffective controls at a vendor or business partner
- Persist
  engine

Assertion

We assert that
presented in a
effectiveness o
period January
confidentiality
Processing Inte
on this evaluat
December 31, 2

Section 2—Independent Accountant 's Report

To Management of XYZ Manufacturing:

Scope

We have examined the accompanying XYZ Manufacturing's Description of its Cybersecurity Risk Management Program throughout the period January 1, 20X1, to December 31, 20X1, (description) based on the description criteria noted below. We have also examined the effectiveness of the controls within that program to achieve the entity's cybersecurity objectives based on the control criteria noted below.

The criteria used to prepare the description are the AICPA's *Description Criteria for Management's Description of an Entity's Cybersecurity Risk Management Program* (description criteria); the criteria used to evaluate whether the controls within the entity's cybersecurity risk management program were effective to achieve the entity's cybersecurity objectives are the criteria for security, availability, and confidentiality set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*) (control criteria).

An entity's cybersecurity risk management program is the set of policies, processes, and controls designed to protect information and systems from security events that could compromise the achievement of the entity's cybersecurity objectives and to detect, respond to, mitigate, and recover from, on a timely basis, security events that were not prevented.

Entity's Responsibilities

XYZ Manufacturing's management is responsible for the following:

- Establishing the entity's cybersecurity objectives, which are presented on page XX of the description.
- Designing, implementing, and operating the cybersecurity risk management program, including the controls within that program, to achieve the entity's cybersecurity objectives
- Preparing the accompanying description of the entity's cybersecurity risk management program
- Providing an assertion about whether the description of the entity's cybersecurity risk management program is presented in accordance with the description criteria and whether controls within the cybersecurity risk management program were effective to achieve the entity's cybersecurity objectives

When preparing its assertion titled *Assertion of the Management of XYZ Manufacturing*, management is responsible for (a) selecting, and identifying in its assertion, the description criteria and the control criteria and (b) having a reasonable basis for its assertion about whether the controls within the entity's cybersecurity risk management program were effective to achieve the entity's cybersecurity objectives by performing an assessment of the effectiveness of those controls based on the control criteria. The description of the entity's cybersecurity risk management program and management's assertion accompany this report.

Accountant's Responsibilities

Our responsibility is to express an opinion, based on our examination, about whether the description of the entity's cybersecurity risk management program is presented in accordance with the description criteria and whether the controls within that program were effective to achieve the entity's cybersecurity objectives based on the control criteria.

5

The first component is a **management-prepared narrative description of the entity's cybersecurity risk management program**. This description is designed to provide information about how the entity identifies its most sensitive information, the ways in which the entity manages the cybersecurity risks that threaten it, and the key security policies and processes implemented and operated to protect the entity's information assets against those risks.

Management's assertion — Management provides an assertion about whether the description is presented in accordance with the description criteria and whether the controls within the program were effective to achieve the entity's cybersecurity objectives based on the control criteria.

The practitioner's opinion — The final component in the reporting framework is the CPA's opinion on the description and on the effectiveness of controls within that program.

Sources: https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/illustrative-cybersercurity-risk-management-report.pdf

https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/cybersecurity-fact-sheet.pdf

Management's description

Management's description is intended to provide users of the report with information that can help them understand the entity's cybersecurity risks and how it manages those risks.

REVISED & EXPANDED

Trust Services Criteria for **Security, Availability,** Processing Integrity**, Confidentiality,** and Privacy

NEW

Description Criteria for **management's description** of the entity's cybersecurity risk management program

Description Criteria for management's description of the entity's cybersecurity risk management program:

Presents criteria established by the Assurance Services Executive Committee (ASEC) of the AICPA for use by ***(a)*** management, when preparing a description of an entity's cybersecurity risk management program, and ***(b)*** practitioners when evaluating that description, in connection with services performed on an entity's cybersecurity risk management program.

Applicability and use of description criteria:

- Examination of an entity's cybersecurity risk management program
- Consulting services

Suitability and availability of the description criteria:

- Relevance
- Objectivity
- Measurability
- Completeness

Categories of description criteria:

- Nature of business and operations
- Nature of information at risk
- Cybersecurity risk management program objectives (cybersecurity objectives)
- Factors that have a significant effect on inherent cybersecurity risks
- Cybersecurity risk governance structure
- Cybersecurity risk assessment process
- Cybersecurity communications and the quality of cybersecurity information
- Monitoring of the cybersecurity risk management program
- Cybersecurity control processes

Source: *Description Criteria for Management's Description of an Entity's Cybersecurity Risk Management Program*
https://www.aicpa.org/InterestAreas/FRC/AssuranceAdvisoryServices/Pages/AICPACybersecurityInitiative.aspx

Satisfying the needs of a variety of users

Stakeholders can benefit from a SOC for Cybersecurity report in a number of ways.

Board of Directors

Board-level reporting: The Board of Directors (including Audit Committee), and Senior Management have an important oversight role relative to cybersecurity. They need to be able to establish appropriate oversight of the company’s cybersecurity risk management program, including the controls within that program to: 1) **thoughtfully assess management’s assertions** about the design and effectiveness of the company’s cybersecurity defenses; and 2) **credibly and understandably communicate related findings** to key stakeholders: like investors, counterparties, customers, regulators, and the public, as appropriate.

Regulators

Regulatory pressures: The **NYDFS cybersecurity regulation** (effective March 1, 2017) for banks and insurers requires each company (“covered entity”) to assess its specific cybersecurity risk profile and design a program based on a series of specific requirements that addresses its risks in a robust fashion. A “covered entity” will need to certify to its compliance with the NYDFS on an annual basis.

On February 20, 2018, the **SEC issued interpretative** guidance (to expand upon its 2011 guidance) to assist public companies when preparing disclosures about cybersecurity risks and incidents. It also conveys the Commission’s views on the importance of maintaining comprehensive cybersecurity policies and procedures and the application of insider trading prohibitions in the context of cybersecurity.

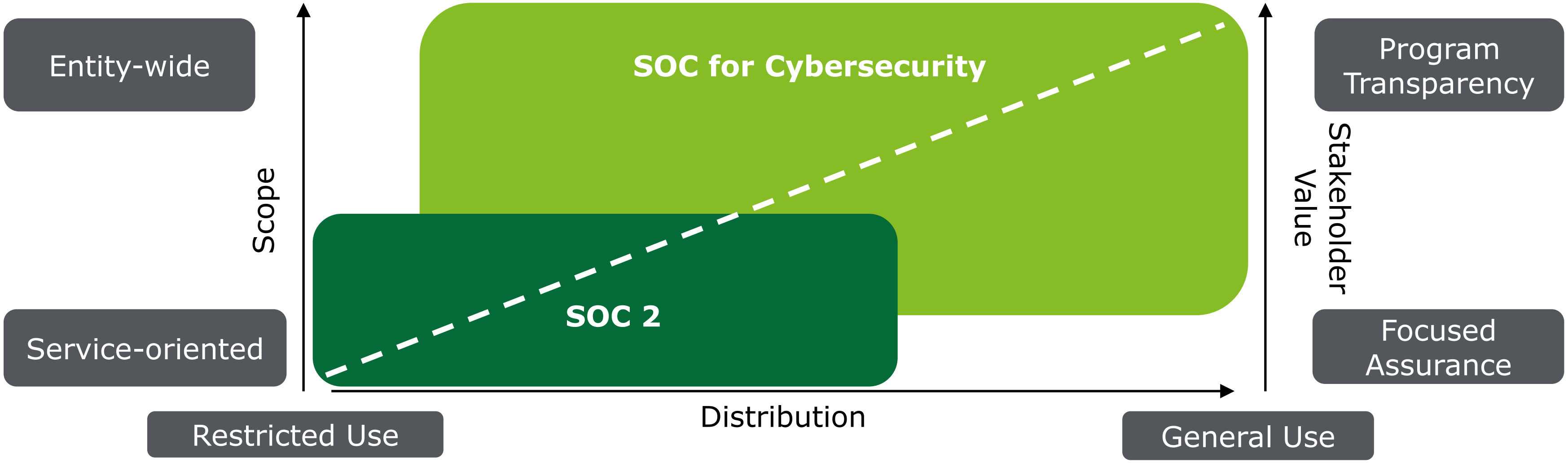
Customers

Customers & prospective customers: Clients and potential clients of service organizations want to be sure that they are outsourcing tasks to an organization that takes cybersecurity as a serious matter and are addressing the relevant risks associated with the outsourcing of a function to a service organization.

Cyber Insurance

Cyber insurance: A Cybersecurity Risk Management Examination report can potentially be leveraged by insurance carriers during the underwriting and risk assessment process by providing useful information about an entity’s (customer’s) cybersecurity risk management program, including the controls within that program, contributing to effective determination of coverage needs and policy pricing.

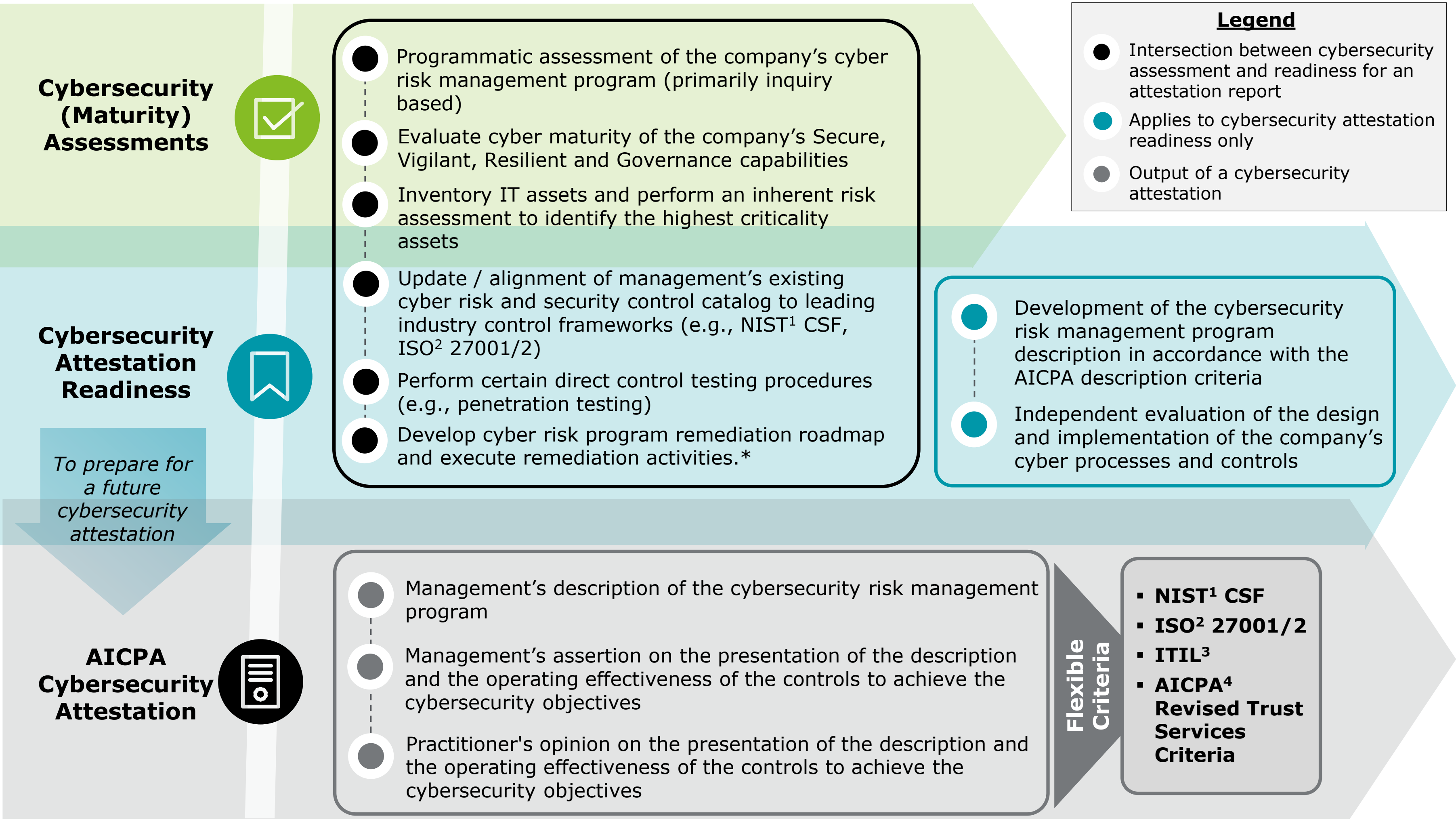
Comparison between SOC 2 & SOC for Cybersecurity



	SOC for Cybersecurity reporting	SOC 2 engagement
Purpose	Provide a variety of users with information about an entity's cybersecurity risk management program	Provide existing or prospective customers (system users) with information about controls at a service organization related to the Trust Services Criteria
Intended users	Management, directors, regulators, analysts and third parties	Management of the service organization and other specified parties with sufficient knowledge and understanding of the system
Criteria	Flexible (NIST CSF, 800-53, ISO 27001, etc.)	Trust Services Criteria
Report contents	Description of the cybersecurity risk management program, management assertion, and CPA firm's opinion	Description of the service organization's system, management assertion, practitioner's opinion, and description of tests of controls and results

Cybersecurity Assessments

There are various types of cyber assessments we perform as a firm. Cybersecurity attestation readiness to prepare for a future attestation is complementary to other services that we provide today. Depending on the company's overall cybersecurity maturity and key drivers (board oversight, regulation, response to an event, etc.) influencing the direction of the cyber program, there are options to understand the company's existing cyber capabilities.



Legend

- ● Intersection between cybersecurity assessment and readiness for an attestation report
- 🔵 Applies to cybersecurity attestation readiness only
- ⚪ Output of a cybersecurity attestation

Cybersecurity (Maturity) Assessments

Cybersecurity Attestation Readiness

To prepare for a future cybersecurity attestation

AICPA Cybersecurity Attestation

- ● Programmatic assessment of the company's cyber risk management program (primarily inquiry based)
- ● Evaluate cyber maturity of the company's Secure, Vigilant, Resilient and Governance capabilities
- ● Inventory IT assets and perform an inherent risk assessment to identify the highest criticality assets
- ● Update / alignment of management's existing cyber risk and security control catalog to leading industry control frameworks (e.g., NIST[1] CSF, ISO[2] 27001/2)
- ● Perform certain direct control testing procedures (e.g., penetration testing)
- ● Develop cyber risk program remediation roadmap and execute remediation activities.*

- 🔵 Development of the cybersecurity risk management program description in accordance with the AICPA description criteria
- 🔵 Independent evaluation of the design and implementation of the company's cyber processes and controls

- ⚪ Management's description of the cybersecurity risk management program
- ⚪ Management's assertion on the presentation of the description and the operating effectiveness of the controls to achieve the cybersecurity objectives
- ⚪ Practitioner's opinion on the presentation of the description and the operating effectiveness of the controls to achieve the cybersecurity objectives

Flexible Criteria

- **NIST[1] CSF**
- **ISO[2] 27001/2**
- **ITIL[3]**
- **AICPA[4] Revised Trust Services Criteria**

Note: [1] *National Institute for Standards and Technology;* [2] *International Organization for Standardization;* [3] *Information Technology Infrastructure Library;* [4] *American Institute of Certified Public Accountants*

* *D&T cannot provide remediation services to audit clients with the exception of providing input into management's remediation plan.*

Inherent limitations of a cybersecurity risk management examination engagement

Inherent limitations (language included in illustrative practitioner's report/opinion)

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. Because of inherent limitations in its cybersecurity risk management program, an entity may achieve reasonable, but not absolute, assurance that all security events are prevented and, for those that are not prevented, detected on a timely basis.

Examples of inherent limitations in a cybersecurity risk management program include the following:

- Vulnerabilities in information technology components as a result of design by their manufacturer or developer
- Ineffective controls at a vendor or business partner
- Persistent attackers with the resources to use advanced technical means and sophisticated social engineering techniques specifically targeting the entity

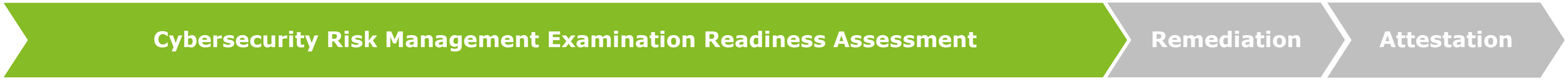
Furthermore, projections of any evaluation of effectiveness to future periods are subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

The AICPA guide, *Reporting on an Entity's Cybersecurity Risk Management Program and Controls,* acknowledges the following as a fundamental tenet of cybersecurity: *an entity that operates in cyberspace is likely to experience one or more security events or breaches at some point in time, regardless of the effectiveness of the entity's cybersecurity controls.* Understanding this tenet is essential to dispelling user misconceptions that an effective cybersecurity risk management program will prevent all security events from occurring. In fact, because of inherent limitations in its cybersecurity risk management program, an entity may achieve reasonable, but not absolute, assurance that security events are prevented and, for those not prevented, that they are detected, responded to, mitigated against, and recovered from on a timely basis. In other words, an effective cybersecurity risk management program is one that enables the entity to detect security events on a timely basis and to respond to and recover from such events with minimal disruption to the entity's operations.

Source: AICPA Guide: Reporting on an Entity's Cybersecurity Risk Management Program and Controls

Preparing for a future cybersecurity examination

Given the varying levels of maturity of cybersecurity risk management programs, performing a cybersecurity examination readiness assessment prior to embarking on an attestation is key. The cybersecurity risk management examination readiness assessment approach consists of the following phases and key activities.:



Cybersecurity Risk Management Examination Readiness Assessment

Risk Assessment (Phase 1): Advise management in performing a cybersecurity risk assessment, including an inherent risk assessment to identify the highest criticality assets and update/align the company's existing IT risk & control catalog to leading industry control frameworks (e.g., NIST-CSF, ISO 270001/2, or Revised AICPA Trust Services Criteria (TSC), etc.).

Description of the Entity's Cybersecurity Risk Management Program & Execute Controls Assessment (Phases 1 and 2): Provide advice and recommendations for management's consideration on the company's efforts in developing the description of the their cybersecurity risk management program in accordance with the description criteria developed by the AICPA for use when preparing and evaluating the description of the entity's cybersecurity risk management program, based on internal controls and process documentation that has already been developed, prepared or created by company management.

Conduct Gap Analysis (Phase 2): Assess the design and implementation of the current state of internal controls included within the company's cybersecurity risk management program against a leading industry control framework (e.g., NIST-CSF, ISO 27001/2, or Revised AICPA Trust Services Criteria (TSC), etc.). Prepare a gap analysis report consisting of: 1) the company's current state cybersecurity controls, designed and implemented by management; 2) potential internal control gaps / observations identified; and 3) advice and recommendations for management's consideration to address the potential internal control gaps identified.

Remediation Roadmap (Phase 2): Review management's remediation plan to address the internal control gaps identified and provide advice and recommendations for management's consideration.

Remediation

Management to execute on remediation activities

Attestation

Assure: Engage an independent third-party audit firm to execute a Cybersecurity Risk Management Examination engagement in accordance with the new AICPA attestation reporting framework.

As used in this document, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Q&A

Contact Information

Gaurav Kumar
Principal | Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
gukumar@deloitte.com
+1 212 436 2745

Jeff Schaeffer
Managing Director | Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
jschaeffer@deloitte.com
+1 973 223 4864

Charlie Willis
Managing Director| Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
chwillis@deloitte.com
+1 215 299 4534

Tony DiLiberto
Manager | Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
tdiliberto@deloitte.com
+1 708 224 1776

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.

U.S. PARALYMPICS

Official Professional Services Sponsor

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

As used in this document, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.