Cybersecurity reporting

Trust, but verify

A new reporting option is now available to improve stakeholder communication relative to cybersecurity risk management

Building a better working world

Board members, investors, business partners; finally, an option for them to obtain greater transparency, clarity and assurance relative to an entity's cybersecurity risk management program.

Overview

1

The AICPA has developed a new reporting model and set of evaluation criteria for evaluating and reporting on an entity's cybersecurity risk management program.

2

The reporting model and criteria, which are flexible, scalable and comprehensive, facilitate the consistent communication of relevant, validated information to stakeholders and decision-makers to enable them to make informed decisions relative to cybersecurity risk.

3

Criteria will soon be available to allow for:

- Enhanced reporting/evaluation of service organizations
- New reporting/evaluation of supply chain vendors

Background

In recent years, the marketplace has experienced numerous technological and operational advancements. As a result, today:

- Most critical business-related information is retained (and accessible) electronically.
- Most technology devices are (or have the ability to be) networked and potentially accessible from anywhere in the world.
- Most: key business controls (e.g., calculations, postings, exception reporting, summarizations, approvals) and key operational controls are automated and are dependent upon the accuracy and integrity of computer processing.

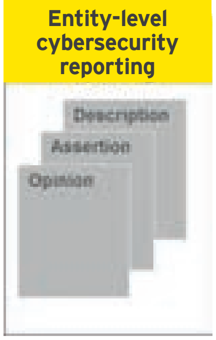
Similarly:

- An ever-expanding list of key business and operational/support services are being outsourced.
- Companies are more dependent than ever on supply chain vendors to manufacture and distribute their goods in a timely manner.

The benefits of these advancements, however, are threatened by concerns raised from the cyber attacks that continue to plague the marketplace. While many organizations have continued to mature their cybersecurity risk management programs to lessen the likelihood and impact of these attacks, there has not been an effective means for providing stakeholders (e.g., board members, investors, business partners) with an objective and comprehensive evaluation of these programs.

Cybersecurity reporting

Doveryai, no proveryai (trust, but verify)



This old Russian proverb, which was made popular during the Reagan/Gorbachev nuclear disarmament talks in the mid-1980s, is also applicable today as stakeholders struggle to understand and evaluate the impact of cybersecurity risk. While stakeholders have an underlying trust in the information they have historically been provided by management regarding an entity's efforts to manage cybersecurity risk, they still desire:

- A heightened level of visibility/transparency into the effectiveness of the cybersecurity risk management program implemented across the entity
- Clarity into the alignment of the program with leading practices and its ability to prevent and/or detect, respond and recover from a significant cyber breach
- Assurance as to the integrity of the information provided

Building upon its historical role in the marketplace of providing trust and confidence in the financial markets, the American Institute of Certified Public Accountants (AICPA) undertook an effort to satisfy these stakeholder needs. Specifically, the AICPA developed a reporting model and evaluation framework that was flexible, scalable and comprehensive and that facilitated the consistent communication of relevant, validated information to stakeholders and decision-makers to enable them to make informed decisions relative to cybersecurity risk.

The new reporting model includes a management's assertion and auditor's opinion to support the integrity of management's description and provides assurance over: (1) the completeness and accuracy of management's description of its cybersecurity risk management program and (2) the operational effectiveness of the supporting controls.

Management's description is intended to provide transparency into key elements of an organization's cybersecurity risk management program based on defined criteria. These key elements include an overview of:

- The nature of the entity's business and operations
- The nature of the information at risk
- The cybersecurity risk management program objectives (i.e., the objectives that the program has been designed to achieve)

[1] Reporting at the entity level includes the entire corporate environment and all IT assets connected to the enterprise network.

The cybersecurity reporting criteria have multiple uses; in addition to serving as a basis for attestation reporting, it can also be used internally by management teams as a basis for designing and implementing a cybersecurity risk management program, or self-evaluating the adequacy of an existing program.

- Factors that have a significant effect on inherent cybersecurity risks
- The entity's cybersecurity risk governance structure
- The entity's cybersecurity risk assessment processes
- The entity's approach to communicating its cybersecurity objectives, exceptions, etc., to internal and external users
- The entity's process for monitoring and assessing the effectiveness of controls including in its cybersecurity risk management program

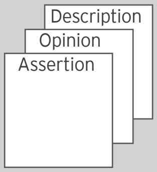
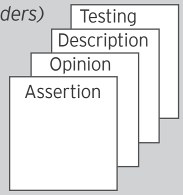
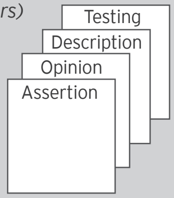
The purpose of the criteria is to help ensure a consistent level of content is included in management's description of the entity's cybersecurity risk management program and evaluation of the entity's program by the independent auditor.[3]

Three reporting levels

In addition to the preparation of cybersecurity reporting at the entity level, two additional levels of reporting were determined to be needed due to the expanded focus on vendor and supply chain risk management activities by the market both of which will leverage the new evaluation criteria:

- Updated reporting at the service provider-level (i.e., updating existing SOC 2 guidance)
- New reporting at the supply-chain level[4]

The table below summarizes the intended audience for each level of reporting, along with the associated benefits:

Reporting levels	Intended audience	Benefits (entity and recipient)
‣ Entity 	‣ Board/audit committee ‣ Management ‣ Investors ‣ Regulators ‣ Analysts	‣ Provides transparency to key elements of the entity's cyber risk management program ‣ Improves communications ‣ Enhances confidence in the integrity of information presented
‣ Service provider *(SOC 2 for Service providers)* 	‣ Business unit management ‣ Vendor risk management ‣ Accounting/Internal audit ‣ Chief Information Security Officer ‣ Business continuity planning	‣ In addition to entity level benefits, provides sufficient, detailed information to address the users, vendor risk management needs
‣ *Supply chain (SOC 2 for Supply chain vendors)* 	‣ Business unit management ‣ Supplier risk management ‣ Accounting/internal audit ‣ Chief Information Security Officer ‣ Business continuity planning	‣ In addition to entity-level benefits, provides sufficient, detailed information to address the user's supply chain risk management needs

[3] Management's assertion and the auditor's opinion relate to whether processes and controls within the organization's cybersecurity risk management program have been properly designed and operating effectively when evaluated against the evaluation criteria. An unqualified opinion is not intended to imply that a successful attack cannot occur; rather, that reasonable controls have been implemented to complicate, detect, respond and recover from such an attack.

[4] Currently, the consumers of supply chain goods do not have an effective means to evaluate the adequacy of the cybersecurity risk management program at their supply chain vendors or understand the potential impact a cyber event could have on the vendor's manufacturing and distributing processes.

The following is a summary of the expected issuance and effective dates for the various levels of reporting:

Reporting level	Issuance date	Effective date
Entity	**April 26, 2017**	**April 26, 2017**
Service provider *(SOC 2 for Service providers)*	**April 26, 2017** ‣ For the period from the issuance date to the effective date entities will have the option to issue their SOC 2 reports under the current criteria or the updated criteria. ‣ Subsequent to the effective date, entities will issue their SOC 2 reports under the updated criteria.	**December 15, 2018**
Supply chain *(SOC 2 for Supply chain vendors)*	**Early 2018**	**Early 2018**

Given the lack of any legislative or regulatory mandates requiring third-party entity level attestation, this reporting is voluntary on the part of the organization.

Potential effects on companies

While there are no current legislative or regulatory requirements relating to cybersecurity reporting, the ongoing discussions taking place within Congress and by key regulatory bodies lead many to believe that such reporting may eventually become a reality. Accordingly, organizations should consider the following:

Entity-level reporting	Service organization/supply chain reporting — when you are a user of services or receive goods from others	Service organization/supply chain reporting — when you provide services or goods to others
‣ Do you operate in a heavily regulated sector? ‣ Do you have new board members, a new senior leadership team or activist investors who are routinely asking questions regarding the adequacy of the organization's cybersecurity safeguards? ‣ Have you had recent publicized breach activities against your systems? ‣ Do you have a need to materially differentiate yourself from your peers? If so, you should be prepared for inquiries from your board, regulator or other stakeholders, who may show increased interest in obtaining additional insights and confidence into the effectiveness of the organization's cybersecurity risk management program.	‣ Do you engage third parties to: ‣ Provide a *service* to the organization that significantly affects your ability to transact business (e.g., manufacture and/or deliver goods or services to the market and/or your internal operations and/or control environment? ‣ Provide *goods* to the organization that significantly affects your ability to transact business (e.g., manufacture and/or deliver goods or services to the market)? If so, you should consider requesting a service organization-level or supply chain-level (as appropriate) cybersecurity report from your third parties to obtain additional insights and confidence into the effectiveness of their cybersecurity risk management program.	‣ Are you engaged as a third party to: ‣ Provide a service to another organization that significantly affects their ability to transact business (e.g., manufacture and/or deliver goods or services to the market) and/or their internal operations and/or control environment? ‣ Provide goods to another organization that significantly affects their ability to transact business (e.g., manufacture and/or deliver goods or services to the market)? If so, you should be prepared for inquiries from your customers who may show increased interest in obtaining a service organization-level or supply chain-level (as appropriate) cybersecurity report to obtain additional insights and confidence into the effectiveness of your cybersecurity risk management program.

In addition, as these examinations will represent a comprehensive evaluation, some organizations may be concerned that their process and/or control procedures:

- May not address all of the relevant risks
- May not be applied across the entire enterprise
- May not be adequately documented
- May not be consistently applied

In these situations, we encourage management to have a preliminary assessment of its cybersecurity risk management program performed against the criteria to proactively identify issues and provide for timely remediation.

Frequently asked questions

Reporting necessity

Question – are these types of reports really needed?

Response – at the present time there is no legislative or regulatory requirements mandating cybersecurity reporting at the entity-level, and none are anticipated in the near-term; as a result, this level of reporting is voluntary on the part of the organization.

The decision on whether to undertake an entity-level examination (or the initial step of having an assessment performed to help identify issues requiring remediation) should be based on the unique needs of the organization and its stakeholders, and their expectations of future legislative or regulatory requirements. Conversely, the decision on whether to: require service organization/supply chain reports from key vendors and prepare service organization/supply chain reports for your customers will be driven by market demand and evolving risk management requirements.

Legislative/regulatory mandates

Question – what is the anticipated time frame for when the market should expect to see a legislative or regulatory requirements relating to third-party reporting over an entity's cybersecurity risk management program?

Response – given the evolving legislative and regulatory climate, it is difficult to predict what will happen in the coming years. However, given that: cyber events are continuing to occur at a rapid pace and there are currently 12 House and Senate committees that have jurisdiction over some element of cybersecurity and numerous federal regulatory bodies that are actively studying and evaluating what can be done to support the marketplace, many believe that the possibility of a medium-term or long-term legislative or regulatory requirement cannot be dismissed.

Understanding the benefits

Question – should the receipt of an unqualified opinion on a cybersecurity report provide readers with confidence that the entity's environment will not be materially impacted by a cybersecurity event?

Response – the underlying objective of the AICPA's initiative was not intended to achieve this lofty goal, and given the pace of change within the marketplace, this level of assurance can not be realistically achieved. The objective was to enhance the level and quality of communication taking place between entities and their stakeholders to a point where more effective risk management decisions can be made relative to this evolving business risk.

The receipt of an unqualified opinion on a cybersecurity report is intended to convey that the entity has implemented reasonable controls to complicate, detect, respond and recover from a cybersecurity event when measured against criteria that have been vetted in the marketplace and deemed to be suitable for the intended purpose and based on specific cybersecurity objectives the entity is obligated to achieve.

Using other criteria as a basis

Question — our organization has aligned the development of our cybersecurity risk management program around another framework (e.g., the NIST Cybersecurity Framework, ISO 207001, internally-developed hybrid framework. Are we required to utilize the evaluation criteria that has been developed by the AICPA?

Response — the AICPA guidance does not require that the evaluation criteria developed in conjunction with the reporting model be utilized in all instances. If an organization, and its auditor, determine that an alternate set of criteria are "suitable" to evaluate the identified subject matter (as defined by the AICPA) and available to intended users, the alternate criteria can be utilized.

Keep in mind that various frameworks being leveraged in the marketplace were originally developed as a "management framework" to assist organizations in establishing a program, versus an "assessment framework" that would be used to evaluate a program's effectiveness. As a result, certain frameworks may not satisfy the suitability requirement.

Segment-level reporting

Question — our organization is in the process of deploying our comprehensive cybersecurity risk management program across the enterprise on a segment-by-segment basis. Does the guidance allow us to perform cybersecurity reporting at a level less than the entity as a whole (e.g., covering one or more of our key business segments)?

Response — the AICPA guidance would not prohibit an organization from issuing a cybersecurity report on a scope that is less than the entity as a whole; however, the distribution of the deliverable would need to be limited to internal users (e.g., board, internal management) to avoid any misunderstanding regarding the scope of the examination.

The value of an assessment

Question — how high of a bar has the AICPA set for the marketplace to obtain an unqualified opinion?

Response — the criteria against which an entity's cybersecurity risk management program were developed after considering a combination of various market-recognized frameworks (e.g., COSO's Internal Control — Integrated Framework, AICPA's Trust Services Principles, COBIT 5, NIST's Cybersecurity Framework, NIST's Special publication 800 series, ISO/IEC 27000 series standards, HIPAA Security Rule, PCI's Data Security Standard).

Entities that have proactively adopted these (or other) comprehensive frameworks when designing their cybersecurity risk management program and have considered the need for enterprise-wide adoption will not be surprised by the areas of focus; conversely, entities that have adopted a less rigorous strategy or piecemeal deployment may find that their processes and/or control procedures may require enhancement.

Accordingly, an assessment of the organization's cybersecurity risk management program may be warranted if management is concerned that their process and/or control procedures:

- May not address all of the relevant risks
- May not be applied across the entire enterprise
- May not be adequately documented
- May not be consistently applied

Possible incremental uses

Question - can these reports be used to help satisfy reporting obligations under other regulatory or legislative reporting requirements being discussed in the marketplace, such as the Advance Notice of Proposed Rulemaking (ANPR) and the Global Data Privacy Regulation (GDPR)?

Response — possibly. As the ANPR is still in the early stage of development, the final reporting obligations are not yet know; similarly, the compliance requirements under the GDPR have not been specifically identified. However, the cybersecurity reporting options may prove to be an appropriate reporting structure to help entities satisfy certain reporting obligations.

Basis for management assertion

Question — since a management assertion is included in the report, does management need to conduct its own independent evaluation and testing of controls, similar to internal controls over financial statements?

Response — management is required to have a basis for its assertion, which would include an evaluation as to the effectiveness of its controls. This is similar to the internal control reporting required under Section 404 of Sarbanes-Oxley, as well as other SOC reports. While independent testing of controls may form part of that basis, other control evaluation techniques may also be appropriate, such as continuous control monitoring. Given the comprehensive nature of an entity-level examination, we encourage management to utilize the AICPA evaluation criteria (or other suitable criteria, see previous discussion) as the basis of its evaluation, and perform testing and other techniques covering a minimum of two control execution cycles to help ensure the controls are operating effectively.

Areas that may require remediation

Question — the scope of these examinations will likely touch parts of the company's control environment that have not been previously subjected to extensive evaluation and testing. Where would you recommend that we focus our initial assessment efforts to help ensure that adequate time is available to remediate any issues identified?

Response — every organization will have unique challenges relating to the maturity of its control environment; factors affecting this maturity include the complexity of the company's operations, the level of control standardization it has achieved, the use of third-party service providers to support key control/process areas, the extent of merger, acquisition and divesture activities, etc. However, the following are examples of key areas that will be covered within an examination that may require additional efforts to mature the program:

- **Inventory of IT assets connected to the network and access points to the network** — the entity will be expected to have a comprehensive inventory of all IT assets that can connect to the enterprise network, along with processes for adding and retiring assets, monitoring for change activity that does not follow the standard process, monitoring of new software added to the system, etc. In addition, the entity will be expected to have complete and accurate records on the access points through which its network can be accessed.
- **Incident management** — the entity will be expected to have an incident management program that includes comprehensive processes for monitoring, detecting and resolving detected incidents as appropriate.
- **Vendor risk management** — the entity will be expected to have a comprehensive vendor risk management program in place to evaluate vendors (initially and on an ongoing periodic basis) that are provided system access and/or support the execution of key processes and controls within the cybersecurity risk management program. Unlike other SOC reports, a carve-out option is not available to exclude such vendors from the scope of the examination; accordingly, the entity must have appropriate controls in place to effectively evaluate and monitor the services provided.
- **Threat and vulnerability management** — the entity will be expected to have a comprehensive threat and vulnerability management program in place to identify new threats and vulnerabilities that could impact the entity, evaluate their impact, and respond to the identified risks.

Summary

The issuance of a reporting model and evaluation criteria is an important first step in helping organizations address their internal and external communication needs relating to cybersecurity risk management.

While there are no current legislative or regulatory requirements relating to the issuance of cybersecurity reports, the uncertain legislative and regulatory climate make it challenging to predict future events. Accordingly, management and the board should further educate themselves on the objectives and value of these reporting options and the potential future impacts to the organization and evaluate their existing cybersecurity risk management program against the criteria.

For some organizations, significant remediation activity may be required to address identified gaps. Early identification of these gaps is essential to plan and execute remediation activities in an efficient, balanced and cost-effective manner.

EY | Assurance | Tax | Transactions | Advisory

About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

1704-22668881

ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax or other professional advice. Please refer to your advisors for specific advice.

ey.com