Are you prepared for global risk?
Chartered Global Management Accountant (CGMA®)

CGMA is the most widely held management accounting designation in the world. It distinguishes more than 150,000 accounting and finance professionals who have advanced proficiency in finance, operations, strategy and management. In the U.S., the vast majority are also CPAs. The CGMA designation is underpinned by extensive global research to maintain the highest relevance with employers and develop competencies most in demand. CGMAs qualify through rigorous education, exam and experience requirements. They must commit to lifelong education and adhere to a stringent code of ethical conduct. Businesses, governments and nonprofits around the world trust CGMAs to guide critical decisions that drive strong performance.

cgma.org

Association of International Certified Professional Accountants

The Association of International Certified Professional Accountants (the Association) is the most influential body of professional accountants, combining the strengths of the American Institute of CPAs (AICPA) and the Chartered Institute of Management Accountants (CIMA) to power opportunity, trust and prosperity for people, businesses and economies worldwide. It represents 650,000 members and students in public and management accounting and advocates for the public interest and business sustainability on current and emerging issues. With broad reach, rigor and resources, the Association advances the reputation, employability and quality of CPAs, CGMAs and accounting and finance professionals globally.

Acknowledgments

Kenneth W. Witt, CPA, CGMA, of the Association of International Certified Professional Accountants prepared this tool based on a webcast series that Kenneth R. van Wyk, President and Principal Consultant of KRvW Associates LLC presented.

Kenneth R. van Wyk, an affiliate of the webcast series sponsor Ridge Global Education, is a faculty member at the Institute for Applied Network Security (IANS), and Visiting Scientist at Carnegie Mellon University, providing consulting and training services for CMU’s Software Engineering Institute, CERT/CC. Van Wyk also is author of Enterprise Software Security: A Confluence of Disciplines (2014), with Mark G. Graff, Dan S. Peters and Diana L. Burley.
## Contents

2 Introduction

4 Understanding cybersecurity  
   What problems do we face today?  
   Who are the bad actors?  
   Risk of security vulnerabilities

6 Cybersecurity fundamentals  
   Security objectives  
   Security controls: protection, detection, response

10 Applied cybersecurity  
   Centralised management: desktops, laptops, mobile devices, networks, applications  
   Centralised monitoring: SIEMs and SOCs

13 Advanced topics  
   Forensic analysis  
   Malware analysis  
   Penetration testing  
   Software security

16 Conclusion: SME “short-list”

17 Appendix I: Cybersecurity insurance

18 Appendix II: Cybersecurity risk management reporting framework

20 Additional reading and resources
Introduction

Cyber risk has become a front-and-center issue in today’s global economy. The media is rife with reports of cyberattacks ranging from major customer records thefts and health care records breaches, to political incidents.

Unfortunately, we are living in a world where the risk of a cyber intrusion is no longer a question of if, but a question of when. In fact, according to the World Economic Forum 2017 Global Risk Report, data fraud or theft, and cyberattacks rank fifth and sixth, respectively, on their list of Top Ten Risks in Terms of Likelihood.

In a WEF article, “What cyber-security insiders discussed at Davos 2017,” industry insiders made three points about the theme of the summit — “responsive and responsible leadership”:

1. Be proactive, prevent threats and prepare yourself.
2. Educate your people.
3. Promote cyber resilience.

Systems security is no longer an issue that resides solely with the IT department and chief information officer. In this day and age, it is imperative that executives and boards take a top-down, bottom-up and organisation-wide approach to cybersecurity.

This tool provides an overview for doing just that. It provides an understanding of security risks, approaches and responses to addressing this threat. In addition, it incorporates essential elements from a framework developed by the American Institute of CPAs that you can use to develop an effective cybersecurity risk management programme and ensure the continued success of your organisation.
Cybersecurity tool: Cybersecurity risk, response and remediation strategies
Understanding cybersecurity

Understanding cybersecurity in today’s complex digital world begins with knowing what the most common threats are, who the potential “bad actors” are, and what we can do to shore up our defenses.

What problems do we face today?
The most common threats to our cybersecurity include malware, including ransomware, botnets, malvertising, phishing and application attacks.

Malware is the term used for malicious software intended to do any number of things ranging from the stealing of credentials, other information or money to the general wreaking of havoc, or denial of service. Some of the more typical types of malware include:

- **Ransomware** is a type of malicious software designed to block access to a computer system until a sum of money is paid.

- **Botnets** are networks of interconnected computers that are infected with a “botnet agent” designed to do the attacker’s bidding.

- **Malvertising** involves injecting malicious or malware-laden advertisements into legitimate online advertising networks and web pages. Malvertising is a serious threat that requires little or no user interaction.

- **Phishing** usually is an email designed to lure the reader into doing something ill-advised by masquerading as a trustworthy source or legitimate enterprise. Phishing requests to execute an attachment to the email or click on a link are designed to install malware on the user’s computer, generally for the purpose of stealing money. Phishing can also involve more direct requests to provide private information such as passwords, credit card account details or other sensitive data.

Application attacks are increasingly common as application development is moving more and more to the web. In addition to complex business applications being delivered over the web, our personal mobile phone applications and our home devices connected to the internet via internet of things platforms create widespread vulnerabilities.

Application attacks, while varied in nature and design, usually have the same intents and purposes as malware attacks — stealing data from database servers, running attack scripts on other users’ computers, stealing user credentials, etc.

Who are the bad actors?
While the term “hacker” may have had its origin as a term used to describe especially talented computer programmers and systems designers, and may still include those considered “curious” hackers, the term has become much more widely used to describe computer intruders or criminals with less-than-desirable intent. In addition to basic thieves, these “bad actors” can be outsiders, such as business competitors or nation-states. They can also be insiders, such as disgruntled, or otherwise malicious, employees.
Cost of doing business in the digital age

According to the 2016 Cost of Data Breach Study: Global Analysis benchmark research IBM sponsored and Ponemon Institute LLC independently conducted, the following findings highlight the cost of data breaches for 383 companies in 12 countries:

- $4 million is the average cost of a data breach
- $158 is the average cost per lost or stolen record
- The biggest financial consequence is lost business — organisations need to take steps to retain customers’ lost trust to reduce the long-term financial impact
- Regulated industries such as health care and financial services have the most costly breaches because of fines and the higher that average rate of lost business and customers

Risk of security vulnerabilities
Cybersecurity vulnerabilities can be technical in nature or procedural. Technical deficiencies that create exposure to sensitive functionality or information include software defects and the failure to use security protections such as encryption adequately. Procedural deficiencies can be IT related, including system configuration mistakes, or failure to keep up with software security updates. However, many procedural deficiencies are user related, such as poorly chosen passwords.

Whatever the cause, when exploited, these vulnerabilities can be costly and result in:

- **Down time** — Loss of business production or revenue generation opportunities
- **Tarnished reputation** — Company and brand value negatively affected
- **Customer flight** — Especially critical with increasing level of e-commerce
- **Legal consequences** — Fines, lawsuit costs and settlements can be staggering
- **Industry consequences** — Health care records breaches have been extensive

Cybersecurity tool: Cybersecurity risk, response and remediation strategies
Cybersecurity fundamentals

It is essential that businesses address these risks and implement security measures to protect their information assets and ensure the ongoing viability of their enterprise.

Cybersecurity objectives
As outlined in Appendix II, the AICPA has developed a cybersecurity reporting framework that organisations can use to demonstrate to key stakeholders the extent and effectiveness of an entity’s cybersecurity risk management programme. A critical element of any cybersecurity risk management programme is the formulation of objectives by management.

Management establishes cybersecurity objectives that address cybersecurity risks that could affect the achievement of the entity’s overall business objectives (including compliance, reporting, and operational objectives). They vary depending on the environment in which the entity operates, the entity’s mission and vision, the overall business objectives established by management, risk appetite and other factors.

Key cybersecurity objectives outlined in the framework resource Description Criteria for Managements Description of the Entity’s Cybersecurity Risk Management Programme include:

- **Availability** — Enabling timely, reliable, and continuous access to, and use of, information and systems
- **Confidentiality** — Protecting information from unauthorised access and disclosure, including means for protecting proprietary information and personal information subject to privacy requirements
- **Integrity of data** — Guiding against improper information modification or destruction of information
- **Integrity of processing** — Guarding against the improper use, modification, or destruction of systems

Security controls: protection, detection, response
In order to achieve these security objectives and mitigate these risks, security mechanisms need to be implemented having the objectives of protecting information assets, detecting malicious activity when (not if) it occurs, and responding effectively to that malicious activity in order to minimise the impact on the business.

Different controls need to be implemented at different levels of the software, across the spectrum of components outlined below:

---

### Things we protect

- Servers
- Desktops
- Mobile devices
- Networks
- Data storage
- Business applications

### How we protect them

- Policies and policy management
- Software updates
- Configurations
- Security products
- Application software controls
**Protection** — First and foremost, we try to protect our information assets and systems against attack. Protection strategies are our first line of defense, and breaches usually are a failure of protection strategies.

Protective controls include the following measures:

- **Identification** — In order to have confidence in accountability for users, whether individuals or interactive system components, we need to have identification, e.g., usernames
- **Authentication** — Also need to be able to authenticate that identification, e.g., passwords, fingerprints, etc.
- **Authorisation** — In addition to authentication, we need to make sure user is authorised to conduct transaction — verification of the user’s level of authority for particular type of access or transaction
- **Protecting secrets** — e.g., encryption of credit card information
  - *At rest* — while being stored
  - *In transit* — while being transmitted

Certificates are a significant underpinning of security systems, especially where payments or particularly sensitive information is involved. Certificates are used for all kinds of practical applications, including the transmission of confidential information and the digital signing of documents.

Certificates are used in what is referred to as a “handshaking” procedure to verify the identity of the sender, enable the transmission of encrypted confidential information privately, and also enable the receiver to know whether the information has been tampered with via the use of tamper-evident seals.

There is a public half and private half of a certificate. It is critical that the private half of the certificate be kept secure and not passed between parties. Within an organisation, certificates can be centrally managed to enable users to access the public certificate for someone to whom they want to send encrypted information. For external use, public certificates are issued by third-party certificate authorities that verify the identification of parties using them.

**Man-in-the-middle attacks**

Certificates are essential for circumventing man-in-the-middle (MitM) attacks. MitM is the term used for attacks in which the attacker independently makes connections with the victims and relays messages between them to create the impression that they are communicating with each other when, in fact, the attacker is controlling the conversation.
Detection — In addition to protective or preventive strategies, it is also essential that entities employ detection strategies to identify when threats occur — essentially the computer equivalent of the security camera.

Common detection strategies include:

• **Event monitoring** — Documentation of events logged into files can be reviewed to look for unusual patterns of activity

• **Intrusion detection and prevention systems** — Sophisticated applications are now available that enable the ability to perform ongoing monitoring

• **Threat monitoring** — Security community can study the tools and techniques that attackers use in order to develop “threat intelligence” that can be used to inform the development of new controls

• **User reports** — User reports can also be very helpful in identifying unusual activity

Response — Part of the evolution of cybersecurity is the advent of Computer Incident Response Teams (CIRTs), sometimes referred to as Computer Security Incident Response Teams (CSIRTS).

The primary functions of the response team are to:

• Reduce losses

• Help the business get back into business as soon as possible

• Support investigations when necessary — law enforcement, forensic

• Provide decision support during incident-situational awareness, plan of action, informed decisions

• Facilitate crisis communications — customers, law enforcement, media, etc.

When an organisation is attacked, the key role of an incident response team is to serve as an advocate for the business and "keep the patient alive."
Cybersecurity tool: Cybersecurity risk, response and remediation strategies
Centralisation is an important element of cybersecurity with respect to implementing preventive and detective controls and responding to cyber breaches, especially when considering enterprise-level systems with huge numbers of desktop computers, laptops and mobile devices.

Centralised management

**Desktops** — Modern operating systems are fortunately very feature-rich in terms of security features. Centralised management is a key way to control and orchestrate key security features. The ability to “push” security protocols, software updates and security update “patches” to remote users enables the scalability of security for large enterprise-level systems. Centralisation also provides the ability to maintain a directory of user profiles that enables users to access their information from multiple locations.

**Laptops** — While many security features are common between desktop and laptop computers, the inherent mobility of laptops, especially the risk of lost or stolen devices, presents some unique challenges. Whole disk encryption, whether a feature of the operating system or an endpoint product, is an essential feature to ensure the security of data on laptop products.

**Mobile devices** — There are third-party Mobile Device Management (MDM) products to facilitate the centralised management of such devices. Some companies consider it important to have company-owned devices and will implement a configuration profile that will prohibit the download of non-company applications.

Many companies now have what are referred to as bring your own device (BYOD) programmes. In order to ensure security for these employee-owned devices, they require employees to submit those devices for company-wide management, similar to laptop security policies. To allow for flexibility in the implementation of security policies, companies can create different configuration profiles for different classes of users for their mobile devices.

**Network configuration** — Another critical component that companies use to enforce policies across the spectrum of corporate networks, including desktops, laptops and mobile devices is network configuration. The value of these network-level controls is that they are exceedingly difficult to circumvent.

**Network firewalls** — Pre-defined policies about who can access what, can be used to restrict access to social media or other categories of websites. Access control lists implemented at the network level can be used to provide people with access to sites that may not be allowed to others. The communications team, for example, may be authorised to have access to social media sites for company purposes.

VIP travel: “Throw-away systems”

Many companies with employees or executives travelling to remote locations set up “traveler laptops,” especially for the trip. Whole disk encryption is used, and only the data necessary for the trip is set up on the device. When the executive returns, any files used on the trip are retrieved while the operating system and files are completely removed and reinstalled for future use.

Some companies travelling to particularly sensitive locations actually destroy the computer, rather than run the risk of compromising proprietary information.
Container applications: Creating a “world within a world”

Containerisation is very useful for securing data on mobile devices. It involves encapsulating an application in a container with its own operating environment. Containers allow you to put software written for your company environment in a container so employees do not need to use the device applications for company data. The container is entirely encrypted so you can keep your company data in the enclave and keep personal data out. These are popular for enterprise deployments, especially for basic services such as exchange email, calendar sharing, etc.

Application firewalls — In addition to network firewalls intended to restrict access to authorised individuals, application firewalls can also be used to protect against known web applications attacks.

Antivirus and endpoint products — In addition to centralised management of security features, “endpoint products” also are commonly used by most organisations to augment the features that the operating system provides. Endpoint products are especially valuable in ensuring security in enterprise-level systems that are accessed by multiple users, from multiple locations with multiple devices. These products can ensure compliance with the organisation’s policies and standards in addition to verifying the integrity of application products and detecting viruses, blocking activity if issues are found.

Centralised monitoring

Fortunately, as enterprise systems with hundreds or even thousands of laptops have become the norm for organisations, centralised monitoring of systems activity has fortunately also evolved over time. Important components of centralised monitoring include:

Event logging and aggregation — All modern computer operating systems keep a ledger of their activity — Who logged in? What programmes did they run? What files were accessed? What were the failures as well as the successes? The event logging on operating systems is largely superficial. However, it still is essential for administrative and accountability purposes as well as potential forensic use.

Best practice is to send logs to a central monitoring point, usually in the data center or security operations center (SOC). In addition to professional considerations, privacy considerations dictate that these “logs” are viewed only by security personnel. While logging of this information is critical for forensic purposes, the real value is to look at this data while activity is occurring.

Security information and event management (SIEM) — SIEM systems have been developed to make this monitoring more effective. SIEMs analyse all of the available data and look for specific patterns in the data that might suggest a possible attack or security compromise.

SIEMs dive deeply into possible incidents, automating the process of analysing what might be referred to as “needle in the haystack” scenarios.
Modern Security Operations Center (SOC) functions
— SOC environments have matured over time and have a range of important teams, or functions:

- **Incident response team** — When the team monitoring the SIEM identifies a potential threat, they initiate an incident response process. Their focus is on business continuity.

- **Threat intelligence team** — The mission of the threat intelligence team is to monitor current trends, especially in the specific industry sector in which the organisation is involved. Threat intelligence teams feed that information to the team that is responsible for monitoring activity via the SIEM.

- **Hunt team** — The mission of this team is to operate on the assumption that the organisation already has breached, but the SIEM team has not yet determined that the breach has been occurred.

- **Insider threat team** — Research also has identified factors that are associated with employees involved in breaches, e.g., employees passed up for promotion, declining performance evaluations, financial challenges, etc. While some organisations have deployed insider threat teams, investigating for potential insider involvement has serious privacy and legal considerations.

The incident response team is in effect the “EMT” of the IT world.

The role of the hunt team is to look for “footprints in the sand” for possible intrusions.

The importance of threat intelligence and hunt teams

According the Verizon 2016 Data Breach Investigations Report (DBIR), the gap between security breaches and detection is widening.

- In 93% of breaches it takes only minutes or less for attackers to compromise systems.

- In four out of five cases victims do not realise they’ve been attacked for weeks or longer.

- In 7% of cases the breach goes undiscovered for more than a year.
Advanced topics

Prevention is the goal of any cybersecurity strategy, along with timely detection and an effective response to the inevitable intrusion. Equally important is gaining a deep understanding of the attack and an ongoing effort to continually improve your systems.

Forensic analysis
Forensic analysis, while using some of the same means and methods as the incident response team, has different objectives. In addition to determining what happened, and how a particular breach might be prevented in the future, forensic analysis is the process of examining what is left behind that might be of value to investigators. The three primary elements of forensic analysis include system-level analysis, storage analysis and network analysis.

System-level analysis — If we know a system has been breached, the first level of analysis would involve looking at the individual system that was compromised for “footprints in the sand” to determine what changes were made including:

- **System components** — Especially with a malware installation, operating system components are often changed by attackers so that when the desktop or laptop is re-booted, the malicious software also is inserted
- **Configuration changes** — Altered system components such as settings and how programmes are executed and run
- **Fake accounts created** — A common re-entry method used by attackers
- **Services enabled without authorisation** — These are things an attacker would do so they can get back onto the system to facilitate further theft or intrusion

Storage analysis
The size of today’s databases and the advent of cloud environments complicate storage analysis greatly. Also, the complex nature of computer storage, in which data are stored in non-sequential locations assigned by the operating system “map,” makes forensic analysis very time consuming and painstaking.

Computer storage media is far from perfect. Media may have “slack space” containing relevant data. Also, “deleted” files often do not really get deleted, they just become unreferenced by the operating system. However, if deleted files happen to get overwritten, the process of recovery becomes especially complicated and enormously time consuming.

A particular complication of cloud environments with respect to forensic analysis involves the external ownership of the servers containing the data. While a subpoena can be issued to the owner of a hard drive containing data that you want to analyse, often the data that you may be interested in may have been deleted and overwritten.

Network analysis
Collecting and analysing network data “traffic” provide different perspectives. While network monitoring does not provide information about the content of what is coming and going, it does provide information about who is coming and going.

One of the greatest advantages of performing network security is that the adversary does not know they are being watched.

Monitoring network traffic in cloud storage services creates privacy considerations that do not exist when you have a company-owned hard drive that you can simply make a copy of.
Malware analysis
If malware is located on the system, especially if it is a piece of unauthorised software, it is important to deeply understand what the malware does.

Reverse engineering — The first step is to reverse engineer the piece of malware and determine how it works and what it does.

The developers of the malware will certainly have made it very difficult for them to get caught and also very difficult for security people to understand how the malware works. Accordingly, they will have "packed" the malware to achieve both of these goals. The malware will be packaged in an "envelope" that will be unpacked during use and packed back into the envelope container when not in use. Malware developers will use multiple envelopes that are packed in a different way, using different tools that must be unpacked a layer at a time by the analyst trying to evaluate it.

A hugely important question is whether the malware was "targeted" or "un-targeted" to a particular industry or company. If the malware is "untargeted," then chances are that the endpoint protection will be able to detect and remove the malware and there is somewhat less concern than if the malware was specifically targeted to your company or industry.

Decompilation and disassembly — Once malware is "unpacked" and decrypted, it is important that it be analysed to fully understand how it worked and what it was intended to do.

Since the malware will be written in machine code that is very programming-language specific, tools designed for de-compiling or disassembling malware facilitate this "byte-level" analysis.

Penetration testing
The purpose of doing penetration testing is to find the weak points in your software before adversaries find them. If weaknesses are found, it may be possible to fix them. Otherwise, it may be possible to put in place a detection mechanism to block an intrusion. Steps for penetration testing include determining how it works and what it does.

Network discovery — The purpose of this step is to identify all of the components on a network by doing a reconnaissance of the entire network.

This is the reconnaissance phase to find targets.

In addition to desktops, laptops and mobile devices, there is an increasing number of "smart" devices on computer networks today, ranging from physical components of business systems connected via what is referred to as the "internet of things." In addition to specific business components, home computer printers, televisions and other devices in home systems might serve as points of access for an intrusion.

Vulnerability probing — With a map of the network prepared, the next phase is to see if any "doors" are unlocked. The purpose of vulnerability probing is to determine which components may have known vulnerabilities or potential weaknesses. There are abundant online databases of vulnerabilities that have been identified for common business systems.

Exploiting vulnerabilities — Knowing where the weaknesses are, the next step is to exploit those vulnerabilities to verify the level of concern by gaining access to a system and attempting things that might be of particular concern to a company.

Not all steps in penetration testing are always carried out. Penetration testing on business applications that are live, active systems requires extensive "hands-on" interaction.

Complexity is the ally of the adversary and the enemy of the security people.
Software security
Software security is the practice of writing software that is resilient to attack. There are essentially three tiers of software security:

- Tier 1 — You want to be able to block an attack from succeeding
- Tier 2 — You also want to be able to alert security (SIEM) about an attack and provide critical information
- Tier 3 — You also want to be able to take evasive actions such as protecting sensitive data, e.g., credit-card information, and locking accounts

Design review — Involves looking for design or architectural weaknesses. Particular areas of sensitivity are customer records, intellectual property and payment information.

Code review — This looks at software at the source-code level. Code-review procedures include looking at key areas of sensitivity such as verification and authentication processes and common areas of programming weakness. Many companies have manuals that prescribe positive coding guidelines that are valuable for performing code reviews.

Security testing — While penetration testing involves testing the resilience against some set of known software vulnerabilities, security testing is diving deeply into software to verify that security requirements are being properly performed.

Security testing is much like an audit. Looking at software from the “inside” for evidence that security requirements are actually doing what they are intended to do.
Conclusion

SME “short-list”

While many of the more sophisticated security measures are more in the domain of larger “enterprise-level” systems, many things also are important for smaller companies, even in an environment with small numbers of desktops or laptops. Following is a short list of small-to-medium-sized business “must-dos.”

The time to start making relationships with outside service providers is not when you have a crisis, but before a crisis.

**Centralised management**—Event logging and concentrating or centralising the event logs is important. There are affordable SIEM products and SIEM-like products available to perform this task. Logs should be sent to a central location, whether to an IT security person or a system administrator. There also are intrusion-detection services available that can look at the logs and send notifications about potential incidents as well.

**Outsourced services**—These should be considered for other needs, especially helping to resolve incidents. Many services are provided by vendors on a retainer basis. Specific tasks to which you might want to have access for an outsourced provider include:

- Forensics
- Malware analysis
- Scanning and penetration testing

As noted, there is always the “trade-off” that these outside providers will see the inside of your system very closely.
Appendix I: Cybersecurity insurance

Since coverage for damages related to cybersecurity incidents is not included in most commercial insurance policies, a separate policy, or rider, is required. This is especially true for organisations that have significant customer or client Personally Identifiable Information (PII), organisations that process online credit card payments, or are otherwise highly dependent upon the web to conduct their business.

In addition to insurance that covers the losses relating to damage to, or loss of information from, IT systems and networks, policies generally include significant assistance with and management of the incident itself, which can be essential when faced with reputational damage or regulatory enforcement.

As outlined in a Lloyd's of London Quick Guide to Cyber Risk, cyber risks fall into first-party and third-party risks:

First-party insurance covers your business's own assets. This may include:

- Loss or damage to digital assets such as data or software programmes
- Business interruption from network downtime
- Cyber exhortation where third parties threaten to damage or release data if money is not paid to them
- Customer notification expenses when there is a legal or regulatory requirement to notify them of a security or privacy breach
- Reputational damage arising from a breach of data that results in loss of intellectual property or customers
- Theft of money or digital assets through theft of equipment or electronic theft

Third-party insurance covers the assets of others, typically your customers. This may include:

- Security and privacy breaches, and the investigation, defense costs and civil damages associated with them
- Multi-media liability, to cover investigation, defense costs and civil damages arising from defamation, breach of privacy or negligence in publication in electronic or print media
- Loss of third-party data, including payment of compensation to customers for denial of access, and failure of software or systems

While cybersecurity insurance is an important aspect of an organisation's strategy, it should not replace best practices, policies and controls. In fact, having an effective cybersecurity programme in place can reduce premiums.
Appendix II: 
Cybersecurity risk management reporting framework

In response to the growing demand for information about the effectiveness of organisational efforts to manage cybersecurity threats the AICPA has developed a cybersecurity risk management reporting framework. While there are many methods and frameworks for developing cybersecurity risk management programmes, this framework is a common language for organisations to communicate about, and report on, these efforts.

This framework is designed to help organisations demonstrate to key stakeholders the extent and effectiveness of their cyber risk readiness efforts. It can be used internally by companies to explain, in a consistent manner, all of the policies, procedures and controls it has implemented to address the cybersecurity risks that are critical to their business. It can also be used for reporting to senior management, boards of directors, and other stakeholders to facilitate their understanding of the entity’s cyber risk management programme.

Being a key component of a new System and Organisation Controls (SOC) for Cybersecurity attest engagement it can also assist organisations in demonstrating to analysts, investors, and other external parties that they have effective processes and controls in place to detect, respond, mitigate and recover from breaches and other security events.

Benchmarks, which can be used by management in describing their cybersecurity risk management programme, are captured in the framework’s Description Criteria for Managements Description of the Entity’s Cybersecurity Risk Management Programme.

An Illustrative cybersecurity risk management report has also been developed to provide an example for how an entity might prepare and present a description of its cybersecurity risk management programme.

The description criteria are categorised into the following sections:

Nature of business and operations — Disclosures about the nature of the entity’s business and operations.

Nature of information at risk — Disclosures about the principal types of sensitive information the entity creates, collects, transmits, uses and stores that is susceptible to cybersecurity risk.

Cybersecurity risk management programme objectives (cybersecurity objectives) — Disclosures about the entity’s principal cybersecurity objectives related to availability, confidentiality, integrity of data, and integrity of processing and the process for establishing, maintaining, and approving them.

Factors that have a significant effect on inherent cybersecurity risks — Disclosures about factors that have a significant effect on the entity’s inherent cybersecurity risks, including the

• Characteristics of technologies, connection types, use of service providers, and delivery channels used by the entity;

• Organisational and user characteristics;

• Environmental, technological, organisational and other changes during the period covered by the description, the entity and in its environment.

Cybersecurity risk governance structure — Disclosures about the entity’s cybersecurity risk governance structure, including the processes for establishing, maintaining and communicating integrity and ethical values, providing board oversight, establishing accountability, and hiring and developing qualified personnel.
Cybersecurity risk assessment process — Disclosures related the entity’s process for

• identifying cybersecurity risks and environmental, technological, organisational and other changes that could have a significant effect on the entity’s cybersecurity risk management programme;

• assessing the related risks to the achievement of the entity’s cybersecurity objectives; and

• identifying, assessing, and managing the risks associated with vendors and business partners.

Cybersecurity communications and the quality of cybersecurity information — Disclosures about the entity’s process for communicating cybersecurity objectives, expectations, responsibilities, and related matters to both internal and external users, including the thresholds for communicating identified security events that are monitored, investigated, and determined to be security incidents, requiring a response, remediation, or both.

Monitoring of the Cybersecurity Risk Management Programme — Disclosures related to the process the entity uses to assess the effectiveness of controls included in its cybersecurity risk management programme, including information about the corrective actions taken when security events, threats, vulnerabilities, and control deficiencies are identified.

Cybersecurity Control Processes — Disclosures about

• The entity’s process for developing a response to assessed risks, including the design and implementation of control processes;

• The entity’s IT infrastructure and its network architectural characteristics; and

• The key security policies and processes implemented and operated to address the entity’s cybersecurity risks.
Additional reading and resources

- AICPA Cybersecurity Resource Center
- AICPA SOC for Cybersecurity
- CGMA Risk Management Toolkit
- Ensuring corporate viability in an uncertain world: Framing the board conversation on risk
- Global Management Accounting Principles
- IRM cyber risk: Resources for practitioners
- ISO/IEC 27001 — Information security management
- NIST Cybersecurity Framework
- Rethinking the value chain
- Risk and innovation

Journal of Accountancy articles:

- Be vigilant about cybersecurity, warns former FBI agent
- How to be street smart when budgeting for security
- The hidden costs of a data breach
- Viewing cybersecurity through a COSO lens