CGI

Experience the commitment®

Understanding Cybersecurity Standards

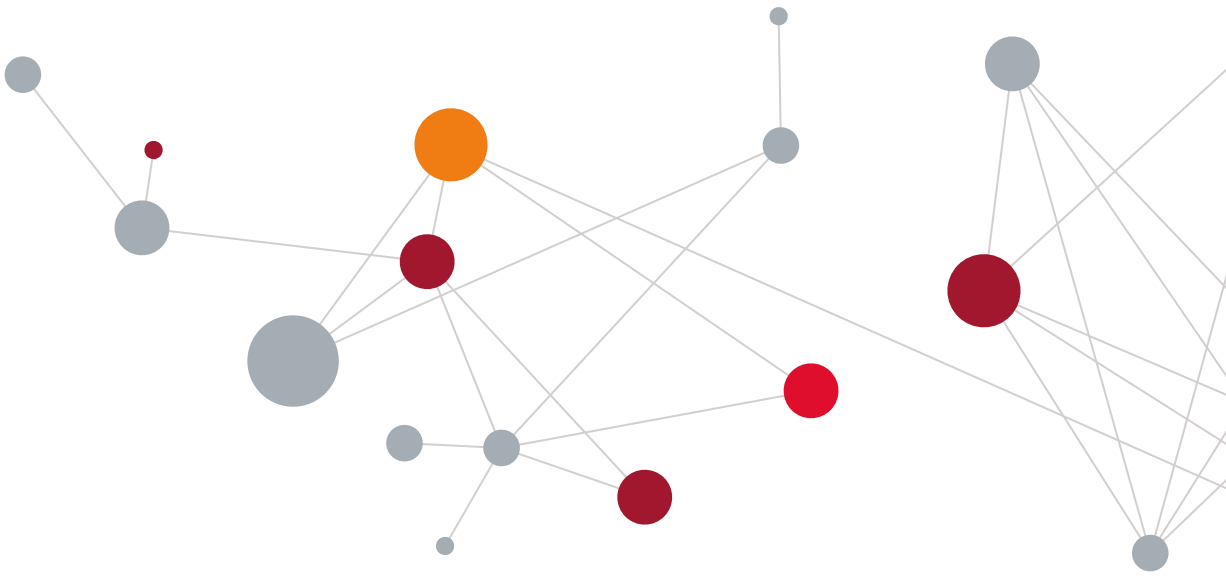
April 2019


information
protection
Shift

Introduction

Given the critical decisions that must be made in an environment of evolving cyber threats, cybersecurity standards are the crucial means by which an enterprise ensures its security strategy and policies are implemented in a consistent and measurable manner. In this paper, we describe the role of cybersecurity standards in the larger IT context, and offer best practices for establishing a cybersecurity standards framework and managing compliance. While this paper focuses on standards related to IT security and privacy, physical security standards also play an important parallel role. In many cases, the basic principles outlined in this paper can be applied to physical security as well.

This paper describes the role of cybersecurity standards in the larger IT context, and offers best practices for establishing a cybersecurity standards framework and managing compliance.



What is a cybersecurity standard?

The Oxford Dictionary defines “standards” as “a level of quality or attainment.” When it comes to standards for cybersecurity, the following definition offers several useful principles:

Cybersecurity standards can be defined as the critical means by which the direction described in an enterprise’s cybersecurity strategy and policies are translated into actionable and measurable criteria.

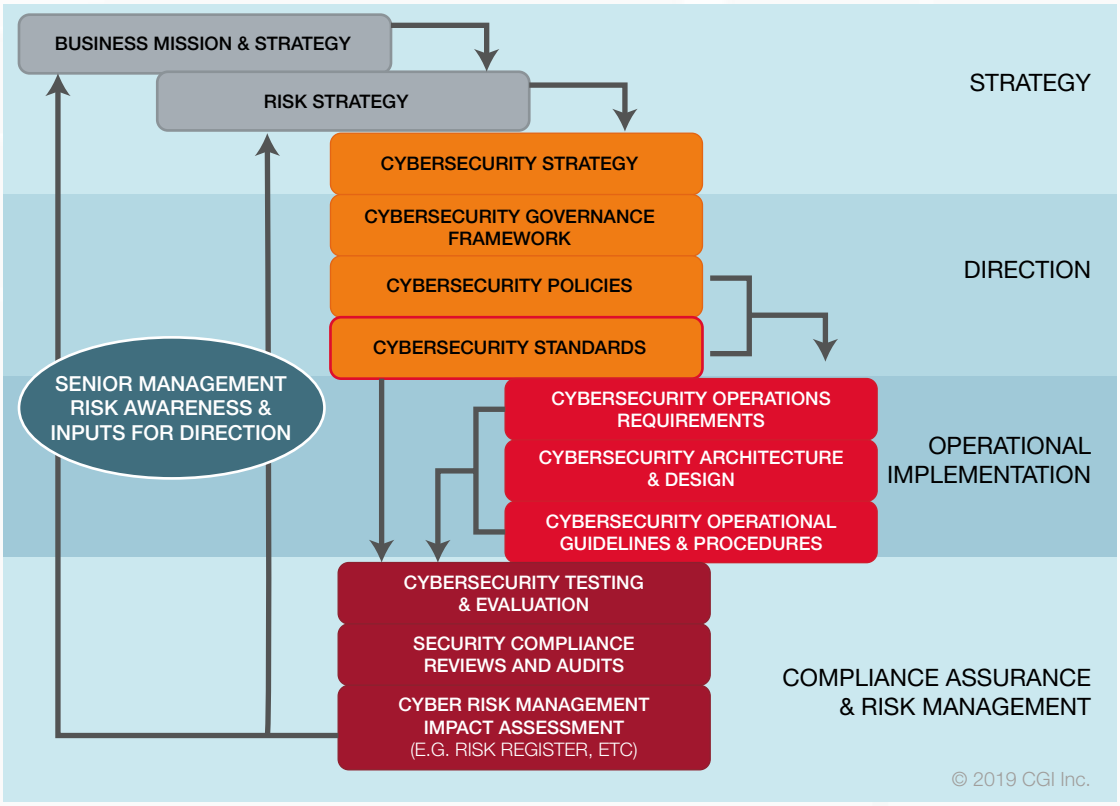
Cybersecurity standards are statements that describe what must be achieved in terms of security outcomes in order to fulfill an enterprise’s stated security objectives. How the standards are to be implemented and what solutions are used to achieve the standard normally are not part of the standard itself. Instead, these activities should be described in ensuing plans and operational procedures that are developed to implement the standard at a given point in time.

Cybersecurity standards in IT governance

Cybersecurity standards represent a key step in the IT governance process. As a means for managing and containing risk to acceptable levels, the standards must be wholly consistent with IT governance instruments and closely aligned with and driven by the enterprise's cybersecurity policies.

The diagram below represents the typical elements of an IT governance hierarchy. Cybersecurity standards sit at the critical interface between the Direction elements and the Operational Implementation elements. Standards provide essential direction for the objectives and outcomes to be achieved through subsequent implementation activities, such as the development of functional and technical requirements, architecture and design, operational guidelines and operating procedures.

Figure 1 - Cybersecurity Standards in the IT Governance Hierarchy



Throughout all steps of the IT governance process, direct traceability is needed to ensure effective management, audit and compliance. Cybersecurity standards must reflect, and be cross-referenced to, both the enterprise's policies and its external regulatory obligations (e.g. external standards and controls, such as financial or privacy regulations).

Establishing a standards framework

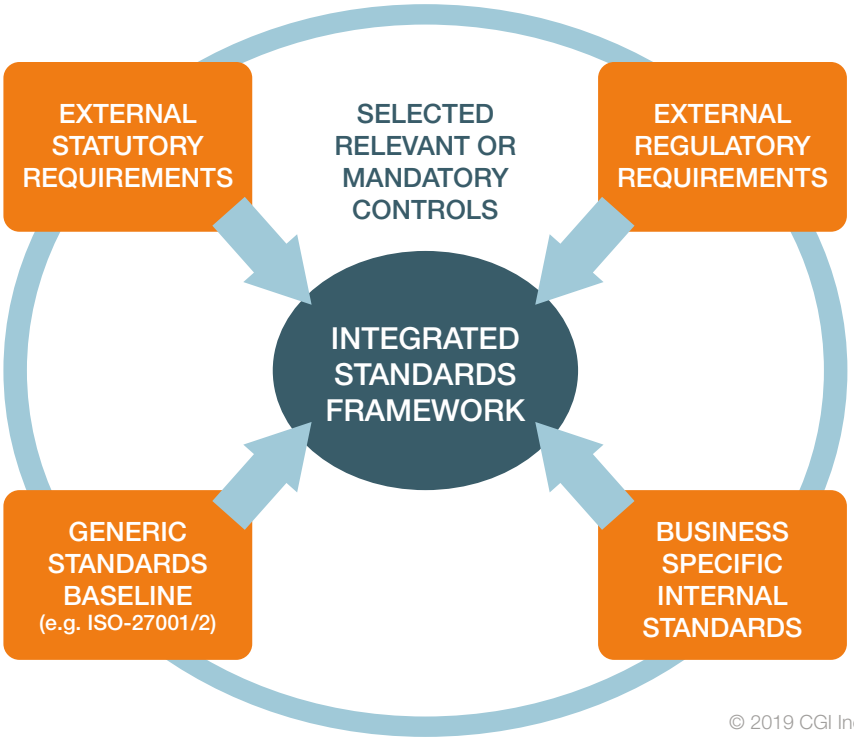
Many enterprises choose to adopt a generic industry cybersecurity standards framework such as the ISO/IEC 27001 family of standards. Although this is an excellent first step, it may not address adequately all of the enterprise's statutory, regulatory and business obligations.

This is because generic standards do not take into account industry-specific or regional requirements. As an example, a financial institution limiting its framework to ISO/IEC 27001 standards would expose itself to risk and potential liability by not taking into account standards required by relevant financial regulatory bodies (e.g. the Office of the Superintendent of Financial Institutions/OSFI in Canada), or other mandatory industry or regional requirements, such as those imposed by the Payment Card Industry (PCI) Security Standards Council, Society for Worldwide Interbank Financial Telecommunication (SWIFT) or the European Union's (EU's) General Data Protection Regulation (GDPR).

Instead, the enterprise should identify all obligatory cybersecurity requirements and controls with which it must comply and combine those with an industry standards baseline in a single integrated framework. The rationale for including these standards or controls should be reflected, at least at a high level, in the enterprise's overarching cybersecurity strategy and policies.

An enterprise should identify all obligatory cybersecurity requirements and controls with which it must comply, and build them into a single, integrated enterprise cybersecurity standards framework.

Figure 2 – A Typical Integrated Cybersecurity Standards Framework



EXTERNAL STANDARDS

Industry and government entities are required to comply with a range of external cybersecurity and privacy standards, requirements and controls, and failure to comply can have significant punitive consequences. The following are a few examples:

- NIST (Special Publication) SP 800-53 or ITSG-33 Risk Management Framework. These frameworks are promulgated by the U.S. and Canadian federal governments respectively. Primarily used by federal government organizations, the frameworks have been adopted by some industry enterprises as well. They provide a methodology as well as a catalogue of up to 900 detailed controls and control enhancements from which a profile can be created to meet almost any requirement.
- NIST Cybersecurity Framework. This "lighter" alternative to NIST SP 800-53 is intended for broader industry adoption.
- ISO/IEC 27001. A set of security standards, issued by the International Standards Organization (ISO), that has been adopted widely worldwide. Many of the control objectives are broad in nature and require supplementation by organizations with external compliance obligations.
- GDPR. Mandatory privacy-based statutory regulations for enterprises processing or controlling private personal data belonging to EU citizens. Punitive measures for non-compliance or breaches can be significant.
- Cyber Essentials. Originally required for companies dealing with the UK government, this lightweight set of standards is now being more broadly adopted as an alternative to either the NIST Cybersecurity Framework, or ISO 27001.
- PCI DSS. This data security standard is mandatory for most enterprises collecting, processing and storing payment card data (e.g. Visa and Mastercard).
- SWIFT Customer Security Control Framework (CSCF). This framework is required for financial institutions participating in and processing transactions via the global SWIFT Network.

INTERNAL STANDARDS

Each enterprise has specific requirements to control risks and guard against liabilities that are unique to their business or industry. Often, these requirements are identified by senior management at the security and risk strategy and policy level. To fulfill the requirements, tailored standards and control objectives need to be defined and added to standards already adopted by the enterprise (see Fig. 2, Page 4).

The only thing worse than not having a standard is having one that is unclear, ambiguous, or impossible to implement.

CREATING INTERNAL STANDARDS

To help ensure standards are clear and relevant, the following 10 basic principles should be applied:

1. **Be linked to policy**. In addition to alignment with business needs, linking a standard to policy also ensures consistent implementation. If your standard is not directly related to the implementation of an approved policy, be prepared for it to be challenged by those who would resist its adoption.
2. **Be collaborative.** Cybersecurity standards can impact many facets of an enterprise. For that reason it is essential to directly engage key stakeholders such as IT operations and business line owners, as well as risk, audit, privacy, and legal departments. Make it a team sport and embrace their inputs. Doing so will make them feel that they have played a role in developing the standard, and they will be less likely to oppose its adoption.
3. **Be approved by an appropriate authority.** Standards must be implemented and supported by more than just IT security. Therefore, it is imperative that standards be "championed" and approved by an overarching authority (e.g. at the C-level). Failure to do so creates a risk that the standard will not be acknowledged and fully implemented across the enterprise.
4. **Be concise.** The wordiness of your description of a standard is inversely proportional to the number of people who will take the time to read it.
5. **Be clear.** Unclear standards lead to ambiguous, inconsistent and interpretive implementations. Standards must clearly state what the objective is in terms that all stakeholders will understand.
6. **Stick to the WHAT.** Standards must clearly state the end-state objective and resist the temptation to delve into how it is to be achieved. Often there are many ways by which a standard can be implemented. This is best left to those who must deploy and execute the standard (as long as it achieves the desired outcome).
7. **Ensure viability.** There is little sense in describing a solution that cannot be achieved in practical business or technical terms. For that reason, those developing the standards must work in partnership with other stakeholders to ensure viability (see Be collaborative).
8. **Ensure auditability.** To be effective, standards routinely must be monitored for compliance. Human nature is such that where monitoring or compliance reviews of a standard are not being done, the standard increasingly will be ignored and its effectiveness will quickly erode. Audit is a key tool in this regard (see Measuring standards compliance, Page 10).
9. **Build in traceability.** Ensuring that standards can be directly traced to an enterprise's policies, as well as external standards, not only demonstrates the importance of the standard, but also assists in updating those standards if the associated policies and external standards change.
10. **Update regularly.** Ensure that cybersecurity standards are regularly reviewed and updated. Policies, technologies and threats are all subject to change, and the standards must also change if they are to remain relevant. Failure to do so will eventually mean that the standard will be considered obsolete and ignored.

UNDERSTANDING A CYBERSECURITY STANDARD

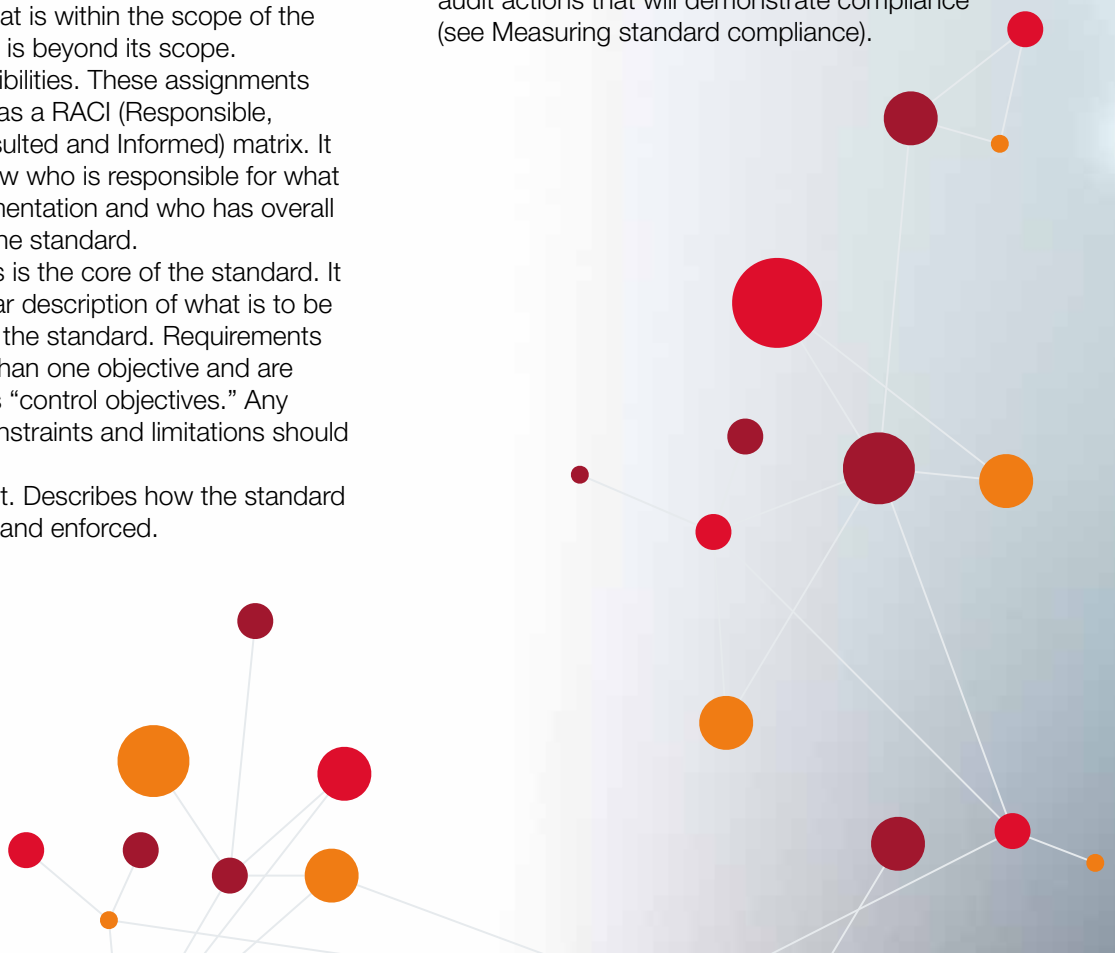
Cybersecurity standards usually are expressed in written form, especially if they include complex requirements. Having standards created as a document, at least by category (e.g. Access Control standards), also allows standards and associated controls to be reviewed by relevant stakeholders and approving authorities more easily.

The following are the minimum content requirements for a typical standards document. Bear in mind the need for both clarity and conciseness in each area:

- Catalogue or tracking number of the standard.
- Effective date.
- Approving authority. This should be an executive authority.
- Key references. This should include associated policies.
- Purpose. This is the purpose for which the standard is created.
- Objectives. These are the outcomes that the standard is intended to achieve.
- Scope. Defines what is within the scope of the standard and what is beyond its scope.
- Roles and responsibilities. These assignments can be expressed as a RACI (Responsible, Accountable, Consulted and Informed) matrix. It is important to know who is responsible for what parts of the implementation and who has overall accountability for the standard.
- Requirements. This is the core of the standard. It must include a clear description of what is to be achieved to satisfy the standard. Requirements can include more than one objective and are often referred to as “control objectives.” Any implementation constraints and limitations should also be described.
- Compliance & audit. Describes how the standard is to be monitored and enforced.
- Exception management. Describes the process by which exceptions to the standard are to be approved and by whom.
- Dependencies. Describes related standards upon which there is a dependency. As an example, an Access Control standard may have a dependency on a separate standard for User Authentication or Privilege Management.
- Related external controls. A mapping or cross-reference to external controls or regulatory requirements that are related to this standard.
- Maintenance of the standard. Describes when or how often the standard is to be reviewed and updated and by whom. A revision table should also be provided.

The following is optional, but should be considered to facilitate testing and auditing:

- Testing and audit method. A description of how the effectiveness of the standard (or its integral control objectives) should be tested or compliance with the standard should be measured; this may consist of a brief description of specific tests or audit actions that will demonstrate compliance (see Measuring standard compliance).



CREATING A STANDARDS MATRIX

Standards are often summarized in a tabular matrix, such as a spreadsheet, which can also be referred to as a control profile. Regardless of whether standards are described in a documented form, the creation of this matrix is important. It allows a single, high-level view of an enterprise's standards and associated controls, thus facilitating management and allowing a better understanding of the relationship between standards. It is also invaluable for compliance testing and audit purposes.

Measuring standards compliance

Measuring standards compliance and effectiveness is necessary for meeting objectives in a sustained manner. Otherwise, there is little incentive for those responsible for implementation to comply, and the risks the standard is designed to address will not be mitigated. The method or type of measurement should be selected to satisfy business objectives and regulatory requirements.

"…my access to [major corporate targets] depended upon the willingness of people to bypass policies and procedures that were in place for years before I compromised them successfully."

Kevin Mitnick, American computer security consultant, author, and hacker, best known for his high-profile 1995 arrest for various computer and communications-related crimes

CERTIFICATION

Certification is an attestation of compliance, generally arising from an external audit, that an enterprise, service, or system complies with a stated set of standards. Most standards bodies do not actually conduct certifications themselves. Instead, external audits are performed by qualified independent auditors to attest that a particular set of standards are being met. Thus, the successful audit report and statement of compliance represents the certification.

Certification can also be conducted against internal standards. Larger enterprises may have a defined process in which new (or significantly modified) services or systems are evaluated prior to becoming operational. The purpose of this evaluation is to assess whether or not the enterprise's security policies and standards have been satisfied and, if not, what the residual risk is to the enterprise. Traditionally, this has been referred to as a "certification & accreditation" process.

In addition to being a useful scorecard for how risks are being managed, certifications can also represent a valuable asset to the enterprise by allowing them to claim conformance with well-known industry security standards, thus providing potential clients with assurance of the enterprises's security diligence and integrity.

TESTING & EVALUATION

Testing is often necessary to ensure that standards have been properly implemented and effectively achieve the objectives of the standards or the controls within them. As an example, scanning systems to detect missing security patches and updates would be one way of testing to ensure compliance with a Patching Standard. In other instances, testing may involve the development and execution of test cases, based on the stated objectives of the standard or its controls.

New systems and services should be tested for compliance with all relevant standards immediately upon deployment (or prior to deployment if a realistic staging environment is available), then retested periodically thereafter at intervals consistent with the enterprise's operational cycle, as well as its security and risk posture. Due to the continually changing nature of IT systems, annual testing is recommended.

AUDIT & REVIEW

Testing and evaluation is intended to determine the compliance status and effectiveness of a standard at a given point in time. Audits and reviews help determine if a standard and its processes are being consistently applied over a period of time.

Reviews are usually conducted internally, with the results reported to senior management and governance authorities. Audits, however, can be conducted by internal or external assessors, but in all cases the assessors should be independent of those responsible for the day-to-day implementation of the standard.

MEASURING THE IMPACT OF NON-COMPLIANCE

Anomalies, shortfalls and gaps identified through testing, evaluation, reviews, or audits should be assessed and expressed as risks to the enterprise. Such risk statements must identify the potential impact to the business mission, operations and services, privacy, assets (including both systems and data), as well as reputation.

Additionally, risks and their projected impacts should be assigned a severity rating, usually based upon the enterprise's risk management strategy and policy, as well as its asset sensitivity definitions. Typically such severity ratings are categorized as LOW, MEDIUM, HIGH and CRITICAL.

Senior management awareness

Ultimately, senior management is held accountable for managing risk within their enterprise. As a result, they must be aware of serious risks arising from the compliance assurance activities described above. Once appropriately informed, senior management should either accept the risks as part of an informed business decision, or ensure that the resources necessary to facilitate their mitigation are available.

It is not necessary for senior management to be informed of every instance of non-compliance. Instead, only the most severe risks are escalated to that level, depending on the enterprise's risk management strategy and policy. The usual vehicle for informing senior management is through the use of a risk register.

USING A RISK REGISTER

Employment of a risk register is becoming increasingly common as a means of ensuring that all key stakeholders, including senior management, are aware of severe risks that could potentially impact an enterprise, and for tracking the status and disposition of those risks to the point of acceptance or mitigation. As such, use of a risk register is a common best practice for security governance and enterprise risk management.

The risk register is typically updated and presented to stakeholders and senior management at regular intervals (e.g. quarterly) at a senior security and risk management venue, such as a Security & Risk Steering Committee.

The risk register is generally presented in tabular form and includes a description of the risk, its potential impact, plans to mitigate the risk, and its ultimate disposition. Risks tracked include all those with a potential impact upon the business or enterprise that is deemed sufficiently severe as to merit escalation to senior decision-makers.

Typical examples would be risks categorized as CRITICAL or HIGH, including those arising from cybersecurity vulnerabilities and standards non-compliance, depending on the enterprise's risk tolerance, risk management strategy and risk categorization policy.

Ultimately, senior management is held accountable for managing risk within their organization. To do so, they must be aware of serious risks.

Conclusion

On balance, cybersecurity standards respresent the crucial means by which an enterprise ensures that their security strategy and policies are implemented in a consistent and measurable manner in day-to-day operations.

Standards can be simple to adopt or create. However, in all cases a sufficient diversity of stakeholder involvement must be considered to ensure that they are viable and have the desired effect without adversely impacting business operations. Once adopted, standards must also be measured regularly for implementation and compliance, otherwise their effectiveness will erode over time and the risks they are designed to address will not be mitigated.

Adopting standards will require an investment, but that investment is minimal when considering the potential impact caused by a major cybersecurity incident. Moreover, that investment will also result in increased trust and confidence on the part of the all stakeholders, including senior management, boards of directors, regulatory bodies, shareholders, customers and the public.

CGI

About CGI

Founded in 1976, CGI is among the largest IT and business consulting services firms in the world. Operating across the globe, CGI delivers end-to-end capabilities, from IT and business consulting to systems integration, outsourcing services and intellectual property solutions, helping clients achieve their goals, including becoming customer-centric digital enterprises.

CGI's cybersecurity capability has global breadth and depth, bringing to our clients in government and industry world-class expertise in managed security services, cybersecurity consulting, and evaluation services. Enterprises look to CGI to help assess security risk, design secure systems and infrastructure, and operate the business with confidence. Cybersecurity is part of everything we do: security controls are baked-in, not bolted on as an afterthought.

CGI has particular expertise and experience helping our clients to develop effective cybersecurity governance and risk management measures to meet threats in today's increasingly connected digital world.

Contact us to see how we can help you:

Email: info@cgi.com