There are myriad standards, frameworks, legislation, guidelines, and best practice references that can inform information security managers about how security controls should be implemented. A fair proportion of this guidance is country specific, especially where data protection and privacy rules apply, further supported by a plethora of industry-specific guidance that can help information security managers advise their executive managers on the best controls to implement to keep the business safe and secure.

As a security manager it pays dividends to align yourself with your organization's legal team so that you garner an understanding of the context of your business and take this back to the security governance team to ensure that these legislative requirements are represented as technical and procedural security controls and embedded into the organization's culture.

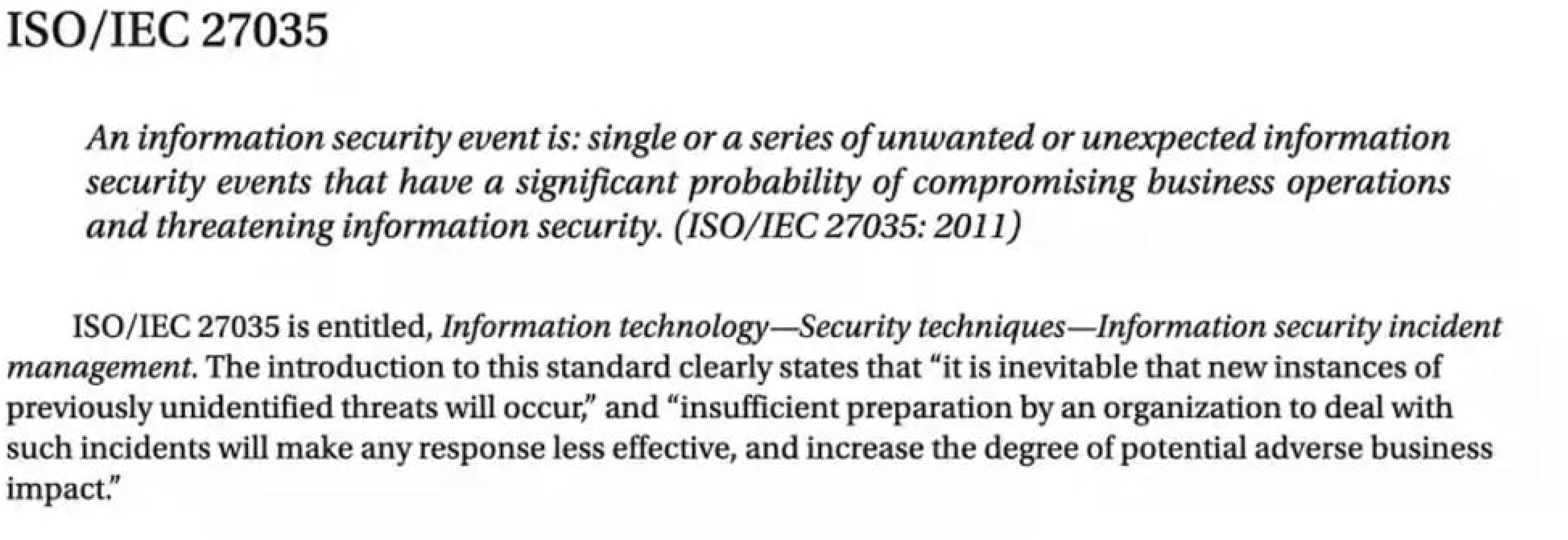
The range of standards within the ISO/IEC 27000 series cover a variety of security management recommendations and best practices that can be adopted to help you build a fully comprehensive information security management system (ISMS).

ISO/IEC 27001

ISO/IEC 27001 is a specification for an ISMS. Being a standard, it is filled with words such as *shall*, denoting the requirements that must be met to be deemed compliant. Like other standards, you can be audited against the requirements it specifies and use the results of the audit to achieve official compliance and certification, which may be used to help you tender for business in certain markets and attest to your security capabilities in relation to customers, suppliers, and partners.

ISO/IEC 27002

ISO/IEC 27002 is not a standard, instead it is pitched as a “code of practice,” which really means it is simply a collection of guidelines that you can follow to meet the requirements of ISO/IEC 27001. Organizations can use ISO/IEC 27002 to help them prepare for an ISO/IEC 27001 implementation, however, compliance with ISO/IEC 27002 will never be tested, instead the specification of ISO/IEC 27001 will be what's used to deem you compliant or not. Some people refer to ISO/IEC 27002 as a control set. This is a good way to look at it, since it provides a series of individual controls that can be used to meet the higher level requirements of ISO/IEC 27001. As such, this means you can decide to not follow ISO/IEC 27002 at all, swapping it out for a completely proprietary control set—either one you have built yourself or one that is provided by your government, for example—and as long as the individual controls can be mapped to the requirements of the ISO/IEC 27001, you can still claim compliance and pass your audit.



ISO/IEC 27035

> *An information security event is: single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security. (ISO/IEC 27035: 2011)*

ISO/IEC 27035 is entitled, *Information technology—Security techniques—Information security incident management*. The introduction to this standard clearly states that "it is inevitable that new instances of previously unidentified threats will occur," and "insufficient preparation by an organization to deal with such incidents will make any response less effective, and increase the degree of potential adverse business impact."

This standard is designed as a reference that will help organizations and especially security operations teams:

- Detect, alert, and accurately assess security incidents
- Manage the response to security incidents so that the process is consistent and repeatable
- Assess the potential business impact of vulnerabilities that have not been exploited and inform the business as to how best to deal with them
- Report on the efficacy of the information security incident management process and ensure that the business learns from all previous incidents and vulnerabilities

threats originate from either internal or external actors and carry out unwanted activities or have intent to carry out something that will have an adverse effect on the business. Threat actors are looking for ways to exploit vulnerabilities or weaknesses in your systems in order to affect the confidentiality, integrity or availability of your information (either systems or services), leading to some kind of harm. Figure 1 is taken from the ISO/IEC 27035 standard and shows the relationship between all the different objects that comprise the information security incident chain. Objects that are shaded are pre-existing and are materially affected by the unshaded ones, leading to an incident.

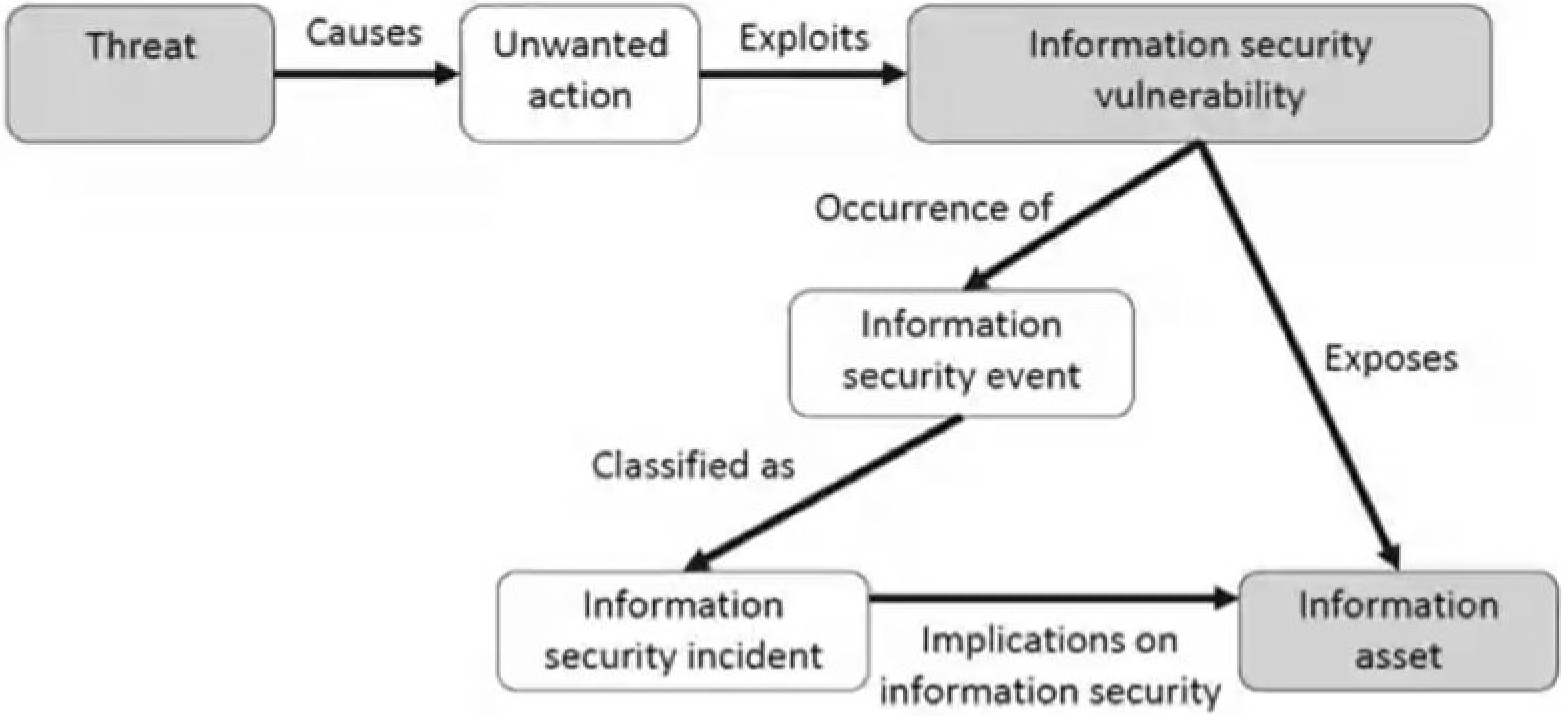

Threat
Causes
Unwanted action
Exploits
Information security vulnerability
Occurrence of
Exposes
Information security event
Classified as
Information security incident
Implications on information security
Information asset

Figure* _ *1.* *Relationship of objects in an information security incident (ISO/IEC 27035:2011)

The main focus of the rest of the standard is to ensure that you build a standard, repeatable process for managing incidents that allows you to improve information security management in general, helping build a consistent approach to reducing adverse business impacts (based on a risk-management approach), which leads to feedback from each incident informing the security team how to strengthen the organization to become more resilient to information security incidents in the future.

List of Published ISO/IEC 27000 Standards

Table 1 contains a complete list of all the ISO/IEC 27000 series of standards currently published. There are others in preparation, covering topics such as intrusion prevention, storage security, network security, and digital evidence, so it's worthwhile making contact with a standards organization and subscribing to their bulletins so you know when these new standards are published.

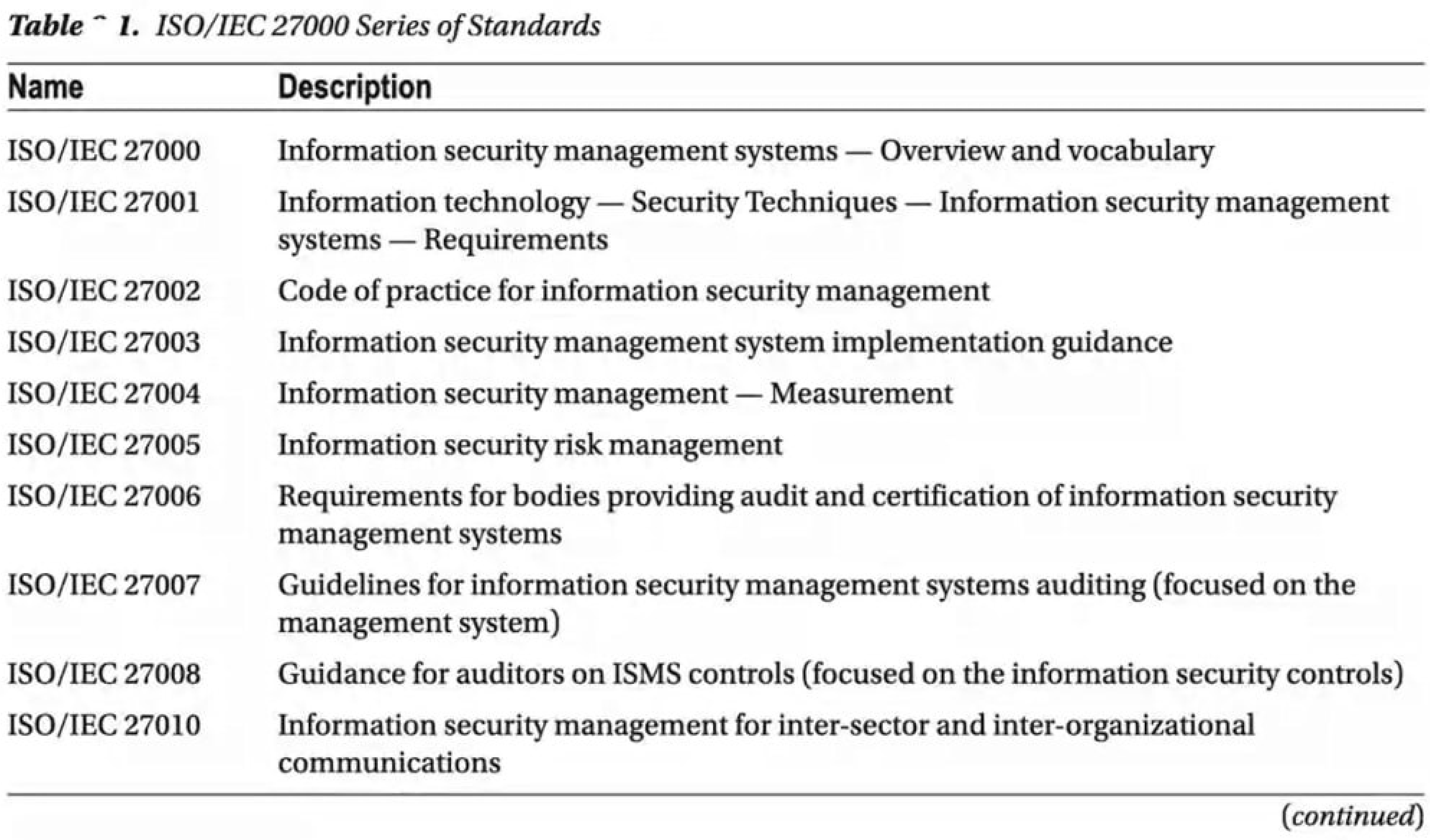


Table ~ 1. ISO/IEC 27000 Series of Standards

Name	Description
ISO/IEC 27000	Information security management systems — Overview and vocabulary
ISO/IEC 27001	Information technology — Security Techniques — Information security management systems — Requirements
ISO/IEC 27002	Code of practice for information security management
ISO/IEC 27003	Information security management system implementation guidance
ISO/IEC 27004	Information security management — Measurement
ISO/IEC 27005	Information security risk management
ISO/IEC 27006	Requirements for bodies providing audit and certification of information security management systems
ISO/IEC 27007	Guidelines for information security management systems auditing (focused on the management system)
ISO/IEC 27008	Guidance for auditors on ISMS controls (focused on the information security controls)
ISO/IEC 27010	Information security management for inter-sector and inter-organizational communications

(continued)

Table ˉ 1. (*continued*)

Name	Description
ISO/IEC 27011	Information security management guidelines for telecommunications organizations
ISO/IEC 27013	Guideline on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1 (for service management)
ISO/IEC 27014	Information security governance
ISO/IEC 27015	Information security management guidelines for financial services
ISO/IEC 27017	Code of practice for information security controls based on ISO/IEC 27002 for cloud services
ISO/IEC 27018	Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
ISO/IEC 27031	Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
ISO/IEC 27032	Guideline for cybersecurity
ISO/IEC 27033	Five-part standard dealing with network security issues, such as reference networking scenarios and secure communications
ISO/IEC 27034	Application security
ISO/IEC 27035	Information security incident management
ISO/IEC 27036	Information security for supplier relationships — Part 3: Guidelines for information and communication technology supply chain security
ISO/IEC 27037	Guidelines for identification, collection, acquisition and preservation of digital evidence