Comparison of the Core NIST and ISO Security Control Categories

By Thomas M. Smith, CD, CISSP

September 2016

ABSTRACT

Whether an organization is adhering to the International Organization for Standardization (ISO) Code of practice for information security controls (ISO 27002) or the core controls provided in the National Institute of Standards and Technology (NIST) *Framework for Improving Critical Infrastructure Cybersecurity*, the end products will be very similar and achieve the same results: good security management practices.

This paper outlines the salient points of each document and a mapping of the similarities in the control functions and categories provided by each standard. When an assessment is necessary to support whether to adhere to either set of good practices, this paper can guide the decision makers.

Introduction

Selecting and implementing information security controls should always have an established security management framework to support the implementation, maintenance and improvements to the controls one selected.

Both the ISO Standard and the NIST provide good frameworks around which the selected controls can be adequately managed. Ideally, the supporting framework must be capable of being tailored to the organization to meet their specific needs and requirements as opposed to merely being foisted upon the organization due to policy or other mandated needs. [1]

When determining which controls are appropriate there are many considerations that must be taken into account such as:

- *Are the controls mandated by policy?*
- *Are the controls required by contractual agreements?*
- *Are the controls necessary to manage specific or general risks?*
- *How will the controls be maintained?*
- *What level of robustness is necessary for each control implementation?*
- *What are the cost considerations?*

Ideally, these questions should be addressed as part of an overall assessment when selecting the actual controls to be implemented.

NIST Core Control Functions and Categories

The NIST Cyber Security Framework core provides a wide variety of categories of security based on the functions to be performed by the controls such as:

- *Identify* – Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.
- *Protect* – Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.
- *Detect* – Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.

[1] Both frameworks will be evaluated in a separate white paper.

- *Respond* – Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.

The controls are then provided according to a category associated with each of these functions:

Identify	• *Asset Management*
	• *Business Environment*
	• *Governance*
	• *Risk Assessment*
	• *Risk Management Strategy*
Protect	• *Access Control*
	• *Awareness and Training*
	• *Data Security*
	• *Information Protection Processes and Procedures*
	• *Maintenance*
	• *Protective Technology*
Detect	• *Anomalies and Events*
	• *Security Continuous Monitoring*
	• *Detection Processes*
Respond	• *Response Planning*
	• *Communications*
	• *Analysis*
	• *Mitigation*
	• *Improvements*
Recovery	• *Recovery Planning*
	• *Improvements*
	• *Communications*

Comparison of the Core NIST and ISO Security Control Categories

Each of these functional categories provide a detailed and comprehensive selection of security controls that must be considered for selection and implementation.

ISO Security Functions and Categories

The management functions for security within ISO are provided in the ISO 27001 Standard and include the following:

- *Business Context*
- *Leadership*
- *Planning*
- *Support*
- *Security Operations*
- *Performance evaluation*
- *Continual Improvements*

The majority of the ISO controls are provided in the Annex to ISO 27001 Standard and these are grouped according to the following categories:

- *Information Security Policies*
- *Organization of Information Security*
- *Human Resources Security*
- *Asset Management*
- *Access Control*
- *Cryptography*
- *Physical and Environmental Security*
- *Operations Security*
- *Communications Security*
- *System Acquisition Development and Maintenance*
- *Supplier Relationships*
- *Information Security Incident Management*
- *Information Security*
- Aspects of Business Continuity Management
- Compliance

Comparison of the Core NIST and ISO Security Control Categories

Implementation requirements and guidance for the controls themselves that are applicable to each category are provided in a separate document, the ISO 27002 Standard.

Comparing the Categories of Controls

While the actual controls that are applicable to the categories can also be compared and it can be determined that they are almost identical, the content related to the categories are also similar as indicated below:

NIST	ISO
Access Control	*Access Control*
Analysis	*Information Security Incident Management*
Anomalies and Events	*Information Security Incident Management*
Asset Management	*Asset Management*
Awareness and Training	*Human Resources Security*
Business Environment	*Business Context*
Data Security	*Cryptography*
Detection Processes	*Operations*
Governance	*Leadership*
Improvements	*Continual Improvements*
Information Protection Processes and Procedures	*Operations*
Maintenance	*Physical and Environmental Security*
Mitigation	*Planning*
Protective Technology	*Communications*
Risk Assessment	*Planning*
Risk Management Strategy	*Planning*
Recovery Planning	*Information Security Incident Management*
Response Planning	*Information Security Incident Management*
Security Continuous Monitoring	*Information Security Incident Management*

Comparison of the Core NIST and ISO Security Control Categories

Each of these sets of categories provide excellent security controls that can be implemented either as a baseline set of controls or abased on managing specific or general security risks.

It is also worthy of note that ISO no longer mandates the use of all of the controls themselves as outlined in Annex A to the ISO27001 Standard, Organization choosing to adopt the ISO standard(s) may select each control based on justifications for using/not using the control. As well ISO permits the use of other controls besides the set in the Annex.

NIST establishes a framework for selecting the controls, with particular emphasis on legal, regulatory and civil liberties requirements and expectations among other needs and obligations.

Summary

It should be noted that there are many overlaps in most of the categories and functions, especially when selecting the recommended controls in each category. Nonetheless, if an organization chooses to select controls using a risk-based approach, they will be well served by either of these two approaches.

Bibliography

BSI standards Publication, Guidelines for auditing management systems, ISO 19011:2011

ISO Information technology — Security techniques —Information Security Management Systems – Requirements, ISO/IEC 27001:2013

ISO Information technology —Security techniques —Code of practice for information security controls, ISO/IEC 27002:2015

NIST, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0, February 12, 2014.