Standards Crosswalk
NIST 800-161rev.1
ISO 27001 and 27036
NASA Solutions for Enterprise-Wide Procurement

Executive Sponsors: Joanne Woytek (Program Director), Theresa Kinney (Deputy Director), and George Nicol (Deputy Director)
NASA Solutions for Enterprise-Wide Procurement

Study Lead: Jon Johnson, Strategic Advisor,
NASA Solutions for Enterprise-Wide Procurement

EXECUTIVE SUMMARY

Issues and concerns around the federal supply chain remain prevalent in today's federal sector. Policy makers and cognizant federal agencies are working hard to implement initiatives that can help secure the information found within federal systems, reduce risk through current manufacturing practices and reshoring incentives, and elevate the transparency and accountability surrounding cyber risk throughout the federal supply chain.

NASA SEWP as a program believes in the use of commercial standards as a means to help address this need. This is a call often lamented by federal CIOs when speaking about issues around security, identity, or other seemingly intractable problems that they face. The call to use commercial standards is understandable as it means that we have to speak in a language that industry understands, and considers industry practices.

The National Institute of Standards and Technology issues publications that serve as the language of government. They are recommendations for applying particular practices or controls in the federal sector to address certain technical problems around ICT systems, security, identity, risk, and a host of other issues. What many do not know is the inter-relationship between the commercial standards and practices leveraged by industry and the NIST recommendations applied within the federal sector. This analysis can be considered a case study in showing that relationship.

This analysis focuses on the relationship between NIST C-SCRM recommendations found in 800-161rev.1 and some of the ISO standards identified by NIST that influenced what they created. As you see in the analysis, these standards map to many of the recommended controls that NIST asks agencies to consider when engaging in buying decisions.

However, it is important to note this analysis does not claim sufficiency in addressing cyber risk in the federal sector. In other words, ISO standards are in-and-of themselves not proof of fit to a particular need, or under particular conditions. That determination would be based on the context of what is being bought, for what purposes, to advance what mission. Further, both commercial standards and NIST recommended practices change over time, so what may be relevant today may not tomorrow.

What can be concluded, however, is that a relationship exists between ISO standards and NIST recommendations, and leveraging commercial standards can be seen as a starting point if applied knowledgably and appropriately.

THE BACKGROUND

The Federal Acquisition Security Act of 2018[1], Section 889 of the 2019 National Defense Authorization Act[2], the Biden Administration's executive orders[3], and bi-partisan congressional action point toward a continued focus on securing various aspects of the nation's supply chain. In 2021, the NASA SEWP program initiated a study mapping commercial Supply-Chain Risk Management standards to recommendations found in existing federal publications.[4][5][6] The study concluded that ISO 20243, the first internationally accepted standard for SCRM, mapped to portions of the controls recommended by NIST in their publications, particularly those requiring a transactional line-of-sight between manufacturer and customer, to maintain product integrity (found in NIST IR 7622) and in some of the control sets in 800-161 (that were particular for addressing hardware counterfeit and malicious product tainting). That study validated the potential use of these standards by federal acquisition personnel, and resulted in an increased adoption of these standards by federal contractors and its use of commercial standards in federal acquisitions.[7]

Upon the release of the initial crosswalk, NIST also released their update to their SCRM recommendations in the form of NIST SP 800-161 Rev.1.[8] This update resulted in the publication having a greater focus on the cyber elements of the supply-chain, and though the O-TTPS ISO/IEC 20243-1:2018for Supply-Chain Risk Management is cited as a foundational commercial standard NIST draws upon, the list and definitions of the recommended controls for critical systems draw upon other commercial standards for their inspiration. There are other international "standards and best practices" that NIST cites as foundational for their cyber supply-chain risk management recommendations cited in 800-161rev.1. These include ISO standards for System Engineering, Information Security, and Supplier Relationships.[9]

The program began extending the crosswalk to include the mapping of other ISO standards. The questions posed were:

---

[1] S.3085 - 115th Congress: Federal Acquisition Security Act. (Dec 18, 2018). https://www.congress.gov/bill/115th-congress/house-bill/2810

[2] HR.5515 - 115th Congress: John S. McCain National Defense Authorization Act. Section 889. Prohibition on certain telecommunications and video surveillance services or equipment. (Aug 13, 2018). https://www.congress.gov/bill/115th-congress/house-bill/5515/text

[3] .S. Library of Congress. Congressional Research Service. Summary of Selected Biden Administration Actions on Supply Chains, by Lida R. Weinstock. CRS Report Insight. Washington, DC: Office of Congressional Information and Publishing, June 14, 2022.

[4] Boyens, J., et al. "NISTIR 7622 (2012) Notional supply Chain risk management practices for federal information systems." National Institute of Standards and Technology, Maryland: 1-3

[5] Boyens, Jon, et al. "NIST Special Publication 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations." NIST. April (2015).

[6] Lord, Ellen "DOD Instruction 5000.90, Cybersecurity for Acquisition Decision Authorities and Program Managers", December 31, 2022, as amended

[7] Reference a few of the procurements found

[8] Boyens, J., et al. "Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations.(National Institute of Standards and Technology, Gaithersburg, MD), Second Draft NIST Special Publication (SP) 800-161, Rev. 1." (2021).

[9] Boyens, J. et al. (2021), pg. 15

- "To what extent can commercial standards be mapped to NIST recommended controls required of the supplier community?"
- Are accepted commercial standards and practices then able to be used in federal acquisitions to expedite a company's ability to assist the government's risk mitigation?"

This is not a unique activity (i.e., mapping the NIST recommended controls to their corresponding commercial standard(s)). For example, Appendix D of NIST SP 171 does the same as it specifically maps security controls found in SP 800-53[10] to the relevant security controls identified in ISO/IEC 27001. [11] Another example included the mapping of the NIST Privacy Framework to ISO 27707:2019 "Security Techniques…for Privacy Information Management".[12][13]

The federal SCRM dialog continues to evolve on this topic as solutions are sought for the complex problems of supply chains, and federal practitioners continue to seek guidance and recommendations on what is required of them and their supplier base. People now understand that the topic of Supply Chain Risk Management is equivocal; it means different things to different people depending on what part of the supply chain one chooses to focus on. There are distinctions between the government's resourcing/re-shoring/friend shoring initiatives; component availability risks due to the continued effects of the global pandemic; the security risks associated with the development and manufacturing of ICT and AV; information risks to the government, particularly without an auditable basis of agreements between prime and sub-contractors; and the risks associated with counterfeit items and malicious tainting of technical and scientific equipment used in critical systems.

THE STUDY'S PURPOSE, GOAL, AND OUTCOME SOUGHT

The *purpose* of this study is to see how well specific commercial standards map to NIST recommended controls found in NIST SO 800-161rev.1. The *goal* of this effort is to continue bringing awareness to the inter-relation between NIST recommended controls and standards and practices accepted by the commercial sector. One *intended outcome*, should a standard prove to meet a majority of recommended controls, would be to identify a means for government and industry to prove competency of practices and show how they may account for identified actions of federal suppliers recommended by NIST. Doing so advances the accounting of (*not the elimination of*) a baseline level of actionable cyber supply-chain risk management for federal buyers and their private sector partners.

THE CHALLENGE QUESTIONS

To what extent are ISO 27001 and ISO 27036 standards applicable to NIST 880-161rev.1? How do the standards relate to one another? Can they be mapped to determine if they complement or contradict one another? To what extent can they be used by agency buyers to help fulfill their obligations associated with NIST 161rev.1?

---

[10] UNIST, LJ. "NIST 800-53 Security and Privacy Controls for Information Systems and Organizations." (2017).
[11] Ross, Ron, et al. "NIST SP 800-171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, Revision 2, February 2020, National Institute of Standards and Technology (NIST)."
[12] https://www.nist.gov/privacy-framework/resource-repository/browse/crosswalks
[13] https://www.nist.gov/privacy-framework/resource-repository/browse/crosswalks/isoiec-27701-crosswalk-microsoft

THE METHODOLOGY/PROCESS/APPROACH

To answer the questions posed, NASA SEWP initiated this study and shared the results with standards bodies, NIST, and a collection of subject matter experts in industry and government. The purpose was to vet and assess the approach, conclusions, and implications laid out below.

This analysis builds on the 2021 study that mapped ISO 20243 to the control group found in 800-161 and NIST IR 7622. That study successfully identified how the standards mapped to particular controls found in the original version of 161, as well as the current SCRM recommendations NIST identified in 7622. That study also addressed 161rev.1 at a surface level, but the way NIST identified the practices developed by the OTTP had changed. Regardless, the study was able to build on the structure of that assessment.

NIST 800-161rev.1[14]

In 2021 NASA SEWP broke down the control group structure of NIST 161.rev.1. In approaching this analysis, this structure was revisited to ensure the controls were properly captured and organized.

The study breaks down and categorized the controls within the NIST framework. Each individually identified control had:

- A "Control Family" which indicated the area of interests similar to the ISO "Families"
- A "Control Number" and "Control" similar to the ISO "Groups" and "Standard Number"
- A "Control Enhancement" which was a step or activity that goes beyond those anchored in the existing, applicable NIST standards
- An indication as to the responsible parties ("Tiers") within a federal agency (Organizational Leadership – Tier 1, Mission/Business Owners – Tier 2, and System Owners – Tier 3)
- NIST SP References

[14] Authors note: It is interesting that the scope of NIST 800-161 was for "high impact systems" as identified in FIPS-199. This scope statement found in section 1.2 of 800-161 was eliminated, making the scope of this publication applicable to "C-SCRM encompasses a wide array of stakeholder groups that include information security and privacy, system developers and implementers, acquisition, procurement, legal, and HR. C-SCRM covers activities that span the entire system development life cycle (SDLC), from initiation to disposal. In addition, identified cybersecurity risks throughout the supply chain should be aggregated and contextualized as part of enterprise risk management processes to ensure that the enterprise understands the total risk exposure of its critical operations to different risk types (e.g., financial risk, strategic risk)."

Individual standards found within NIST 800-161rev.1 were generally organized accordingly:

Family > Control Number > Control Title > Control Description & Requirements > Responsible Party/Tier

For example:

Access Control > AC-1 > Access Control Policy and Procedures > Tiers 1, 2, 3 > NIST SP 800-12 & 800-100

Some controls would also have a "Control Enhancement" that would require activity beyond what is already required through guidance or statue.

For example, Incident Reporting is required for Incident Response has a Control Enhancement IR-6(3) (Incident Reporting - Supply Chain Coordination, further defines the control enhancement, and gives an indication of the responsible party (Tier 3 responsibility – System Owners).

This information was captured, arranged and aggregated for simplicity:

				Level		
Family	**Control Number**	**Control**	**Control Enhancements**	1	2	3
Access Control	AC-1	ACCESS CONTROL POLICY AND PROCEDURES				
Access Control	AC-2	ACCOUNT MANAGEMENT				
Access Control	AC-3	ACCESS ENFORCEMENT	REVOCATION OF ACCESS AUTHORIZATIONS, CONTROLLED RELEASE			
Access Control	AC-4	INFORMATION FLOW ENFORCEMENT	METADATA, DOMAIN AUTHENTICATION, VALIDATION OF METADATA, PHYSICAL OR LOGICAL SEPARATION OF INFORMATION FLOWS			
Access Control	AC-5	SEPARATION OF DUTIES				
Access Control	AC-6	LEAST PRIVILEGE	PRIVILEGED ACCESS BY NON-ORGANIZATIONAL USERS			
Access Control	AC-17	REMOTE ACCESS	PROTECTION OF MECHANISM INFORMATION			
Access Control	AC-18	WIRELESS ACCESS				
Access Control	AC-19	ACCESS CONTROL FOR MOBILE DEVICES				
Access Control	AC-20	USE OF EXTERNAL INFORMATION SYSTEMS	LIMITS ON AUTHORIZED USE, NON-ORGANIZATIONALLY OWNED SYSTEMS — RESTRICTED USE			
Access Control	AC-21	INFORMATION SHARING				
Access Control	AC-22	PUBLICLY ACCESSIBLE CONTENT				
Access Control	AC-23	DATA MINING PROTECTION*				
Access Control	AC-24	ACCESS CONTROL DECISIONS				

The color scheme is just to indicate the responsible parties within the federal sector:

Level	Name	Role	Generic Stakeholder
1	Enterprise	Executive Leadership	CEO, CIO, COO, CFO, CISO, Chief Technology Officer (CTO), Chief Acquisition Officer (CAO), Chief Privacy Officer (CPO), CRO, etc.
2	Mission and Business Process	Business Management	Program management [PM], project managers, integrated project team (IPT) members, research and development (R&D), engineering (SDLC oversight), acquisition and supplier relationship management/cost accounting, and other management related to reliability, safety, security, quality, the C-SCRM PMO, etc.
3	Operational	System Management	Architects, developers, system owners, QA/QC, testing, contracting personnel, C-SCRM PMO staff, control engineer and/or control system operator, etc.

Further, each control was identified to see if there was a corresponding action required by the supply base. Out of the 182 controls, 66 were identified (approximately 36% or just over 1/3) as a recommendation with identified accountability, responsibility, or action on behalf of the private sector supplier base:

				Supplier Action
Family	**Control Number**	**Control**	**Control Enhancements**	
Access Control	AC-1	ACCESS CONTROL POLICY AND PROCEDURES		X
Access Control	AC-2	ACCOUNT MANAGEMENT		X
Access Control	AC-3	ACCESS ENFORCEMENT	REVOCATION OF ACCESS AUTHORIZATIONS, CONTROLLED RELEASE	X
Access Control	AC-4	INFORMATION FLOW ENFORCEMENT	METADATA, DOMAIN AUTHENTICATION, VALIDATION OF METADATA, PHYSICAL OR LOGICAL SEPARATION OF INFORMATION FLOWS	X
Access Control	AC-5	SEPARATION OF DUTIES		X
Access Control	AC-6	LEAST PRIVILEGE	PRIVILEGED ACCESS BY NON-ORGANIZATIONAL USERS	
Access Control	AC-17	REMOTE ACCESS	PROTECTION OF MECHANISM INFORMATION	X
Access Control	AC-18	WIRELESS ACCESS		
Access Control	AC-19	ACCESS CONTROL FOR MOBILE DEVICES		
Access Control	AC-20	USE OF EXTERNAL INFORMATION SYSTEMS	LIMITS ON AUTHORIZED USE, NON-ORGANIZATIONALLY OWNED SYSTEMS — RESTRICTED USE	X
Access Control	AC-21	INFORMATION SHARING		
Access Control	AC-22	PUBLICLY ACCESSIBLE CONTENT		
Access Control	AC-23	DATA MINING PROTECTION*		X
Access Control	AC-24	ACCESS CONTROL DECISIONS		X

By identifying the domains of responsibility of the suppliers within NIST 800-0161rev.1, we had the basis of controls that we were then able to consolidate and provide a reference by which to map towards. We then began the process of organizing and understanding a set of ISO controls that were identified as key references for the team who created these recommendations.

ISO/IEC 27000/27001/27002

We then focused our attention on the 27000 series of ISO standards, first reviewing 27000:2018 "Information technology — Security techniques — Information security management systems — Overview and vocabulary"[15]. This gave an initial foundation on the language and structure of the ISO 27000 series.

The team then closely examined the ISO/IEC 27001:2022 "Information security, cybersecurity and privacy protection — Information security controls."[16]. This document identified control sets broken down by domain, by which companies seeking certification or credentialing should prove in order to be assessed.

[15] ISO, ISO. "IEC 27000: 2018 (E) Information technology–Security techniques–Information security management systems–Overview and vocabulary." International Organization for Standardization Std 27.000 (2018): 2018

[16] ISO, ISO. "IEC 27001: 2022 (E) Information security, cybersecurity and privacy protection – Information security controls." International Organization for Standardization Std 27.001 (2022): 2022

The introduction and sections 1-4 established the foundation, purpose, key terms and definitions, and structure of the document. This included a control layout which outlined the structure for the Organizational Controls (Section 5), People Controls (Section 6), Physical Controls (Section 7), and Technological Controls (Sections 8) identified in the document. Each control found in each section contained:

- A Control Title – A short name identifying the control;
- An Attribute Table – A table that shows the value of each attribute for the given control;
- Control – What the control is;
- Purpose – Why the control should be implemented;
- Guidance – How the control should be implemented;
- Other information – Explanatory text or referenced to other related documents.[17]

Appendix A provided a table of the security controls "directly derived and aligned with those listed in 27002:2022[18], Clauses 5-8." Through focusing on this appendix the team was able to address controls found in the subsequent documentation also identified by NIST as core standards used when developing 800-161rev.1, while also adopting a comparative framework by which to map controls.

The appendix table was adopted to identify, define, and categorize the ISO controls by:

Control Family > Control Title > Control Identifier > Control Definition

27001 Control Family and Definitions			
People Controls	Screening	6.1	Background verification checks on all candidates to become personnel shall be carried out prior to joining the organization and on an ongoing basis taking into consideration applicable laws, regulations and ethics and be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.
People Controls	Terms and conditions of employment	6.2	The employment contractual agreements shall state the personnel's and the organization's responsibilities for information security.
People Controls	Information security awareness, education and training	6.3	Personnel of the organization and relevant interested parties shall receive appropriate information security awareness, education and training and regular updates of the organization's information security policy, topic-specific policies and procedures, as relevant for their job function.
People Controls	Disciplinary process	6.4	A disciplinary process shall be formalized and communicated to take actions against personnel and other relevant interested parties who have committed an information security policy violation.
People Controls	Responsibilities after termination or change of employment	6.5	Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, enforced and communicated to relevant personnel and other interested parties.
People Controls	Confidentiality or non-disclosure agreements	6.6	Confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified, documented, regularly reviewed and signed by personnel and other relevant interested parties.
People Controls	Remote working	6.7	Security measures shall be implemented when personnel are working remotely to protect information accessed, processed or stored outside the organization's premises.
People Controls	Information security event reporting	6.8	The organization shall provide a mechanism for personnel to report observed or suspected information security events through appropriate channels in a timely manner.

For example:

Organizational Controls >

Privacy and Protection of Personally Identifiable Information (PII)>

Control Reference 5.34 >

[17] ISO, ISO. Page 9. 4.3 Control Layout. "IEC 27001: 2022 (E) Information security, cybersecurity and privacy protection — Information security management systems — Requirements." International Organization for Standardization Std 27.001 (2022): 2022

[18] ISO, ISO. "IEC 27002: 2022 (E) Information security, cybersecurity and privacy protection — Information security controls." International Organization for Standardization Std 27.002 (2022): 2022

> The organization shall identify and meet the requirements regarding the preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements.

This information was captured, arranged and aggregated for simplicity. The complete list of controls can be found in Appendix A of this document.

ISO/IEC 27036

An additional ISO standard used for reference by NIST in 800-161rev.1 is ISO 27036. This standard was created to advance cybersecurity considerations into the supplier relationships. This standard advances itself as being a corresponding standard to tightly couple with requirements found in ISO 27002 for Information Security Management, effectively pressing for the communication of standards and accountability down into their supplier relationships.

ISO 27036-1 "Cybersecurity — Supplier relationships — Part 1: Overview and concepts"[19] outlines this series of standards that focus on the supplier relationships. After reviewing the introduction, the requirements found in ISO 27036-2" Cybersecurity — Supplier relationships — Part 2: Requirements"[20] became the focus of this study, however the standards also include "Guidelines for information and communications technology (ICT) supply chain security" (27036-3) and "Guidelines for security of Cloud services" (27036-4).[21]

The scope, terminology, and document structure of ISO 27036-2 were outlined in sections 1-5. Section 6 "Information security in the supplier relationship management process" contained the cybersecurity requirements and controls for the agreement process, organizational project-enabling process, technical management process, and technical process. Section 7 "Information security in a supplier relationship instance" focused on the controls to include cybersecurity requirements in the supplier relationship planning process, supplier selection process, supplier relationship agreement process, supplier relationship management process, and the suppler termination process.

[19] ISO, ISO. "IEC 27036:1 2021 (E) Cybersecurity — Supplier relationships — Part 1: Overview and concepts." International Organization for Standardization Std 27.0361 (2021): 2021

[20] ISO, ISO. "IEC 27036:2 2022 (E) Cybersecurity — Supplier relationships — Part 2: Requirements." International Organization for Standardization Std 27.0362 (2022): 2022

[21] Future studies may look more deeply into 27036-3 and 27036-4 for federal considerations.

Two helpful tools in the appendix were quickly identified as useful. The first is found in Annex C "Objectives from Clauses 6 and 7." This appendix laid out in table form the 23 respective controls found in Sections 6 and 7 of this document as applied to the Acquirer (Buyer) and the Supplier (Seller) side of the contractual equation. This table was then replicated and aggregated for ease of analysis:

Acquirer		Supplier	
6.1.1 - Acquisition proces	Establish a supplier relationship strategy that is based on the information security risk tolerance of the acquirer; defines the information security foundation to use when planning, preparing, managing and; terminating the procurement of a product or service.	6.1.1 Acquisition process	None
6.1.2 Supply process	None	6.1.2 Supply process	Establish an acquirer relationship strategy that: is based on the information security risk tolerance of the supplier; is based on the information security risk tolerance of the supplier; defines the information security baseline to use when planning, preparing, managing and terminating the supply of a product or service.
6.2.1 Life cycle model management process	Establish the life cycle model management process when managing information security in supplier relationships.	6.2.1 Life cycle model management process	Establish the life cycle model management process when managing information security in supplier relationships.
6.2.2 Infrastructure management process	Provide the enabling infrastructure to support the organization in managing information security within supplier relationships.	6.2.2 Infrastructure management process	Provide the enabling infrastructure to support the organization in managing information security within supplier relationships.
6.2.3 Project portfolio management process	Establish a process for considering information security and overall business mission implications and dependencies for each individual project for those projects where suppliers or acquirers are involved.	6.2.3 Project portfolio management process	Establish a process for considering information security and overall business mission implications and dependencies for each individual project for those projects where suppliers or acquirers are involved.
6.2.4 Human resource management process	Ensure the acquirer and the supplier are provided with necessary human resources including screening requirements, confidentiality requirements, training and awareness to ensure personnel competences are regularly maintained and consistent with information security needs in supplier relationships.	6.2.4 Human resource management process	Ensure the acquirer and the supplier are provided with necessary human resources including screening requirements, confidentiality requirements, training and awareness to ensure personnel competences are regularly maintained and consistent with information security needs in supplier relationships.
6.2.5 Quality management process	Establish a quality management process when managing information security in supplier relationships.	6.2.5 Quality management process	Establish a quality management process when managing information security in supplier relationships.

This second helpful tool was found in Annex B "Correspondence between ISO/IEC 27002 controls and this document." This appendix provides a table that maps the controls identified to 49 control groups found in ISO 27002, and proved to be particularly useful when conducting the analysis.

THE ANALYSIS

By breaking down each individual standard document into their component controls or activities, the process of cross referencing drew out the overlap between the standards and controls in a manageable way. The recommended NIST controls for a C-SCRM baseline, applicable to the federal supplier base were identified, Information, including the number and description, for each control was captured in a spreadsheet and organized by NIST Control Families. Then each individual ISO standard was reviewed to see if an identified standard or description appeared to satisfy the associated NIST Control.

In the example below, the study looked at the Access Control Standard AC-4 for Information Flow Enforcement. The description of the control was captured. If ISO 27001 appeared to have a requirement that satisfied this control, their standard was identified (in this instance, organizational controls 5.19 and 5.21 appear to map to this recommendation). If ISO 27036-2 had a standard, control, or activity that also complimented the NIST control, it was acknowledged and also mapped. In this instance, control 6.2.1 "Lifecycle Management, ISO 27036" was identified as mapping to this control.[22]

NIST Control Family	CN	Control Description	Control Definition	27001 Control	27036 Activities
Access Control	AC-4	INFORMATION FLOW ENFORCEMENT	Supply chain information may traverse a large supply chain to a broad set of stakeholders, including the enterprise and its various federal stakeholders, suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers. Specifying the requirements and how information flow is enforced *should* ensure that only the required information is communicated to various participants in the supply chain. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.	(5.19) Processes and procedures shall be defined and implemented to manage the information security risks associated with the use of supplier's products or services. (5.21) Processes and procedures shall be defined and implemented to manage the information security risks associated with the ICT products and services supply chain.	(6.2.1 Life cycle model management process) - Establish the life cycle model management process when managing information security in supplier relationships.

[22] It will be noted again that the application of ISO 27036-2 appears less for the technical application to the NIST recommended control and more to ensure the cybersecurity controls flow down through the subcontracting agreements. Any control that required this contract "flow down" will be complimented by this particular standard.

This methodology was extended through the 66 controls identified as applicable to the supplier base.

800-171 – A Quality Review Shortcut

Once the mapping was initiated, the study had to impose quality control over interpretations. Fortunately, prior to conducting the individual mapping of NIST 800-161rev.1, NIST 800-171rev.2 was consulted. Although not directly related to NIST 800-161rev.1, this was an initiative undertaken by NIST to establish recommended controls for "Protecting Unclassified Information in Nonfederal Systems and Organizations" released this in Feb 2020.

Appendix D of NIST 800-171rev.2 provided a mapping of the supply-chain security controls found in ISO 27001 to the relevant security controls found in NIST 800-53rev.5 "Security and Privacy Controls for Information Systems and Organizations". NIST 800-53 serves as the anchor for the controls used by other NIST publications, including NIST 800-171rev.2 and NIST 800-161rev.1. Therefore, any control number of ISO 27001 that had been mapped by NIST 800-171 as being complimentary to that effort could be used to provide a quality review of the study's mapping.

The study found that 28 of the 66 supplier controls were identified by NIST as already being mapped in NIST 800-171rev.2. It was also discovered that 6 of the controls were found to have no relationship between the NIST controls and those found in the ISO standards. Not all of the NIST controls identified in 161, however, were identical to those found in 171. Therefore the remaining 22 NIST and associated standards map were revisited and reinterpreted for consistency. The study ensured that the mapping was modeled off the table and justifications provided in 171.

The Comparison

Each identified C-SCRM baseline or supplier control and their associated control number was captured on a spreadsheet. Those controls that came pre-mapped as indicated in NIST 800-171rev.2 were identified. The remaining controls were then compared to the ISO standard controls to see if there was a mapping.

Control Description	CN	Corresponding ISO	171 /Control Mapped?
ACCESS CONTROL POLICY AND PROCEDURES	AC-1	27001	(5.15)Rules to control physical and logical access to information and other associated assets shall be established and implemented based on business and information security requirements.
ACCOUNT MANAGEMENT	AC-2	27001	Mapped in 171
ACCESS ENFORCEMENT	AC-3	27001	Mapped in 171
INFORMATION FLOW ENFORCEMENT	AC-4	27001	Mapped in 171
SEPARATION OF DUTIES	AC-5	27001	Mapped in 171
REMOTE ACCESS	AC-17	27001	Mapped in 171
USE OF EXTERNAL INFORMATION SYSTEMS	AC-20	27001	Mapped in 171
DATA MINING PROTECTION*	AC-23	27001	(8.11) Data masking shall be used in accordance with the organization's topic-specific policy on access control and other related topic-specific policies, and business requirements, taking applicable legislation into consideration. (8.12) Data leakage prevention measures shall be applied to systems, networks and any other devices that process, store or transmit sensitive information.

Some of the NIST controls were met by considering a basket of ISO standard controls, as with the example below for "Policies and Procedures" required of the NIST Incident Response Control IR-1:

Control Description	CN	Corresponding ISO	171 /Control Mapped?
POLICY AND PROCEDURES	IR-1	27001	(5.19) Processes and procedures shall be defined and implemented to manage the information security risks associated with the use of supplier's products or services. (5.20) Relevant information security requirements shall be established and agreed with each supplier based on the type of supplier relationship. (5.21) Processes and procedures shall be defined and implemented to manage the information security risks associated with the ICT products and services supply chain. (5.22) The organization shall regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery. (5.23) Processes for acquisition, use, management and exit from cloud services shall be established in accordance with the organization's information security requirements. (5.24) The organization shall plan and prepare for managing information security incidents by defining, establishing and communicating information security incident management processes, roles and responsibilities. (5.25) The organization shall assess information security events and decide if they are to be categorized as information security incidents. (5.26) Information security incidents shall be responded to in accordance with the documented procedures. (5.27) Knowledge gained from information security incidents shall be used to strengthen and improve the information security controls.

Some of the NIST controls were accounted for by combining the Information Management requirements of 27001 with the Supplier Management activities found in 27236-2. For example, the definition for control AU-13 "Monitoring for Information Disclosure" requires communication of threat assessments as the recommended action of accounting within supplier agreements. In this instance a mapping is found by drawing from both standards to address that particular NIST control:

MONITORING FOR INFORMATION DISCLOSURE	AU-13	27001	27036	Monitoring as a capabilitiy is address in the organizational and technical controls, indicating technical monitoring oversight, and communication. The flowdown is a complimentary activity found in 27036. (5.22) The organization shall regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery. (8.16) Networks, systems and applications shall be monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents.

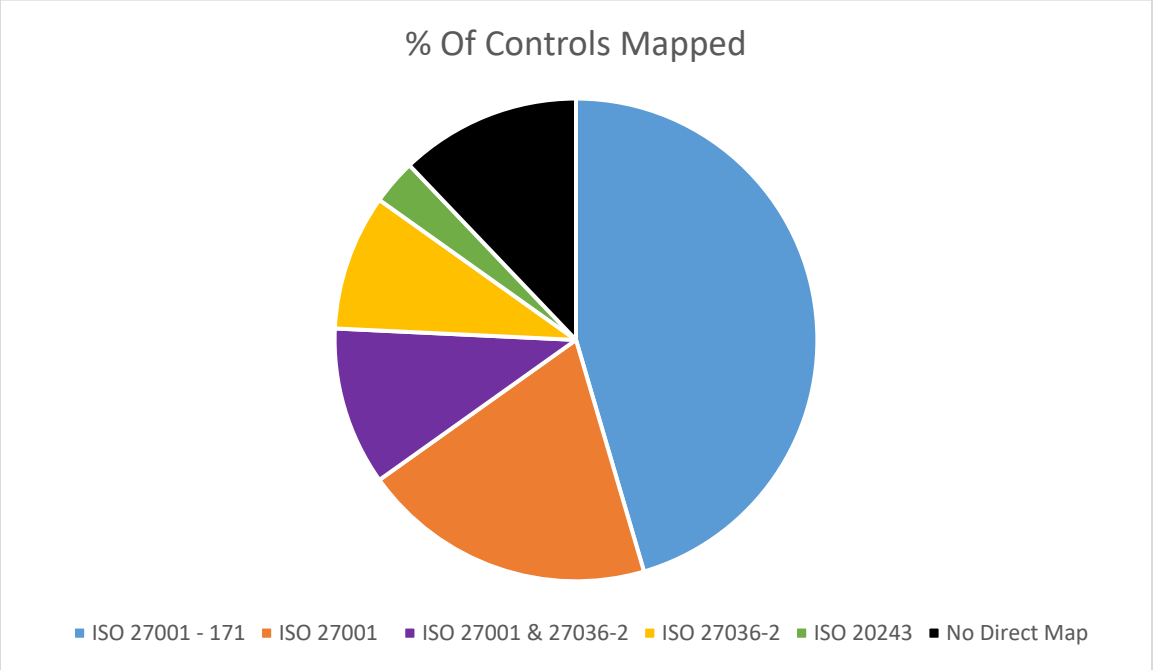
Still other NIST controls were only capable of being met by mapping exclusively to ISO 27236-2. For example, the definition for control IR-9 "Information Spillage Response" states that "The enterprise should include supply chain-related information spills in its information spillage response plan. This may require coordination with suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers. The details of how this coordination is to be conducted should be included in the agreement (e.g., contract). Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors." These supplier-management actions found within the agreements for their supplier base are kind of "flow-down" activities required of 27036-2:

Control Description	CN	Corresponding ISO	171 /Control Mapped?
INFORMATION SPILLAGE RESPONSE	IR-9	27036	27036-2

THE RESULTS

This results of this study was a clear mapping of control sets between those recommended for suppliers in NIST 800-161rev.1 and ISO 27001 and 27036-2.

- 30 of the 66 C-SCRM baseline and supplier controls were already mapped to ISO 27001 in NIST 800-171rev.2.
- 13 of the remaining 36 controls found in NIST 800-161rev.1 appear to map to the controls sets found in ISO 27001.
- 7 of the remaining 23 controls found in NIST 800-161rev.1 appear to be addressed by mapping to a combination of ISO 27002 and ISO 27036-2.
- 6 of the remaining 16 controls found in NIST 800-161rev.1 appear to map to the activity sets found in ISO 27036-2.
- The remaining 10 controls do not appear to have an attributable control capable of being cross walked to those controls found in ISO 27001 or 27036-2.
- 2 of these controls (SI-20 'Tainting' and SR-10 Inspection of Systems or Components) appear to map directly to ISO 20243 for Supply Chain Risk Management. This was not a scope of this crosswalk but a conclusion drawn from the prior SCRM crosswalk developed in the initial study.



THE CONCLUSIONS AND LIMITATIONS

This study leads to conclusions that could assist federal acquisition professionals in applying existing means to partially satisfy obligations required of NIST SP 800-161. The study draws the following conclusions based on the textual analysis and above described methodology:

Conclusions

- The study shows the extent to which ISO 27001 "Information security, cybersecurity and privacy protection — Information security management systems — Requirements" can provide a measure of risk management that agencies can consider to satisfy 65% of the C-SCRM baseline and supplier controls in NIST 800-161rev.1.
- The use of ISO 27001 is not sufficient to meet the recommendations for information flow down through the sub-contract agreements; a condition found in many of the NIST supplier controls. To meet this recommendation, an agency would want to consider the accompanying use of ISO 27036-2.
- Coupling ISO 27001 and 27036-2 accounts for 85% of the C-SCRM baseline and supplier management controls and activities recommended by NIST.
- Therefore, contracting officers and program offices in government can consider accepting ISO 27001 and 27036-2 standards in their requirements documents as a means to satisfy NIST recommendations and help mitigate (not eliminate) cyber supply chain risk.

Limitations

To be clear, there are a number of considerations that go into the asking and acceptance of standards by federal programs and contracting personnel. This analysis *does not* claim that ISO standards are sufficient to protect federal information within its walls and along with its industry partners. Further:

- We do not address the differences between self-attestation vs. audited certification of standards. Though self-attestation can give a program an indication that the provider or contractor has general awareness of particular practices associated with that ISO, it is not the same as a credentialing that has undergone a 3rd party audit verifying those practices.

- Regardless of an audited attestation, some agencies will want to know more because they deal with very sensitive or classified information. Due to the sensitivity of the information they hold, it is right for them to know more about the particular company practices that ensures proper safeguarding.
- Commercial standards and NIST recommendations change. To maintain awareness of how these inter-relate it will require maintaining a line of sight on how each evolve. Control sets, standard sets, or scope changes can affect how each relate to one another. What is true today will have to be revisited tomorrow.

****

The NASA SEWP program is committed to helping federal buyers understand the ever-changing environment, and uses its knowledge, area interest, and expertise to secure the federal government's supply chain. We have a unique role in the federal dialog as we understand both the concerns of the government and our industry partners. Through this assessment, we hope to inform federal buyers on the relationship between NIST Standards and ISO Controls for efficient vendor SCRM responsibilities, and provide the vendor community a pathway to address federal concerns. Finally, thank you to our government and industry colleagues who counseled us throughout this process, and vetted the results of this analysis.

If you have any questions, please email us at help@sewp.nasa.gov.