Cyber Supply Chain Standards Mapping and Roadmap

In a Nutshell: There are a surprising number of standards and guidelines for supply chain risk management. With this many resources, it can be difficult knowing where to start. Selecting the right standard that aligns to an organization's business needs involves settling on an overall risk management framework, understanding your sector and customers, and figuring out your specific role and priorities in the supply chain.

Why multiple standards? Cyber supply chain risk management is a multidisciplinary problem and successfully addressing it requires blending practices from across different organizational silos, industries, and vocabularies.

Organizations frequently do not neatly fall within a clear-cut designation established (somewhat artificially) by a standards body, and they usually have multiple regulatory standards for compliance. For example, the same company may be subject to HIPAA, PCI DSS, and, NERC CIP.

Use the Roadmap on the Following Page to Answer These Three Key Questions:

1. What cybersecurity standards and frameworks (if any) do you currently use? – use the columns in the upper part of the roadmap to guide you.
2. What is/are your industry sector(s)? – use the Sector-specific row in the map to guide you.
3. Where do you want to focus with respect to supply chain risk management? – use the rows on the lower part of the map marked by a large grey arrow.

Each column in the figure starts with the source document. If you do not currently have a framework, start with the NIST Framework. Draw on additional resources from the other columns if you feel it is necessary.

It's acceptable to use multiple documents if you want to augment your practices, as demonstrated by many companies. If you would like to augment your current program with additional resources feel free to use relevant documents from any column/row intersection in the figure. But, be careful to right-size the suite of documents to guide your cyber supply chain activities. Doing too much will overwhelm the individuals responsible for implementation and confuse the effort.

However, it is sufficient if organizations begin from focusing on a single column to build their programs and later, when they have at least somewhat matured their programs, draw in additional resources (listed in other columns, or obtained elsewhere).

Best Practices in Cyber Supply Chain Risk Management

Conference Materials

Roadmap for Selecting Applicable Cyber Supply Chain Standards:

	USING NIST	NO CURRENT FRAMEWORK	USING ISO/IEC	USING Sector-specific or Organization-specific
Security Framework	NIST RMF SP 800-53	NIST CSF	ISO/IEC 27001 ISO/IEC 27002	Sector-specific or Organization-specific
Cyber Supply Chain	NIST SP 800-161 NIST IR 7622**		ISO/IEC 27036 ISO/IEC 20243	FFIEC and OCC Guidelines IEC/ISA 62443-2-4 FS ISAC Third Party Software Security Control Types Cybersecurity Procurement Language for Energy Delivery Systems
Sector-Specific	NIST SP 800-82 NIST IR 7628	Energy Sector Cybersecurity Framework Implementation Guidance Cybersecurity and Risk Management Best Practices: CSRIC WG4	ISO/IEC 27011 ISO/IEC 27015 ISO/IEC 27019	NERC CIP; C2M2 CSRIC
Software Integrity	SAFECode Software Integrity Documents			
Delivery Security	ANSI/ESD S20.20-2007; C-TPAT; AEO; TAPA; Electronics Industry Citizenship Coalition (EICC); Dodd-Frank Conflict Mineral Requirements			
Counterfeits	SAE Standards			
Conformity Assessment	Common Criteria; The Open Group Trusted Supplier Program; A2LA Accreditation; ISO 9001 Certification			