

## Cyber-Supply Chain Risk Management Best Practices

### Interview Questions

- What is the organization's structure for managing supply chain risk? What roles are involved in risk management decisions?
- What are the key business drivers for allocating resources for cyber supply chain risk management?
- Where does the organization see benefits from effective cyber supply chain risk management?
- How does the organization identify supply chain threats, vulnerabilities and overall risks?
  - How are these risks prioritized or measured?
  - What does the organization consider to be major supply chain risks? (examples: quality or products (received or produced), supply chain resiliency, third-party cybersecurity, counterfeits)
- What requirements does the organization put in contracts and service agreements, e.g., security, quality, integrity, etc.? Can provide examples?
  - How does the organization monitor compliance with contractual requirements? How often?
- Has the organization ever felt a need to help a supplier improve their cybersecurity/supply chain practices?
- How does the organization vet or manage third-party suppliers/vendors?
  - Is the organization's cybersecurity considered? Evaluated?
  - If a questionnaire is used, is it a standardized questionnaire, or internally developed? Why?
  - If an audit is required, how are auditors chosen? - do they have cybersecurity expertise?
  - Are suppliers vetted differently depending on what they provide, their size, or some other reason?
  - What kinds of information are collected about suppliers?
- What methods does the organization use to protect their supply chain? (Especially from cybersecurity-related threats)
  - How does the organization assure quality and integrity of products/software they receive?
  - How does the organization track the provenance of a product?
  - How does the organization prevent tampering of products in the supply chain?
  - What methods for protecting supply chains have been most effective?
  - What key metrics does the organization track for cyber supply chain risk management? Is there an executive dashboard to capture and share those metrics?
  - With whom are those metrics shared?
- What standards or guidelines has the organization implemented to assure the quality, integrity, physical and cybersecurity of products?

OMB Control #: 0693-0043  
Expiration date: 03/31/2022

- Is supply chain risk included in cybersecurity policy? Is cybersecurity included in supply chain management policy?
- Does the organization have a plan to manage cybersecurity-related supply chain incidents?
- What makes implementing cyber-supply chain risk management difficult?
- What tools/techniques has the organization found most valuable in managing their supply chain risk?
- What resources would the organization suggest useful to organizations less mature in managing their supply chain risks?

This collection of information contains Paperwork Reduction Act (PRA) requirements approved by the Office of Management and Budget (OMB). Notwithstanding any other provisions of the law, no person is required to respond to, nor shall any person be subject to a penalty for failure to comply with, a collection of information subject to the requirements of the PRA unless that collection of information displays a currently valid OMB control number. Public reporting burden for this collection is estimated to be 60 minutes per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed and completing and reviewing the collection of information. Send comments regarding this burden estimate or any aspect of this collection of information, including suggestions for reducing this burden, to the National Institute of Standards and Technology, Attn: Celia Paulsen <[celia.paulsen@nist.gov](mailto:celia.paulsen@nist.gov)>.

OMB Control #: 0693-0043  
Expiration date: 03/31/2022