Healthcare & Public Health Sector Coordinating Councils

PUBLIC PRIVATE PARTNERSHIP

HEALTH INDUSTRY CYBERSECURITY SUPPLY CHAIN RISK MANAGEMENT GUIDE

October 2019

About the Health Sector Coordinating Council Joint Cybersecurity Working Group

The Healthcare and Public Health Sector Coordinating Council (HSCC) is a coalition of private-sector, critical healthcare infrastructure entities organized under Presidential Policy Directive 21 and the National Infrastructure Protection Plan to partner with government in the identification and mitigation of strategic threats and vulnerabilities facing the sector's ability to deliver services and assets to the public. The HSCC Joint Cybersecurity Working Group (JCWG) is a standing working group of the HSCC, composed of more than 200 industry and government organizations working together to develop strategies to address emerging and ongoing cybersecurity challenges to the health sector.

The JCWG Supply Chain Cybersecurity Task Group developed this supply chain cybersecurity risk management guide as a tool particularly targeted at smaller to mid-sized health organizations. The suggested best practices herein directly address recommendations made in the 2017 Health Care Industry Cybersecurity Task Force "Report on Improving Cybersecurity in the Healthcare Industry."

The Task Group is co-chaired by Darren Vianueva, Vice President of Technology Sourcing and Shared Services for Trinity Health, and Chris van Schijndel, Cybersecurity Director – Customer and Logistics for Johnson & Johnson.

Disclaimer

This document is provided for informational purposes only. Use of this document is not required nor does it guarantee compliance with federal, state, or local laws. Please note that the information presented may not be applicable or appropriate for all health sector organizations. This document is not intended to be an exhaustive or definitive source on safeguarding health information from privacy and security risks.

Table of Contents

Foreword from the Co-Chairs

The supply chain in the health industry is a complex eco-system of interdependent organizations of all sizes, spanning patient care, payment and data management systems, pharmaceutical and technology research and manufacturing, and public health administration. These interdependencies mean that a cybersecurity event in one organization is likely to have ripple-effects on multiple other links within the supply chain.

The effects of a cyber incident or disruption can include: loss of patient data and payment information; theft of intellectual property; or exploitation of medical device vulnerabilities that lead to disruption of functionality or patient harm. The growth of ransomware in recent years threatens the availability of critical systems, leaving organizations unable to provide services or products relied upon by patients and health professionals.

In response, larger organizations have dedicated resources to improve their resiliency. Many small-to-medium sized organizations, however, lack the scale or the budget to staff dedicated teams of cybersecurity experts.

To that end, this document – the Health Industry Cybersecurity Supply Chain Risk Management Guide (HIC-SCRiM) – is primarily written for leadership in small to medium sized organizations. It is intended to provide actionable guidance and practical tools to enable those organizations to manage the cybersecurity risks they face through their dependencies within the health system supply chain. The hope of the co-chairs is that by enabling these organizations to demand secure products and services from their suppliers, we will leverage market forces to raise the bar across the healthcare supply chain to the benefit of all.

While the guidance and tools presented here are aimed primarily at small and medium sized organizations, larger organizations are urged to:

1. Use their reach within the supply chain to disseminate this document to their suppliers and recommend that they incorporate these practices into their own organizations, encouraging their suppliers to do the same in turn.
2. Review their own supplier risk management program against the best practices laid out in this document.
3. Consider joining the HSCC Supply Chain Cybersecurity Task Group to actively shape health-sector supplier risk management. Please register your interest at https://healthsectorcouncil.org/contact/

Stakeholders consulting this resource are invited to provide any feedback to feedback@healthsectorcouncil.org so that the content can be improved periodically.

Chris van Schijndel & Darren Vianueva
HSCC Supply Chain Cybersecurity Task Group Co-Chairs
Health Industry Cybersecurity-Supply Chain Risk Management (HIC-SCRiM)

Executive Summary

Supply chain risk management is an ongoing process. This document provides guidance for health providers and companies on establishing a supplier risk management program involving new and existing suppliers, and how to sustain those activities operationally. It also provides specific templates that can be used as a starting point for your organization's needs.

Given the limitations of cybersecurity skills in small-to-medium size healthcare organizations, the target audience of this document include enterprise leadership and non-IT professionals who are responsible for supplier relationships within such organizations.

HIC-SCRiM is structured to support meeting the National Institute of Standards and Technology's Cyber Security Framework ("NIST CSF") supply chain security practices recently added in version 1.1 of the framework in April 2018. The content is also aligned to the Health Sector Coordinating Council Joint Cybersecurity Working Group's Health Industry Cybersecurity Practices (HICP) resource. The document has 3 sections that map to the NIST CSF "Identify" Function and "Supply Chain" Category (ID.SC-1 to ID.SC-3). The appendices comprise supporting templates and tools.

In the interest of presenting the sector with a useable guide as soon as possible, ID.SC-4 and ID.SC-5 are not covered in this version for lack of time, but are in process for version 2.

The three guidance sections cover the following topics:

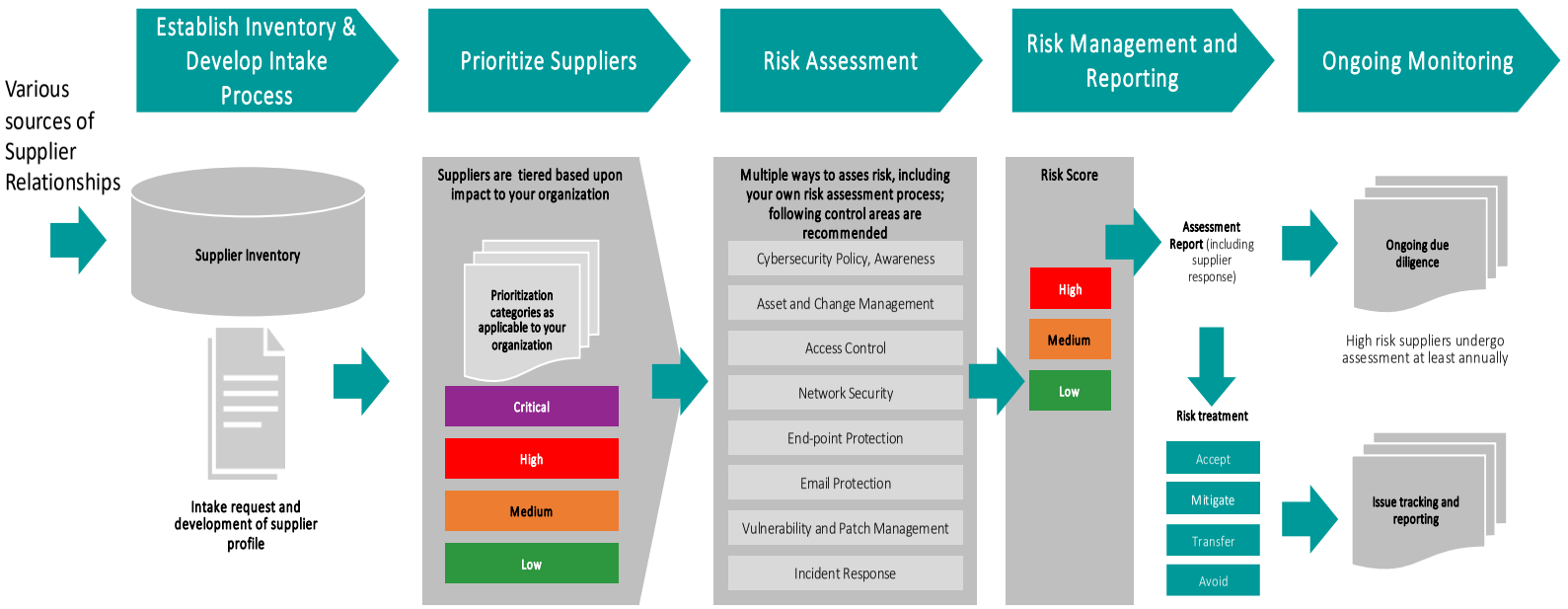
- The 'what' or components of supplier risk management program; e.g., policies and procedures, roles and responsibilities, and establishing overall governance.
- The 'how' or process of establishing and sustaining the supplier risk management program including inventory of suppliers, risk assessment and risk treatment guidance.
- Specific guidance and tools supporting the contract management process.

The Guide provides templates for supplier risk assessment, cybersecurity requirements and language for contracts, supplier inventory attributes, and supplier risk management policy. A process flow diagram is provided for an end-to-end view that links all the sections together.

Finally, the document provides a comprehensive glossary of the terms used in this document.

The infographic on the next page provides a pictorial view of the approach to supplier risk management as summarized above and described in detail in this document.

Supplier Risk Management End-to-End Process



A common process is followed to trigger the Supplier Risk management process, including leveraging a standard intake and utilization of a supplier inventory.

Based on the impact to your organization, suppliers are tiered to determine the level of due diligence required and the scope and depth of the assessment (e.g., evidence).

Gain assurance about the security posture of the supplier by leveraging various approaches to cover all risk areas applicable to your organization.

Risk assessment outcome drives the risk treatment. Risk treatment should be completed prior to contracting with a supplier. For existing suppliers, updates to contracts may be required.

Issue tracking and reporting is performed until issues are closed. Ongoing due diligence is performed based upon suppliers' assessed risk and tiering.

Background

The supply chain is responsible for the acquisition of goods and services from suppliers, which vary in their maturity of information security capabilities. Historically the health industry supply chain profession has relied upon information technology to manage and respond to risks and malware events independently of supply chain. However, cybersecurity risks and threats continue to evolve at an unprecedented rate, resulting in the health sector being susceptible to cyber exploitation. This exploitation often targets internet-connected devices, medical devices, long-lived legacy technology, cloud applications, third-party services and the free flow of suppliers in healthcare facilities. These targets can be exploited through numerous paths (vectors), ranging from a supplier servicing an asset, poor manufacturer security design and on-going patching, installed networks, loaner/rental devices, manufacturer default passwords, supplier applications interfaced into health systems, etc. The combination of exploits and exploitable targets is growing daily, allowing anyone from amateur hackers to malicious nation-state actors an opportunity to breach patient data, disrupt operations and/or cause patient harm.

Properly managing cyber risk within the supply chain requires a proactive strategy to protect patient information and sensitive data against an ever-increasing risk from bad actors outside, and sometimes within, the health system. A supply chain cybersecurity risk management program also serves as a strategy to support and increase preparedness and business continuity planning and countermeasures. This is not just an operational imperative, but a regulatory one, given the Health Insurance Portability and Accountability Act (HIPAA) as the primary governing regulation for the protection of patient information. This dynamic underscores the fact that cybersecurity is no longer an information technology issue but an organizational and health sector issue. It requires all healthcare stakeholders to be vigilant and practice good security hygiene at an individual, enterprise and cross-sector level to improve the security posture of the health industry.

Consequently, the U.S. Food & Drug Administration (FDA), the U.S. Department of Health and Human Services (HHS), and HHS Centers for Medicare and Medicaid Services (CMS) are ramping up requirements for healthcare and their suppliers to improve cybersecurity. This is evidenced by the FDA announcement of new cybersecurity requirements and guidance for suppliers, HHS and CMS statements of concern and recommendations for needed changes, and the launch of the HHS Health Sector Cybersecurity Co-ordination Center (HC3), in November of 2018.

In April of 2018, NIST released version 1.1 of its Cyber Security Framework (CSF). The NIST CSF and other security control references offer a proactive approach for leveraging acquirer and supplier relationships to reduce cybersecurity risks within healthcare. Using the sourcing process to award suppliers who offer better cybersecurity solutions provides the opportunity to create market forces for continuous supplier improvement.

Within the framework updates, a new category within the “Identify” function was introduced focusing on “Supply Chain Risk Management.”

The update included these five subcategories:

Function	Category	Subcategory
Identify (ID)	Supply Chain Risk Management (SC)	ID.SC-1: Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders
		ID.SC-2: Suppliers and third-party service partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process
		ID.SC-3: Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan
		ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations
		ID.SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providers

The remainder of this document will detail each subcategory. In the interest of presenting the sector with a useable guide as soon as possible, ID.SC-4 and ID.SC-5 are not covered in this version for lack of time, but are in process for version 2. The practical advice and toolkits within this publication are designed to help small to medium sized health organizations to identify, monitor and properly manage cyber risks within the supply chain.

Meeting NIST CSF Requirement ID.SC-1

Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders.

The requirement ID.SC1 identifies the need to understand the end to end process and lifecycle for supplier acquisition and management within your organization. The benefits of these good governance practices extend beyond cyber to supplier consolidation, sourcing efficiency, contract consolidation, and lost opportunities for volume discounts.

This section of the document speaks to the 'what'; the components of the supplier risk management program and the foundational groundwork required to manage supplier cybersecurity risk. Subsequent sections deal with the 'how'; the process that brings these components to life.

1) Definition of Supplier Risk Areas

Start by defining the risks that are most applicable to your enterprise.

The following risks should be considered and prioritized **depending on the mission of your organization** and the nature of the relationship with suppliers. It is recommended that cyber risk be considered in the broader context of supplier risk, to include other drivers of enterprise business risk. Specifically, the HIC-SCRiM recommends assessing and managing cyber risk and its impact across the suggested risk areas below:

Suggested risks to assess:

- Operational Risk
- Safety Risk (Patients, employees, contractors, etc.)
- Competitive Risk (intellectual property, trade secrets, go to market)
- Quality Risk (product quality/sabotage/illicit re-use or re-sale, product service integrity)
- Reputational Risk
- Compliance Risk (regulatory, legal)
- Secondary Risk (businesses, non-profits, others) and the broader supply chain ecosystem
- Geo-political risks

Potential Impact to your organization due to these risks:

- Operational Risk – impacting day to day operations
- Safety Risk – impacting patients, employees, contractors, etc.
- Competitive Risk – impacting ability to achieve goals (may include; intellectual property, trade secrets, go to market, etc.)
- Quality Risk – impacting products services and business practices (may include; product quality/sabotage/illicit re-use or re-sale, product service integrity, etc.)
- Reputational Risk – impacting damage to or loss of customer, business partner, or public confidence or perceived image
- Compliance Risk – impacting losses and legal penalties for failure to comply with laws and regulations
- Secondary Risk – transfer of risk to business partners (may include avoiding, reducing, or transferring risk)
- Geo-political Risk – impacts of political events or instability, trade barriers, taxes, or economies

2) Definition of Roles and Responsibilities

Using the outcome from step one (most relevant business risks), identify and enroll an executive sponsor to own the overall supplier cyber risk management program and establish program governance.

The purpose of this role is to provide governance, including:

- Set tone and communication
- Agree on goals, milestones and metrics
- Establish and communicate risk appetite for the organization
- Direct resources
- Remove blockers
- Receive updates on program status

This executive should be someone with the accountability for the business risks identified in step one, and authority to prioritize, influence and obtain organizational resources to address those risks. For that reason, high-level executive leadership is essential for success.

One method for structuring ownership and accountability within the enterprise is use of the "RACI" model – Responsible, Accountable, Consulted, Informed – which lays out roles and responsibilities for any activity or group of activities.

Ultimately, supply chain cybersecurity is a business risk, and not a technology risk.

Who is on Point?

For medium or larger organizations, consider the functional alignment of the proposed executive sponsor and their ability to influence and direct resources. For example, a chief procurement officer, head of enterprise risk committee or chief financial officer may be a better choice than an IT executive.

In addition, for medium and large organizations, a committee-based model is recommended and should include representation from Legal, Procurement, IT, Information Security, Privacy, Compliance, Quality, Facilities and others as relevant to your organization and mission.

3) Definition of Supplier Scope

Start by defining the term 'supplier' as it relates to your organization. For example, this term may include any individual or entity that provides any type of service and/or product to the organization. The word supplier may commonly refer to: supplier, vendor, service provider, consultant, external partner, third party or business partner etc.

Based on your definition, you will need to gather and document the entire inventory of your suppliers. You may need to consider multiple sources to gather this information, e.g. accounts payable, contracting, expense processes, etc. Knowing the size and scope before starting is important in order to prioritize resources and set realistic expectations on the size and complexity of the task. See SC.2 for guidance on this process and the accompanying template.

4) Establishment of Policies and Procedures

Having defined the scope, you will need to define or update the policies supporting the supplier risk management program at your organization to formalize the organization's supplier risk management approach.

4.1 Define/Update Policies

The organization's policies should drive the definition of supplier risk management metrics and reporting requirements in support of the program goals. Metrics should articulate the supplier risk posture and health of the supplier risk program in the context of the organization's key business risks (established above). The metrics and targets should therefore be agreed with the sponsor and should be biased toward driving risk posture improvements and showing progress over time, rather than point-in-time or activity-based measures.

Examples of metrics to consider are:

- Distribution of suppliers by risk tier (more on supplier risk tiering below)
- Distribution of suppliers by most relevant business risk impact
- Number of suppliers not covered by current security assessment (adherence to or coverage of supplier risk program vs. targets)
- Number of suppliers with known open risks and severity of those risks (effective when rendered as a supplier risk heat-map)
- Contract consistency (inclusion of security requirements)
- Volume of supplier assessments planned, in-process and up-coming
- Regulatory issues due to cyber concerns
- Externally reported incidents
- Supplier audit findings
- Insights and commonalities across these metrics

4.2 Define Supplier Tiering

Tiering suppliers can be used to drive differences in both the assessment approach as well as other requirements, e.g. frequency of periodic re-assessments. Prioritization is important to make the task manageable. A good approach is to establish tiers of suppliers which include dimensions such as spend, criticality of product or service to the mission of the organization, safety, hosting or access to sensitive data or systems, etc. Specific guidance for tiering suppliers

in order to prioritize risk management activities is provided in the SC.2 section of this document.

The tiering structure and prioritization rules should be agreed and approved by the sponsor and governance committee (if applicable).

5) Definition of a Supplier Risk Assessment Approach

5.1 Define Lifecycle Scope

The supplier risk management program should encompass the end-to-end supplier lifecycle from pre-contracting to termination of the supplier and its products and/or services, including any requirements for records retention and destruction. While supplier onboarding is a sensible place to start the implementation of the program, it is important that the scope of the program cover the full lifecycle. It should be noted, however, that the focus here is risk assessment of the supplier, *not risk assessment of the supplier's product*. Lifecycle touchpoints to consider within the assessment program are:

- Pre-contract/exploratory/innovation/business alliance development activities.
- Consistency of language and terms across all contracts.
- On-going monitoring, re-assessing supplier risk over time/re-validation (periodic or trigger-based). Examples of triggers include acquisition of supplier by another entity, change in scope of relationship, etc.
- End-of-relationship considerations/exit checklist (e.g. return of assets).

New suppliers acquired through mergers and acquisitions should be subjected to the same lifecycle approach and governed by the same program principles. Perform a gap assessment and, as necessary, program alignment and integration. When acquiring a legacy supplier risk management program, any differences in acquired supplier risk assurance metrics may require re-assessment of particular suppliers.

5.2 Define Risk Identification and Treatment

Adopting accepted industry frameworks has the benefit of inherited acceptance and recognition from regulators, government entities and the suppliers themselves, which helps reduce friction in the redlining and auditing processes.

Internationally recognized frameworks include the National Institute of Standards and Technology (NIST) Cyber Security Framework and the International Organization for Standardization (ISO) 27000. Others are available. Notably, the Health Sector Coordinating Council Joint Cybersecurity Working Group has created a publication, Health Industry Cybersecurity Practices (HICP), that can support risk assessments tailored to small and medium sized organizations. The assessment and contractual language templates within the HIC-SCRiM toolkit align closely to HICP.

A consistent risk assessment framework should be developed to ensure standardization of assessment and treatment options across all lines of business tailored to supplier tiering and the assessor organization's skills and resources. Common risk assessment approaches include:

- Supplier self-assessment questionnaires: these can be managed manually using spreadsheets or automated with commercially-available software
- Evidence-based audits by the assessor or an independent third-party certification: Other techniques of risk identification include framework audits and certifications as proxies for assurance (e.g. ISO, NIST, commercial 3rd party certifications) and external sources of assurance (e.g. AICPA SOC 1/2/3 reports).
- On-site assessments/supplier audits
- External "outside-in" risk monitoring and scoring solutions: Services exist that provide external risk monitoring for a fee, gathering data and reporting cybersecurity posture based on the publicly visible digital footprint of suppliers.

The organization must also define an approach for treatment of identified supplier risk, to include criteria for:

- Mitigating risk (implementing compensating controls)
- Transfer of risk (e.g. cyber insurance, third-party credit card processing service)
- Accepting risk (a business decision informed by an understanding of the risk vs. the business value)
- Avoiding risk (find alternate supplier or alternate solution to meet the business need).

5.3 Outsourced approach to Supplier Risk Management

Another option for organizations to consider is contracting a specialized third party to perform supplier risk assessments. Third parties that provide such services may have the skills and scale to perform this work more efficiently than doing it in-house. These and other service providers may also provide questionnaire-based or on-site assessments as well as external risk monitoring using tools mentioned above.

Any health organization looking to outsource risk assessments may consider subscribing to a Third Party Risk Management services partner. A number of for-profit and not-for-profit providers are available. Stakeholder community references for reputable firms are often available in forum discussions among members of private-sector cybersecurity information sharing organizations. More information about membership in these information sharing organizations – an essential part of a proactive cyber risk management program - can be found in the Health Industry Cybersecurity Matrix of Information Sharing Organizations (HIC-MISO).

6) Supplier Risk Management as Part of Business Operations

Having established the program, the organization needs to put in place the structure to sustain that program on-going. The following activities are recommended:

People

- Assign executive sponsor
- Establish required staffing and skills:
  - Role matrix supporting the processes
  - Skills inventory supporting the role matrix
  - Projection of required staffing for each role based on demand
- Train stakeholders and provide continual awareness of the program.

Process

- Establish executive governance that monitors the health of the program overall, including strategic direction, resourcing, etc.
- Establish operational governance dealing with performance to plan, issue management, and coordination of activities such as assessments and audits.
- Establish and maintain a risk register or ideally integrate with an enterprise risk management program
- Maintain the current supplier inventory, including a current supplier relationship owner. The recommendation is that the enterprise procurement function, as the gatekeeper of the contracting process, plays this role
- Provide sponsorship and organizational change management to ensure the required changes are harmonized with existing processes and integrated into business operations
- Track and communicate supplier risk posture and visibility
- Harmonize supplier assessment/engagement processes across functions and geographies to provide better user experience for both internal stakeholders and suppliers
- Document processes such as auditing, project management, task management, and compliance.

Tooling

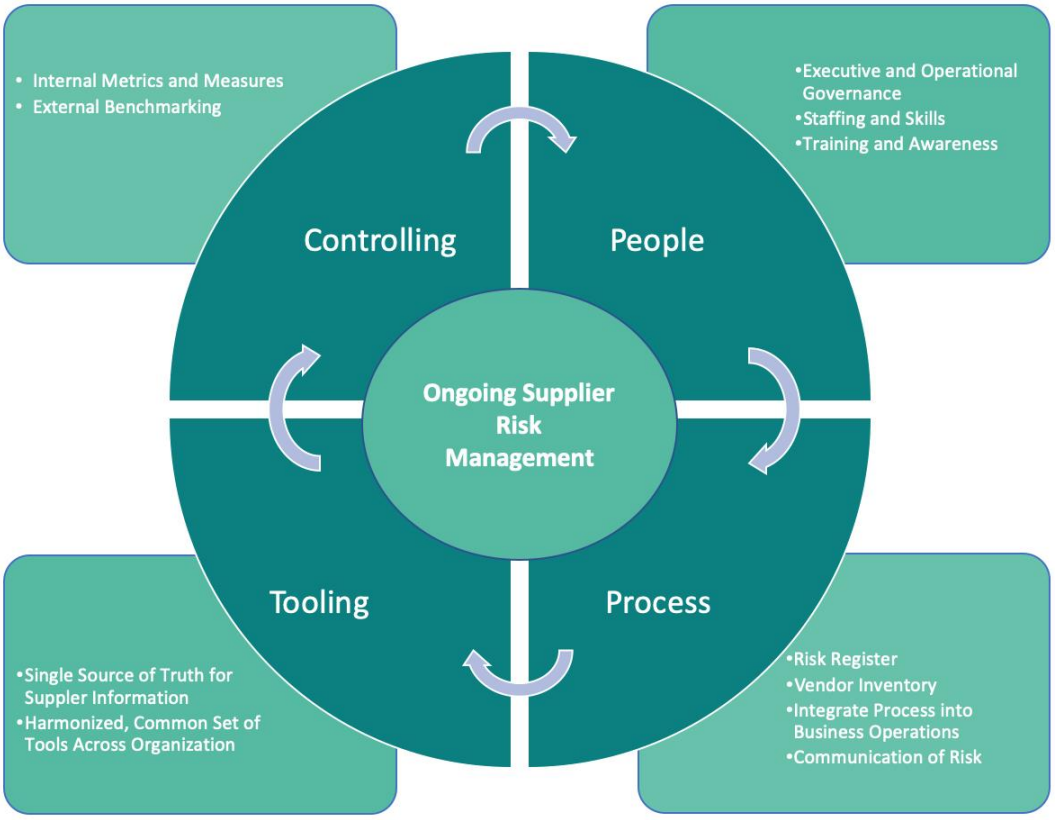
- Establish a single authoritative database for suppliers for the organization
- Harmonize supplier assessment/engagement tools across functions and geographies to provide better user experience for both internal stakeholders and suppliers
- Ensure tooling provides capabilities for real-time visibility to the status of supplier risk management activities
- Leverage advanced technology for analytics and process automation to achieve higher scalability and efficiency.

Controlling

- Collect (ideally automatically) data to drive metrics and measures
- Establish owners, targets, audience, communication cadence for metrics and measures

- Engage in benchmarking with industry partners to continuously improve the program and processes.

The infographic on the next page provides a pictorial view of the Supplier Risk Management Lifecycle.



Meeting NIST CSF Requirement ID.SC-2

Suppliers and third-party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process

1) Define Organization's Supplier Risk Management Policy, and Establish Roles and Responsibilities

1.1 Defining and Publishing Policy

The Supplier Risk Management Policy should be defined in consultation with the executive sponsor of the Supplier Risk Management Program and, depending on the size of the organization, representation from legal, procurement, IT, security, privacy, compliance, quality, and facilities.

To define and document your organization's Supplier Risk Management Policy, you may either refer to the example provided in Appendix B and modify it to meet your needs, or develop a policy from scratch. Policy documents should contain the following structural elements, incorporating information from the SC.1 guidance document:

- Purpose (as defined above)
- Scope (as defined above)
- Definition of terms used
- Roles and responsibilities (including those defined above)
- Policy requirements (as defined following review of SC.2)
    - This document should follow the supplier lifecycle:
        - Pre-contracting Due Diligence
        - Contracting
        - Supplier Governance and On-going Monitoring
        - Expiration/termination of Supplier Contract and Relationship
- Exception management
- Approval matrix
- Effective date
- Version history.

1.2 Establishing Roles and Responsibilities

In addition to selecting an Executive Sponsor, it is important that the organization define a business function that is directly responsible for owning the supplier inventory and maintaining its currency and accuracy. While IT may provide the underlying system, the inventory and process are more typically owned by procurement, finance or legal.

2) Identify Suppliers

It is foundational to identify a list of suppliers selling products or services to your organization. The information gathered in this crucial step will drive prioritization and enable risk scoring for each supplier. For some suppliers, further granularity may be required; for example, a large supplier with multiple geographies, services, and subsidiaries, which may have independent contracts representing different types of risk.

For existing suppliers, there can be many sources for inventory information. Some starting suggestions would be within the following areas/departments:

- Accounts Payable
- Business Associate Agreements
- Contracts
- IT Inventory (CMDB, Network, etc.)
- Procurement
- Value added resellers (VARs) / Aggregators
- Data export from Enterprise Resource Planning (ERP) system

Once existing suppliers are identified, it is important to maintain the currency and accuracy of the inventory by capturing any new, changing or retired supplier relationships. Additional suggestions for process triggers to update the inventory include:

- Legal Counsel
- Project Management Office (PMO)
- Departmental strategic decisions
- Procurement Teams
- Risk Committee

In addition to the above process triggers, a periodic review of the supplier inventory is necessary to ensure accuracy, with frequency depending on the size and turnover within your organization's supplier inventory.

Recommendation for supplier inventory system: While a spreadsheet is provided here as a starting point, there are commercially-available software options, where organizational resources allow, which enable workflow automation, collaboration, links to contract repository and risk assessments, data resiliency, and version control.

An excel template to capture the inventory of suppliers is available in Appendix A as part of the reference material supporting this document.

3) Prioritize Suppliers

Once a complete list of suppliers with their products/services is captured, the next step is prioritizing the suppliers so that risks can be adequately managed. Prioritization categories and their associated weights will vary between organizations.

Below is a suggested starting point for prioritization categories:

- **Annual Spend:** Referencing contracts, Accounts Payable or Procurement should produce the annual spend on a per-supplier or per-service basis. This "spend analysis" can be useful in prioritization, especially when deciding which suppliers may be strategic vs. transactional. The difference between a strategic and transactional supplier is determined by the relationship and the services they will provide. A strategic supplier typically has a long-term relationship and provides ongoing services for critical functions or business processes. A transactional supplier typically has a shorter duration contract and has limited scope and/or is project focused.

- **Sensitive/Confidential Data:** Referencing Business Associate Agreements, departmental meetings or the IT Inventory may produce artifacts surrounding sensitive data types and counts. This prioritization category may be important due to regulatory compliance and/or customer risk. Within this prioritization you should consider the volume of data as well as the sensitivity of each record.

- **Patient Risk:** Clinicians can provide valuable input and help rate any potential impact to patient risk. For example, the lack of availability of products, services and technology may pose significant patient risk and should be considered in this exercise.

- **Revenue Impact:** Reference the enterprise resource planning system, accounts payable and other financial and sales departments to identify which supplier's products or services directly affect or impact revenue-generating services.

- **Operational Impact/Business Criticality/Geopolitical:** Similar to revenue impact, work with stakeholders to understand if the in-scope products or services would have an impact on day-to-day operations (regardless of revenue). IT may also become a good resource for this information if the organization has a mature Disaster Recover/Business Continuity program and has performed a Business Impact Analysis (BIA).

- **Regulatory Compliance:** Similar to the efforts performed in the "Sensitive Data" analysis, work with those teams to understand if the product or service is in-scope for any regulatory compliance issues (HIPAA, Sarbanes-Oxley, GxP, etc.).

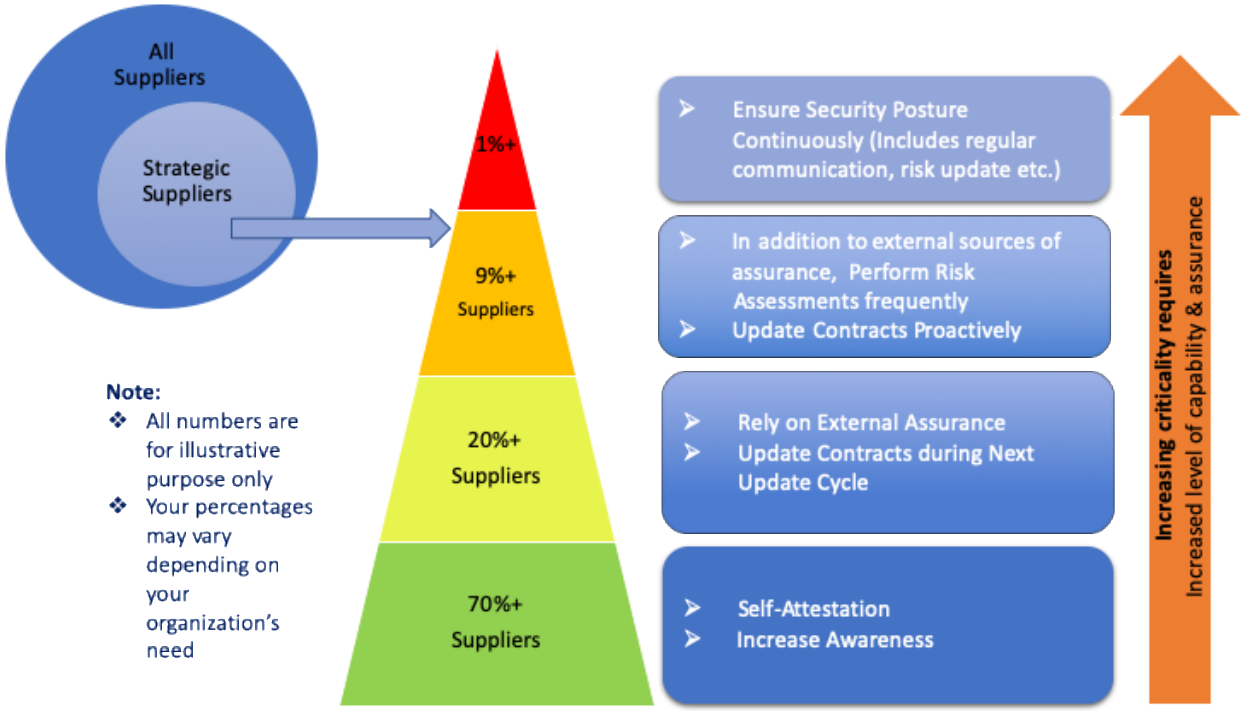
- **Reputational Impact:** Work with Legal Counsel and related departments to understand if any services or platforms may have reputational impact to the organization (e.g. customer facing websites, scheduling applications, etc.).

Appendix A contains a spreadsheet example of these prioritization categories, weights and scoring calculations to align with the inventory. The outcome of steps 1 through 3 will become your prioritization matrix to drive the risk assessment process.

3.1 Tiering the Supplier

Based on the outcome of the identification and prioritization steps, the organization should tier its suppliers based on risk.

This tiering will allow for systematic risk assessment of suppliers. The organization should define their own tiering structure based on the inventory data and risk spread. This could be a High-Medium-Low tiering, or a similar 2 or 4 tier model, or others.



4) Assess Supplier Risk

There are many methods to assess supplier cybersecurity risk. The following two approaches applied separately or in combination represent best practices for small and medium sized organizations.

4.1 Rely on certifications (e.g. ISO 27000, NIST, PCI, SOC 2, other 3rd party certifications)

Rather than performing your own assessment of the supplier's cybersecurity posture, you may decide to place reliance on one or more external certifications held by the supplier, provided independently by an authorized third party. It should be noted that there are varying levels of assurance and timing considerations for external certifications; an assessment based on a certification by itself does not guarantee the supplier's cybersecurity posture. Additional analysis and review may be necessary for strategic suppliers (i.e. critical, high, tier 1, tier 2, etc.)

614 The following certifications are common examples that provide broad-based coverage for
615 cybersecurity controls assurance:
616

	AICPA SOC 2	ISO 27001	Commercial 3rd Party Assessments and Certifications
Description	The AICPA created the Trust Services Criteria and SOC 2 report to evaluate an organization's information systems relevant to security, availability, processing integrity, confidentiality, or privacy. The controls within the Trust Services Criteria are aligned with the 2013 COSO Internal Control Framework. Note that SOC 1 reports are also available; however, these are focused on IT controls supporting financial accounting accuracy.	An information security standard, part of the ISO 27000 family of standards, which specifies a management system to bring information security under management control and gives specific control requirements.	Other proprietary 3rd party assessments and certifications provided by different vendors are available with different levels of industry penetration and acceptance. For the most part these certifications are based on, or take elements of, other established standards such as NIST CSF and ISO 27000.
Rationale for Inclusion	Widely recognized framework by non-IT/IS professionals.	International standard with a relatively high adoption rate.	Third party certifications provide an alternate way for suppliers to provide assurance on their security posture.

617
618 Suppliers may offer other certifications as alternatives, in which case your organization should
619 do its own analysis as to their limits of applicability and coverage.
620
621 *4.2 Perform own assessment of supplier's cybersecurity posture*
622
623 For strategic suppliers, organizations should perform their own assessment as frequently as
624 needed for business operations, but at a minimum annually. Based on the outcome of the
625 assessment, contracts may need to be updated. and executive management informed for
626 awareness and for enabling them to make decisions about the relationship.
627 Please refer to Appendix C for a suggested template for risk assessment.
628

Send the assessment to the supplier and have them complete it and return it to you.

The first section of the assessment template assesses the 'common core' of controls which are relevant across all supplier relationship types. In addition, the later sections of questions are supplemental based on the type of good or services your organization is looking to acquire from the supplier. In this instance only the relevant sections need be completed.

Once the assessment is completed and returned, review the color coding of the results and the comments made by the supplier. The questions in the assessment template are yes/no in nature in order to keep it simple for non-cybersecurity SMEs in your organization to review the output. While the reality is that there may be shades of grey in some of the responses, the controls listed are the bare minimum necessary, and therefore if the supplier is unable to meet one of these requirements fully you should consider the amount of risk you would be taking on by entering a relationship with them.

As already mentioned above, you may want to contract with qualified assessor organizations for this risk assessment activity.

Additional Sources of Information

As part of the assessment process, third party security services provide data on a supplier's public-facing cybersecurity posture. Such services provide a useful datapoint but should not be considered as complete assurance of an organization's cybersecurity posture.

Your suppliers may also offer self-attestations of their public-facing cybersecurity posture, but those attestations should similarly not be considered as complete assurance.

Simple internet searches can also provide additional input into your risk assessment, detailing any public data breaches, security risks, known vulnerabilities etc. Examples include the U.S. Computer Emergency Readiness Team (US-CERT), Industrial Control Systems CERT, www.privacyrights.org and US Dept. Health and Human Services https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf and the FDA cybersecurity safety communications for medical devices https://www.fda.gov/medical-devices/digital-health/cybersecurity#safety.

5) Respond to Supplier Risk Assessment

The supplier risk management program's executive sponsor is required (potentially in consultation with legal counsel) to take a position on the amount of risk the organization is willing to accept. The output of the supplier inventory, prioritization and assessment process should be reviewed initially (and then periodically thereafter) with senior leadership so that supplier risks can be understood and measured in the context of that risk appetite, and appropriate recommendations can be made.

Once the risk posture of the supplier is identified and measured, if the risk level falls within the risk appetite established by the executive sponsor, the next step is for the organization to ensure that the contract with that supplier adequately covers the necessary controls. For this purpose, refer to guidance in SC.3. Robust documentation should be maintained showing identified risks, decisions taken in response and, where appropriate, requirements for supplier accountability for implementation of mitigations of identified risks.

In the case that the risk level falls outside the risk appetite of the organization, the following steps are recommended:

1) Document the identified risks and business impact for the organization
2) Determine if additional controls or mitigations (which may include cybersecurity insurance) can be implemented by the supplier within a satisfactory timeframe
3) Inform the executive sponsor of the recommendation.

If the decision from the executive sponsor is to continue the relationship, the purchasing organization should work with the supplier to update the contract to reflect additional control requirements and mitigations to be implemented in line with committed timeframes.

If the supplier is unable or unwilling to update or modify its practices or capabilities to meet the required risk level, the executive sponsor must decide whether to accept the risk and continue the relationship or terminate the engagement.

If the decision from the executive sponsor is to terminate the relationship, the organization should initiate its sourcing process to find an alternative supplier, using the same cybersecurity risk assessment approach as part of the selection process.

Meeting NIST CSF Requirement ID.SC-3

Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.

This section of the document is intended to help health organizations establish the information security requirements that should be included in contractual agreements with their suppliers.

It provides guidance on:

1. Limitations of contracts to mitigate, transfer or avoid risk
2. Sample contract language (regardless of which of the contracting party's paper is being used)
3. Contractual redlining process against template language
4. How the buyer might obtain assurance that the terms of the contract are being fulfilled
5. Other contractual forms of risk transference and avoidance (e.g., cyber insurance).

1) Guidance on the limitations of contracts in managing cybersecurity risk.

All supplier relationships involving the procurement of goods or services that are enabled by, or dependent on, technology or data involve a degree of cybersecurity risk. Contracts by themselves do not mitigate risks completely. They *may* facilitate the transfer of risk to a supplier or insurance provider, but are more commonly effective in:

- Clarifying the roles and responsibilities for the controls that the contracting parties commit to enact to manage the risk.
    - What is the buyer committing to do in order to ensure the security?
    - What is the supplier committing to do in order to ensure security?
- Stipulating mechanisms whereby the contracting parties can gain visibility to adherence (or not) to the contractual commitments made over time, e.g., sharing independent audit reports, scan/test reports, on-site audits, etc.
- Establishing Service Level Agreements, patching vehicles and disclosure requirements in the case of a security incident or new vulnerability being discovered. Language should include definitions of a breach or incident, committed time-frames for customer notification, root cause analysis, restoration of service, producing a patch or implementation of long-term resolution, etc.
- Ensuring that the supplier applies the same contractual requirements to any sub-contractors/suppliers that they involve in the provision of the product or service to the customer.

A contract may give the purchasing organization a level of confidence in the safeguards promised by the supplier, as it forms the basis on which a legal claim can be made in the event losses are suffered through a cybersecurity incident. However, it is important that the purchasing organization understands that after-the-fact legal recourse may be of little comfort when stacked against the reality of operational losses, reputational damage (regardless of actual liability) or even patient harm in the event of an incident. Therefore, even with the contractual assurances provided by the supplier, the purchasing organization should ensure that the value created for the organization by entering into a relationship with the supplier outweighs the potential risks to its stakeholders (customers/patients, employees, other suppliers, communities, the environment and any stock-holders).

2) Sample contractual boilerplate language for inclusion into contracts.

The contractual template in Appendix D of this document is an industry best-practice set of requirements to get started.

The requirements are derived from the Health Sector Coordinating Council (HSCC) publication, Health Industry Cybersecurity Practices (HICP), which identifies the top five current threats and top 10 cybersecurity best practices. The requirements are designed to be specific enough to be actionable and drive accountability on the part of the supplier, while being modest enough in their aspirations that they represent a minimum level of security good practice that any organization of any scale should be able to meet. If the supplier you are working with is unable

or unwilling to meet the requirements articulated in this template, **that may be an indicator of their scale and level of maturity and consequently may be a cause for concern**.

Guidance on the redlining process (that is the process by which the legal representatives of each contracting party negotiate on the contractual language) follows below. However, it is important to note that as a generic starting point, the relevance and importance of the different controls described in the template will depend on the nature of the relationship with the supplier and the risk that represents for your operations and those whose data you hold or who rely on your products and services. Therefore, establishing which threats and which supplier relationships are most critical to your operations and to the stakeholders is an essential starting point. See sections SC-1 and SC-2 of this publication for more detail on how to achieve this.

Understanding that the audience for this document is non-technical, we have tagged each control within the contractual boilerplate to one or more of these threats to help the purchasing organization understand the implications if a supplier is unable or unwilling to commit to a given control in the contract.

Before commencement of the contracting process, consult the table below and identify the most relevant threats and how your organization and customers could be put at risk through an incident at the supplier, or how the relationship with the supplier could introduce them into your environment.

Next determine the supplier relationship type and gather the contractual template from Appendix D, including the 'common core' as well as any 'supplemental' contractual requirements relevant to specific types of supplier relationship.

This language can then either be added into your own contract document or into the supplier's document if the contracting is to take place on their paper. If the supplier is unwilling to add these requirements into their contract you should insist that they demonstrate equivalence. These requirements are considered to be the minimum base that any organization should be willing to meet (they are after all in the supplier's own self-interest).

It is recommended that you have your legal counsel review the contracting template.

Table 1 – Cybersecurity Threats and Impacts by Supplier Relationship Type

Threat	Potential Impact of Attack (non-technical audience)	Examples of supplier Relationships
E-mail phishing attack	E-mail 'phishing' is the most common form of cyber-attack. It typically involves the victim receiving a malicious e-mail that persuades them to either click on a link or open an attachment. Links may take the victim to a look-alike or	• A supplier storing/processing sensitive data on your behalf.

	malicious website where they are either persuaded to enter their user id and password (thereby giving those details to the attacker), or the malicious website or e-mail attachment may download malware to the victim's computer. Different malware have different functionality e.g. spying on the user, giving the attacker control of the computer or other computers on the same network, or to hold the victim's data ransom (see below). Phishing is not restricted to e-mail; other vectors could be unsolicited SMS messages, instant message app messages or even malicious USB devices.	• A supplier with access credentials to your computer systems; for example, for tech support or to input orders.
Ransomware attack	Ransomware is a type of malware whereby the attacker encrypts the victim's data making it inaccessible and demands payment to release it. Ransomware is among the most common cybercrimes and impacts organizations of all sizes. Unavailability of mission-critical data or software can cripple an organization's ability to serve patients or operate as a business. As with the effects of a fire or other disaster, many organizations never recover from a period of down-time exceeding a week. Ransomware affects not only "traditional" computer systems (desktops, tablets etc.) but also connected "smart" devices such as medical devices, thermostats, building control systems, security cameras, etc.	• A supplier that is the sole supplier for a mission-critical product or service (if they are down, you are down). • A supplier that is the exclusive holder of data critical to your mission. • A provider of IT hosting, IT support services, cloud-based software or software within devices that your organization sells or depends upon.
Loss or theft of equipment or data	Theft of media storage, files or devices holding sensitive data; for example, patient data	• A supplier storing/processing sensitive data on your behalf. • A supplier with access credentials

		to your computer systems. • A supplier with physical access to your devices or network.
Accidental or intentional data loss	Accidental loss of data; for example, downloading data onto a laptop which is then lost or stolen, mailing data storage which is lost in the mail, leaking of data by an insider to other organizations not authorized to access it	• A supplier storing/processing sensitive data on your behalf. • A supplier with access credentials to your computer systems. • A supplier with physical access to your devices or network.
Attacks against connected medical devices that may affect patient safety	Tampering with the proper functionality of "smart" or connected medical devices or making those devices unavailable, for example by shutting them down or locking legitimate users out of them. Examples could include pumps or dispensers of medication, scanning or monitoring devices, wireless-connected implants, surgical robotics, etc.	• A supplier of connected medical devices or software operating medical devices. • A supplier with access credentials to your computer systems. • A supplier with physical access to your devices or network.

797
798 *From* ***Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients***

Table 2. Cybersecurity Practices and Sub-Practices for Small Organizations

Cybersecurity Practice	Sub-Practice for Small Organizations		Page
E-mail Protection Systems	1.S.A	E-mail System Configuration	6
	1.S.B	Education	7
	1.S.C	Phishing Simulation	7
Endpoint Protection Systems	2.S.A	Basic Endpoint Protection	9
Access Management	3.S.A	Basic Access Management	11
Data Protection and Loss Prevention	4.S.A	Policy	13
	4.S.B	Procedures	14
	4.S.C	Education	15
Asset Management	5.S.A	Inventory	16
	5.S.B	Procurement	17
	5.S.C	Decommissioning	17
Network Management	6.S.A	Network Segmentation	18
	6.S.B	Physical Security and Guest Access	18
	6.S.C	Intrusion Prevention	19
Vulnerability Management	7.S.A	Vulnerability Management	20
Incident Response	8.S.A	Incident Response	21
	8.S.B	ISAC/ISAO Participation	22
Medical Device Security	9.S.A	Medical Device Security	23
Cybersecurity Policies	10.S.A	Policies	24

799
800
801

802 **3) Guidance on the Redlining Process**

803 The intended audience for this contracting template is small to medium sized organizations,
804 typically those without dedicated cybersecurity subject matter experts on staff. This
805 publication therefore attempts to provide a contracting template that incorporates technical
806 concepts into a workable format, without requiring an in-depth cybersecurity knowledge.

807 The contracting template is based upon the following guiding principles:

808 1. The template is structured with a 'common core' set of requirements which are
809 applicable to any supplier relationship and 'supplemental' requirements specific to the
810 type of supplier relationship. Note: the supplemental requirements are not mutually
811 exclusive and multiple requirements may be applicable to a single contract.
812 Furthermore, there may be relationship types outside of this list which are not
813 effectively covered. In that case, you should seek independent guidance from a
814 qualified cybersecurity subject matter expert.

2. The template is based upon the HSCC HICP. It is designed with enough specificity to be actionable and enforceable, while also representing a value-adding but basic cybersecurity maturity level. This maturity level is intentional to minimize the redlining during contracting process. If the supplier you are working with is unable or unwilling to meet these requirements, it may require additional due diligence because that may be an indicator of their relative scale and level of capability to meet your organization's needs and consequently may be a cause for concern. Similarly, if the relationship is particularly sensitive or critical to your organization, you may wish to contract independent subject matter expertise to give case-specific guidance going beyond the lowest common denominator cybersecurity practices that this document lays out.

Keeping those principles in mind, as with any negotiation, it is common for compromises to be made in order to arrive at an agreement that is acceptable to both parties. Not all of the stipulations of the template language below will be equally important in every case. Their importance will depend on the nature of the supplier relationship and the impact a cybersecurity incident may have for each party. For example, if the nature of the relationship is such that the supplier is hosting or has access to the customer organization's data, some controls may be more important than if the supplier is simply providing a product without access to the data.

Another common scenario is for the supplier to insist on their own contractual language as the basis for the agreement. In this case you can either ask that this contractual template be inserted into that document or ask the supplier to map their requirements to this template and demonstrate how they meet or exceed their terms.

Ultimately, if the supplier is unwilling to meet one or more of the terms of this recommended contract language, your organization must decide whether to proceed regardless or seek alternatives. The decision to proceed with the relationship should be based on whether the potential derived value is greater than the potential risk to the organization and, more specifically, its patients, customers, employees, environment, and shareholders/owners in the event of a cybersecurity incident of the type detailed in Table 1 above.

4) Guidance on how the buyer might obtain assurance that the terms of the contract are being fulfilled

Contracts define the vehicles for the buyer to gain assurance that the controls promised are actually in place, be they technical controls implemented within a product or process controls that the supplier executes as part of how they provide their service or maintain/support their product over time.

Unfortunately, suppliers may have little incentive to provide transparency, especially to smaller customers with less leverage/purchasing power. Moreover, even if such transparency were provided, small organizations have limited capacity and capability to digest and understand the

information. Therefore, for small organizations it is important to focus on the most important supplier relationships based on potential impact. In addition, consider the following:

- **Security is expensive.** A supplier may be cutting costs of their security program to reduce overall IT expenses.
- **Security is hard.** All other things being equal, larger suppliers (with more demanding larger customers) are more likely to have the scale which enables them to secure their products and services, whereas smaller companies may find this more challenging.
- **Security is a moving target.** Whereas functionality may still meet the need five or ten years from now, the security may no longer be adequate as security threats are constantly evolving. Consider the useful life of the product and beware high-risk engagements with little in the way of long-term relationship or support.
- **Regulatory compliance is not equal to security.** Healthcare is a highly regulated sector of the economy, and while the FDA is increasingly taking an interest in cybersecurity, especially in the medical device space, compliance with regulation does not necessarily mean good security. A security program that is designed to only comply with regulations may be putting an organization at significant risk.
- **Indicators of good practice.** While your organization may not be able to audit a supplier or test the security of their products or services, there are still indicators of good practice:
    - The supplier proactively tests their controls or has them independently audited
    - The supplier demonstrates openness and transparency about their security controls
    - The supplier has industry certifications such as ISO 27000, SOC 2, or other proprietary for-profit 3rd party certifications. Their products may comply with standards such as NIST CSF or FIPS 140-2. While these indicators have limitations, they may point to a company culture that embraces the need for good security practices.
    - The supplier holds cyber insurance. While cybersecurity insurance is still an evolving field, underwriters often ask businesses for minimum levels of cybersecurity maturity before they are willing to assume a company's risk by selling them a cybersecurity insurance policy. This is therefore another potential indicator that the company is doing the right things. More comments on cyber security insurance follow below.

5. Guidance on other contractual forms of risk transfer and avoidance (e.g. cyber insurance)

Cybersecurity insurance is a growing business within the insurance industry and is an option for organizations to limit their exposure to some of the costs in the event of a security incident. Some important considerations before purchasing cyber insurance follow:

- First vs Third-Party Insurance: Is the policy providing your organization compensation for the impact from a breach/incident or only compensating the affected supplier?
- Does the insurance cover only the legal fees or liability claims, or does it also cover loss of revenue/business or personal injury claims (given the healthcare context)?
- Does the insurance cover acts of war or terrorism? Note that some of the highest profile ransomware incidents of recent years have been attributed to governments rather than criminals, and therefore some insurance providers have considered them acts of war or terrorism and have disputed claims.
- Cyber insurance is not a replacement for a structured cybersecurity risk management program. Any short-term payout may well turn out to be insignificant compared to the long-term patient safety, reputational or financial losses incurred as a result of an incident.

Closing Summary

Supplier risk management is an ongoing process.

This publication provides the reader with guidance for establishing a supplier risk management program, for both existing suppliers and new, and illustrates how to sustain the activities on an ongoing basis, with specific templates that could be used as a starting point for your organization's needs.

The focus of the publication is small to medium sized organizations operating in the health sector that don't necessarily have in-house cybersecurity subject matter experts.

Throughout the document we covered NIST CSF supply chain requirements across the following 3 sections:

- Components of a supplier risk management program, such as defining policies and procedures, roles and responsibilities, and establishing overall governance

- Process of establishing and sustaining the supplier risk management program, including inventory of suppliers, risk assessment and risk treatment guidance

- Contract management process and a suggested template for cybersecurity.

The document provides multiple templates for risk assessment, contract cybersecurity language, supplier inventory attributes, supplier risk management policy. A process view diagram is provided for an end-to-end view that links all the sections together.

Finally, the document provides comprehensive glossary of the terms used in this document.

Appendix A – Excel Template for supplier inventory

https://healthsectorcouncil.org/wp-content/uploads/2019/09/HIC-SCRiM-Third_PartyInventory_and_Prioritization.xlsx

Appendix B – Policy Template

Purpose

This policy describes the minimum requirements for managing information risks resulting from the utilization of a supplier's services and/or products.

All new supplier relationships must comply with these requirements by [*Insert Date*].
All existing supplier relationships must comply with these requirements by [*Insert Date*].

Scope

All supplier relationships (including IT and non-IT relationships) are in scope for this policy and its supporting documentation.

Due to the unique requirements of contracting with government and regulatory agencies, exceptions may be made to the scope of this policy.

Definitions

- Commercial off-the-shelf or commercially available off-the-shelf (COTS) products: Packaged solutions which are adapted to satisfy the needs of the organization making the purchase, rather than the commissioning of custom-made solutions.
- Cybersecurity: The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction to provide confidentiality, integrity, and availability.
- Supplier(s): Broadly interpreted to include any individual or entity that provides any type of service and/or product to Organization. Also, commonly referred to as "vendor", "service provider", "consultant", "external partner", "third party" or "business partner".
- Contractual Documents: Legally-binding and appropriately signed legal documents between Organization and the supplier. They can take multiple forms such as Master Service Agreements, Amendment, Addendum, Task Order, Statement of Work, etc.
- Supplier Relationship: Any engagement with a supplier responsible for handling Company information, paid or unpaid, resulting from a legally binding contract. One or more contracts can constitute a single supplier relationship.
- Executive Sponsor: Organizational leader with the accountability for the business risks that originate from the utilization of a supplier's services and/or products and is able to influence and obtain organizational resources to address those risks.
- Relationship Owner: Organization employee who is accountable for the relationship with the supplier. Relationship Owners can delegate their responsibilities but not their accountability. A relationship owner:
    - Is the primary Organization point of contact for the supplier;
    - Consults with the Global Sourcing and Procurement function and collaborates with other relationship owners, where a supplier has multiple engagements with

Organization, to provide comprehensive oversite to the relationship;
- Understands and stays updated about the services and/or products provided by the supplier;
- Collaborates with appropriate IT functions to manage supplier information risks.

- Supplier Information Risk Management: Risk Management practices employed to identify, manage, and mitigate the level of information risk resulting from the utilization of a supplier's services and/or products.

Requirements

This Policy follows the supplier relationship through four different phases. These phases include Pre-contracting Due Diligence, Contracting, Supplier Governance and On-going Monitoring, Expiration / termination of Supplier Contract and Relationship. These phases account for overall lifecycle of a supplier relationship.

Since this Policy is taking the lifecycle approach to managing supplier risks, the role of 'relationship owner' becomes critically important to manage supplier risks. This role's responsibilities are discussed in the following sections and are spread across all the phases of the relationship.

Pre-contracting Due Diligence

1. Prior to signing off on a contract, the following requirements must be met. Government or regulatory agencies are exempt from this requirement when the type of engagement does not permit it.

    1.1 The supplier must demonstrate a current, valid and appropriate certification of cybersecurity posture

    1.2 If the supplier does not demonstrate a current, valid and appropriate certification as per 1.1, a risk assessment must be performed

    1.3 Relationship owners must plan for and complete the remediation of identified gaps uncovered by the assessment detailed in section 1.2 in a satisfactory timeframe after signing off on the contract, or as agreed by the executive sponsor.

Supplier Contracting

2. Relationship owners must ensure the following security requirements are met or as needed defined in contracts or service agreements:

    2.1 Suppliers must hold and maintain current, relevant and appropriate certifications and/or attestations when the services and/or products provided need to comply with laws or regulations requiring such certifications (e.g. PCI-DSS.)

    2.2 Ensure contracts incorporate a right to audit the supplier or the right to obtain evidence of an independent audit (e.g. Statement on Standards for Attestation Engagements

(SSAE) No. 16 type SOC2, or International Standard on Assurance Engagements (ISAE) 3402.)

2.3 Where relevant (e.g. externally hosted systems or applications, SaaS, Cloud, etc.), ensure the contract incorporates a right to perform or request evidence of vulnerability scans of supplier information systems that host or process company information.

2.4 Changes in supplier personnel with access to Organization information including changes in role must be communicated to affected relationship owners as soon as possible.

2.5 When suppliers providing services to Organization engage with additional suppliers (e.g. 4th or 5th party suppliers / aggregators, subcontractors, etc.), the information risk management terms and conditions of our contract are applicable to their lower tier agreements as well.

Supplier Governance and Ongoing Monitoring

3. Managers of relationship owners must ensure new relationship owners are assigned when there is a change in the relationship owner for a given supplier.

4. When a supplier has multiple relationships with the organization, all associated relationship owners must participate in the governance of the supplier.

5. When modifications are made to an existing supplier relationship that result in changes to our organization's information systems or changes in the access to Organization information, the supplier risk assessment must be refreshed.

6. Relationship owners must ensure that the supplier's access to Organization information assets is appropriately updated when personnel change notifications are received from the supplier. Access changes must be implemented in line with the Organization's own information security policy.

7. Ensure information exchanges occur over connections that are secure, authorized, maintained and terminated when the engagement ends or the scope of the supplier relationship changes.

7.1 The organization must conduct an annual review of established information exchange connections between the Organization and suppliers and take appropriate action.

Expiration/Termination of Supplier Contracts and Relationship

Suppliers may have one or more contracts with the Organization. In a single-contract relationship, the expiration or termination of the contract results in the termination of the entire relationship with the supplier. In multiple-contract relationships where additional contracts are still in effect, the expiration or termination of a single contract does not necessarily result in the expiration or termination of the entire relationship. In those cases, follow the requirements outlined in the contract that has expired or is being terminated.

8. Where information is not stored on Organization-managed infrastructure, relationship owners must ensure that Organization information is returned securely to Organization at

the end of the relationship or upon expiration or termination of the relationship, unless agreed upon in the original contract. This includes both electronic and non-electronic information.

9. When the supplier hosts or processes Organization information using its own information systems, relationship owners must ensure that after the required information has been returned to Organization, the supplier securely erases or destroys Organization information from its information systems including backup and archival media and provides evidence that the information was securely erased or destroyed, unless agreed upon in the original contract.
10. Access by supplier personnel to Organization information and information systems must be removed as part of the expiration or termination of supplier relationships. Any physical connections (e.g. site-to-site VPN) and system-to-system integrations must also be disconnected as part of the expiration or termination of the relationship.
11. Where applicable, relationship owners must also ensure that the Organization's information assets (e.g. laptops or mobile devices etc.) are securely returned to the Organization at the end of the relationship without erasing the contents, unless agreed upon in the original contract. The proper disposition of Organization's software licenses must also be addressed as part of this process.

DOCUMENT CONTENT APPROVALS

Approval:	
Individual Role	{Signature/Date}
Any signature qualification/caveat	

VERSION HISTORY

Version:	**Date:**	**Author:**	**Description:**
1.0	01-JAN-2019	Name	Description of version/change

Appendix C – Risk Assessment Template

https://healthsectorcouncil.org/wp-content/uploads/2019/09/HIC-SCRiM-Supplier-Risk-Assessment-Template.xlsx

Appendix D – Contractual Language and Requirements Template

Instructions:

The following cover-page section and the Exhibit are to be properly numbered and inserted where appropriate in the agreement being negotiated. All paragraph styles, formatting, numbering, definitions, etc. must be conformed to the agreement into which this is being inserted.

The Exhibit for Information Security requirements is divided in two separate sections.

- **Core requirements** are non-negotiable. The controls implemented to achieve compliance with this agreement should be based upon the recommendations found in the HSCC HICP volume 1 for small organizations and technical volume 2 for medium sized organizations as well as NIST CSF.

- **Supplemental requirements** are based on the type of supplier relationship and are additive in nature. This means if your supplier falls in multiple categories, you should add requirements from all the applicable categories.

Contract Template:

Exhibit <nnn>

Core (Mandatory) requirements

Cybersecurity Policy, Training and Awareness

1. Supplier shall have documented information security policies in place, refreshed annually, to ensure the confidentiality, integrity, and availability of Supplier and Company Information. These policies shall cover all business geographies and business functions of the Supplier, including their own sub-contractors/suppliers. These policies shall address the following core and supplemental requirements detailed in the agreed contract and shall ensure that enforcement mechanisms including training and awareness exist.

Asset and Change Management

2. Supplier shall maintain inventory of its information system assets, refreshed annually, that documents the identification, ownership, usage, location and configuration for each item. The Supplier shall ensure that changes to assets follow a documented change management procedure.

Access Control

3. The Supplier shall be accountable for providing appropriate identity management for authentication and authorization according to principle of least privilege. The supplier shall have a documented process for provisioning and deprovisioning of access (including elevated privileges) to their physical facilities and information system assets which must include independent approval, a formal periodic review of access (at least annually) and timely removal of access.
4. Supplier shall limit elevated privileges to the minimum number of users needed for effective operations and shall actively manage such privileges by reviewing periodically at a reasonable frequency higher than the general user access review and revoking immediately when no longer needed.

Network Security

5. The supplier shall allow inbound access into their organization's network with explicit approach, the default rule being to deny all inbound traffic. The supplier shall restrict access to assets with potentially high impact by use of further internal network segmentation.

6. The supplier shall restrict physical access to information system assets to authorized personnel.

7. The supplier shall implement controls to protect information system assets from potential malicious activities which penetrate the first line of a layered defense as established by Firewalls and other such controls. The supplier shall implement intrusion prevention and intrusion detection controls and configure them to update automatically.

Endpoint Protection

8. The supplier shall implement an anti-malware solution which shall include a local firewall capability on their workstations, servers and mobile devices. The solution shall prevent disabling by end users and shall automatically receive updates on a regular basis. The solution shall perform both real-time and periodic scans.

9. The supplier shall ensure that end users who are not designated administrator do not have system administrator permissions, including permissions to install or modify software on the endpoint.

10. The supplier shall ensure that security patches are monitored, reviewed and applied to all end points in line with the guidance given by the software provider.

11. The supplier shall ensure that use of administrator and elevated privileges require multi-factor authentication.

12. The supplier shall ensure that all manufacturer default user id's and passwords in the software and technology devices are changed upon installation of the software or device.

Email Protection

13. Supplier e-mail systems shall support encryption in transit via TLS 1.2 and above and DMARC standards. The supplier shall conduct awareness and training specific to phishing.

Vulnerability and Patch Management

14. The supplier shall employ a vulnerability scanning solution to detect security vulnerabilities in systems and externally facing websites hosted within their environment and remediate detected gaps in a timely manner. The process must incorporate a defined patch management cycle and controlled changes to configuration.

15. The supplier shall subscribe to threat intelligence sources such as HC3, US-CERT, Med ISAO, not for profit ISAC groups and others. For a listing of cybersecurity information sharing organizations, the HSCC's Health Industry Cybersecurity Matrix of Information Sharing Organizations (HIC-MISO)

Incident Response

16. The supplier shall implement a procedure to respond to security or privacy incidents and shall perform detailed investigation and response activities to assist in identification, containment, eradication and recovery actions for potential security incidents.

Supplemental Requirements based on type of supplier relationship:

1. Suppliers that are mission-critical to buyer's business with or without data access.

   Adoption of the core (mandatory) requirements referenced above are recommended to be supplemented with additional guidance (such as legal counsel) for Supplier relationships that fall into this category.

2. Suppliers with direct connectivity and/or access to your organization's information system assets and/or data.

   If the Supplier becomes aware that a Cybersecurity Event has or may have occurred, the Supplier and/or service provider designated to act on behalf of the Supplier, shall conduct a prompt investigation and notify the Organization immediately, disclosing all known Indicators of Compromise.

   The Supplier shall notify the Organization immediately when Supplier employees and contractors with access to the Organization's information system assets no longer require that access to perform their job functions.

3. Suppliers that host/manage applications used by the Organization, or the Organization's data on their own infrastructure.

   a. If the Supplier becomes aware that a Cybersecurity Event has or may have occurred, the Supplier and/or service provider designated to act on behalf of the Supplier shall conduct a prompt investigation and notify the Organization immediately, disclosing all known Indicators of Compromise.

   b. The supplier shall encrypt any of the Organization's data in storage on all media types and when in transit outside of the Supplier's network. Encryption keys shall be periodically rotated and stored separately from the encrypted data. Supplier shall adequately protect the keys from loss/destruction or unauthorized access.

   c. The supplier shall employ a Data Loss Prevention solution configured to detect unexpected or unauthorized transference of the Organization's data within or outside the supplier's network.

   d. Any software code that the supplier builds and maintains as part of its services to the Organization shall undergo peer review by a qualified individual (other than the

developer of the code) and code scanning with an automated tool to ensure that malicious or dangerous coding bugs and/or logical design flaws are detected and remediated before they are moved into the production environment.

e. Any software that the supplier builds and maintains as part of its services to the Organization shall undergo security penetration testing performed by a qualified individual at least annually or with the deployment of any major change, in order to highlight security vulnerabilities in the software that are exploitable by malicious actors. Any exploitable vulnerabilities detected in this process shall be remediated within a reasonable timeframe not to exceed 30 days.

f. In the event of termination of the contract, the supplier shall return the Organization's data to the Organization in readable format including any equipment or software necessary to access the data. The supplier shall destroy all other copies of the Organization's data following confirmation from the Organization that the returned data is readable and accessible unless the contract explicitly permits retention.

4. Suppliers of medical devices or software as medical device.

a. The supplier shall provide one or more current, available and supported endpoint protection solutions approved to be installed on the medical device acquired by the Organization without impact on the terms or duration of the warranty provided by the Supplier over the equipment.

b. The supplier shall integrate cybersecurity risk assessment, security architectural design analysis, security requirements and security testing into its Quality Management System.

c. The supplier shall inform the Organization of the presence of any exploitable security vulnerability which risk patient health or materially impact the expected function of the acquired device immediately and provide a patch within 30 days of the vulnerability being reported to the supplier.

-- The above controls and others are detailed in the HSCC's Medical Device and Health I.T. Joint Security Plan (JSP), which advises medical technology companies on best practices for developing and implementing a product cybersecurity design, manufacturing and servicing program. --

d. The Supplier shall comply with the regulatory guidance for pre- and post-market management of cybersecurity in medical devices. Example is US FDA pre and post market cybersecurity guidance. Other national regulatory agencies may provide similar guidance.

FDA Pre-Market Guidance

https://www.fda.gov/regulatory-information/search-fda-guidance-documents/content-premarket-submissions-management-cybersecurity-medical-devices

FDA Post-Market Guidance
https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM482022.pdf

European Union equivalent regulation
https://www.emergobyul.com/blog/2007/06/europe-issues-new-guidance-document-medical-device-post-market-surveillance-and

5. Suppliers operating in high risk geographies.

    a. The supplier shall employ a Data Loss Prevention solution configured to detect unexpected or unauthorized transference of the Organization's data within or outside the supplier's network.

    b. The supplier shall implement segmentation capabilities that enable immediate isolation of operations in the high-risk geography from the rest of the Supplier's operations in the event of a cybersecurity incident.

6. Suppliers of COTS products hosted/installed at buyer.

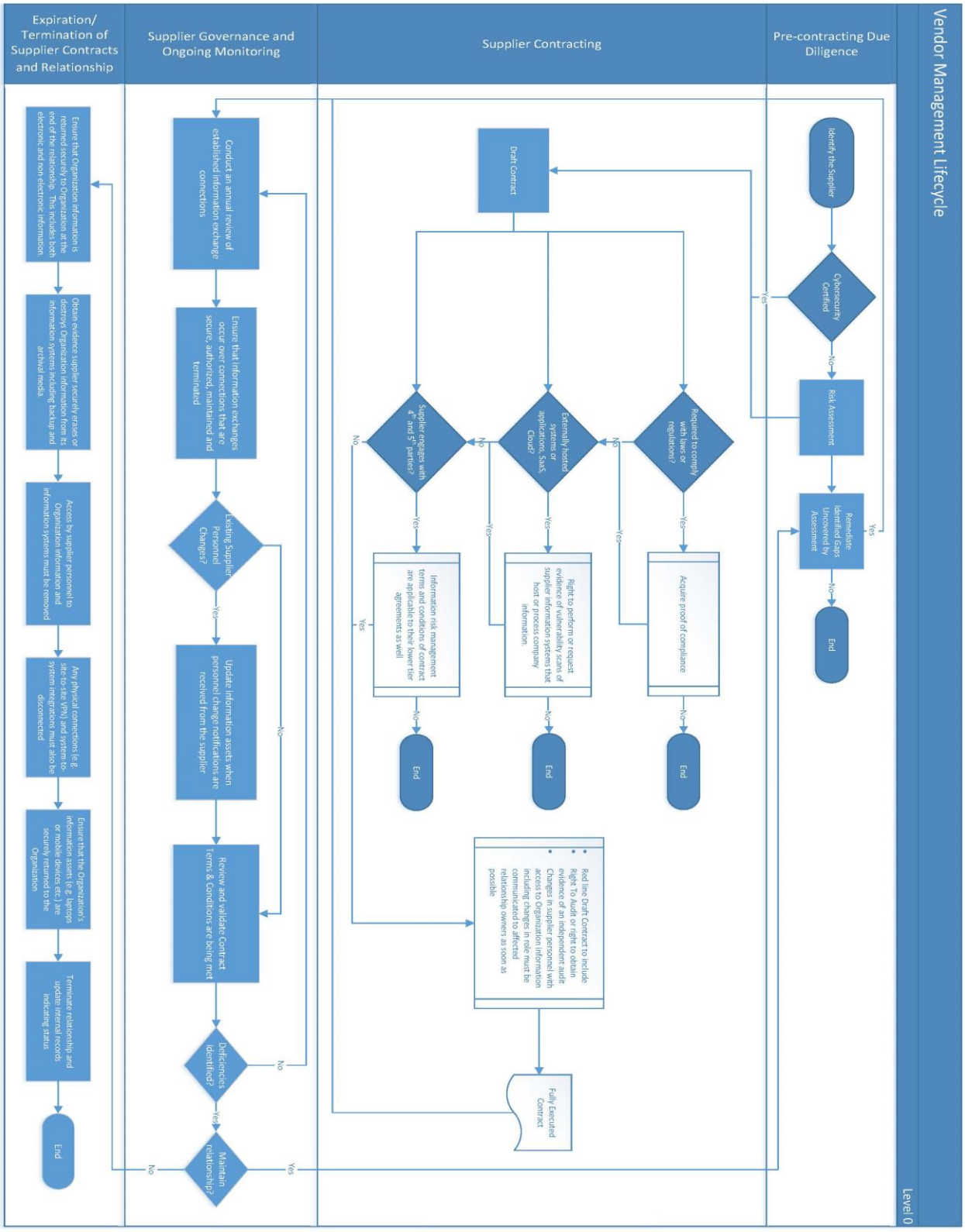
    a. If the Supplier becomes aware that a Cybersecurity Event has or may have occurred, the Supplier and/or service provider designated to act on behalf of the Supplier shall conduct a prompt investigation and notify the Organization immediately, disclosing all known Indicators of Compromise.

    b. Any software code that the supplier builds and maintains as part of its services to the Organization shall undergo peer review by a qualified individual (other than the developer of the code) and code scanning with an automated tool to ensure that malicious or dangerous coding bugs and/or logical design flaws are detected and remediated before they are moved into the production environment.

    c. Any software that the supplier builds and maintains as part of its services to the Organization shall undergo security penetration testing performed by a qualified individual at least annually or with the deployment of any major change, in order to highlight security vulnerabilities in the software that are exploitable by malicious actors. Any exploitable vulnerabilities detected in this process shall be remediated within a reasonable timeframe not to exceed 30 days.

Appendix E – Supplier Risk Management Lifecycle – Process Flow Diagram

WEBLINK TO IMAGE BELOW IN HIGHER RESOLUTION



Glossary of Terms

Authentication: Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.

Authorization: The right or a permission that is granted to a system or entity to access a system resource.

Breach: Means the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information. Visit the HHS site for a complete definition of a Breach.

Business Associate Agreement: A "business associate" is a person or entity, other than a member of the workforce of a covered entity, who performs functions or activities on behalf of, or provides certain services to, a covered entity that involve access by the business associate to protected health information. A "business associate" also is a subcontractor that creates, receives, maintains, or transmits protected health information on behalf of another business associate. The business associate contract also serves to clarify and limit, as appropriate, the permissible uses and disclosures of protected health information by the business associate, based on the relationship between the parties and the activities or services being performed by the business associate. Visit the HHS site for a complete definition of a Business Associate Agreement (BAA).

Business Impact Analysis (BIA): Business impact analysis (BIA) is a process that identifies the potential effects of an interruption to critical business systems and/or operations. These interruptions typically are a result of a natural or man-made disasters, accidents or emergencies.

Configuration Management Data Base (CMDB): A configuration management database contains information about hardware and software within an organizations Information Technology environment.

Controls: A safeguard or countermeasure prescribed for an information system or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements. (Synonym, Security Controls)

Cyber Insurance: Cyber-insurance is an insurance product used to protect businesses and individual users from Internet-based risks, and more generally from risks relating to information technology infrastructure and activities. Wikipedia

Cyber Risk: The overall risk of financial loss, disruption or damage to the reputation of an organization from some sort of failure of its information technology systems.

Disaster Recovery/Business Continuity Program (DR/BCP): A Disaster Recovery plan is a written plan for processing critical applications in the event of a major hardware or software

failure or destruction of facilities. NIST SP 800-82 Rev 2. A Business Continuity Plan is a document that is a predetermined set of instructions or procedures that describe how an organization's mission/business processes will be sustained during and after a significant disruption. NISP SP 800-34 Rev 1

Enterprise Risk Management Program: The methods and processes used by an enterprise to manage risks, including the identification, prioritization and remediation of risks that will have an impact on the enterprise mission. The program would include the Enterprise Risk Management policy, procedures and reporting structure for enterprise leadership review and action.

Enterprise Resource Planning: A system that integrates enterprise-wide information, including human resources, financials, manufacturing, and distribution, and connects the organization to its customers and suppliers(see NIST SP 800-82 Rev 2)

Firewall: An inter-network gateway that restricts data communication traffic to and from one of the connected networks (the one said to be "inside" the firewall) and thus protects that network's system resources against threats from the other network (the one that is said to be "outside" the firewall).

Gap Assessment: An assessment designed to assist your organization in obtaining full compliance with the appropriate regulations, guidelines and/or best practices. The resulting report will summarize your organization's current level of compliance and provide the details for developing appropriate corrective action. (See https://www.riskbasedsecurity.com/gap-analysis/)

Impact: The effect on organizational operations, organizational assets, individuals, other organizations, or the Nation (including the national security interests of the United States) of a loss of confidentiality, integrity, or availability of information or an information system.

Incident: An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. (Synonym: Security Incident)

Intrusion Detection: The process of monitoring events occurring in a computer system or network and analyzing them for signs of possible incidents.

Intrusion Prevention: The process of monitoring the events occurring in a computer system or network, analyzing them for signs of possible incidents, and attempting to stop detected possible incidents.

Large Organization: An organization that typically has dedicated Information Technology functions including a Chief Information Security Officer and dedicated cybersecurity staff.

These organizations will typically have integrated delivery networks across multiple geographical locations. Large size organizations include but are not limited to Health Plans, national device manufactures and pharmaceutical companies. HICP Table 1

Least Privilege: A security principle that restricts the access privileges of authorized personnel (e.g., program execution privileges, file modification privileges) to the minimum necessary to perform their jobs.

Malware: Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code.

Medium Organization: Will typically have some dedicated Information Technology staff performing various functions, including cybersecurity. The overall size of the organization is typically will not exceed 50 physicians or 500 providers across a single of multiple geographical locations. Medium size organizations include but not are limited to Practice Management organizations, smaller device manufacturers and small payor organizations. HICP Table 1

Patch: A "repair job" for a piece of programming; also known as a "fix". A patch is the immediate solution to an identified problem that is provided to users; it can sometimes be downloaded from the software maker's web site. The patch is not necessarily the best solution for the problem, and the product developers often find a better solution when they package the product for its next release. A patch is usually developed and distributed as a replacement for or an insertion in compiled code (that is, in a binary file or object module). In many operating systems, a special program is provided to manage and track the installation of patches.

Privilege(s): A right granted to an individual, a program, or a process.

Risks: A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. Information system-related security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation. (See NIST SP 800-53 Rev 4 under Risk (FIPS 200))

Risk Appetite: The amount and type of risk that an organization is willing to take in order to meet its strategic objectives.

Risk Assessment Framework: A strategy for prioritizing and sharing information about the security risks to an organization's data and information technology components. The program will typically define the roles and responsibilities and a common assessment method for

identifying the vulnerability and likelihood of the event occurring and the overall impact. The Risk Assessment Framework should also include the documentation of the results of the assessment and reporting results to stakeholders.

Risk Register: A tool for documenting risks, and actions to manage each risk. The Risk Register is essential to the successful management of risk. A Risk Register helps in documenting the risk and the actions taken to respond to the risk.

Root Cause Analysis: A principle-based, systems approach for the identification of underlying causes associated with a particular set of risks.

Safeguards: Actions, devices, procedures, techniques, or other measures that reduce the vulnerability of an information system.

Security Assessment: The testing or evaluation of security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for an information system or organization. NIST SP 800-53 Rev 4

Small Organization: An organization that will typically not a have dedicated Information Technology or Cybersecurity staff. These functions could be outsourced to third parties. The overall size of the organization typically will not exceed 25 physicians or providers. (See HICP Volume 1)

Supplier: Product and service providers used for an organization's internal purposes (e.g., IT infrastructure) or integrated into the products of services provided to that organization's Buyers. NIST CSF v1.1 "Supplier" in the context of this document may be public or private sector, for profit or not for profit and may provide software, hardware and/or services and also non-technology enabled products and services.

Supplier Risk Management Program: A comprehensive enterprise program for managing the risks associated with the Information Technology products and services provided by an organization's suppliers. The program typically consists of a policy defining the roles and responsibilities of an organization's teams in managing suppliers, contract language obligating the supplier to meet the organization's cybersecurity program, a supplier cybersecurity assessment program to validate how a supplier is meeting their contractual obligations and a reporting mechanism to track and report to the organization's leadership.

Supplier Risk Profile: A quantitative or qualitative assessment of a supplier's ability to meet the organization's cybersecurity program. The assessment method will include the type of data, volume of data, the maturity of their cybersecurity program, the complexity and size of their organization, and their ability remediate identified gaps.

Supply Chain: Linked set of resources and processes between multiple tiers of developers that begins with the sourcing of products and services and extends through the design, development, manufacturing, processing, handling, and delivery of products and services to the acquirer. NIST 800-53 Rev 4

Technical Controls: The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system.

Threat: An event or condition that has the potential for causing asset loss and the undesirable consequences or impact from such loss.

Value Added Reseller: A value-added reseller is a company that adds features or services to an existing product, then resells it as an integrated product or complete "turn-key" solution. This practice occurs commonly in the electronics or IT industry, where, for example, a VAR might bundle a software application with supplied hardware. Wikipedia

Vulnerabilities: A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy. (See NIST SP 800-47)

Acknowledgements

The co-chairs are grateful for the significant investment of personal time by the authors of this document in its creation. The authors represent some of the most skilled and experienced experts in their field and this document would not have been possible without their generosity, leadership and commitment to a more secure health sector supply chain. We would also like to acknowledge the support of the authors' employers in lending their employee's time, office facilities and information technology infrastructure in the development of this material. We especially grateful for the leadership and editorial skills of Greg Garcia, Executive Director of the HSCC-CWG and to the support of Omar Tisza, Business Operations Coordinator.

While many individuals supported and assisted in the development and review of this content, the primary authors of the first iteration of this document were:

- Steve Dunkle, Chief Information Security Officer, Geisinger Health
- Phil Englert, Specialist Leader, Deloitte
- Justin Formosa, Cyber Security Specialist, Shriners Hospital for Children
- Jon Fredrickson, Information Security & Privacy Officer, Blue Cross Blue Shield of Rhode Island
- Vish Gadgil, Director of IT Risk Management, Security and Compliance, Merck
- Ed Gaudet, CEO, Censinet
- Ty Greenhalgh, CEO, Cyber Tygr
- Dave Leonard, Executive Advisor, Anthem
- Gabe Portillo, GRC Program Manager, University of Chicago Health
- Rich Skinner, Senior Principal, West Monroe Partners
- Darren Vianueva, Senior Vice President, Trinity Health
- Chris van Schijndel, Cybersecurity Director – Customer and Logistics, Johnson & Johnson

##