Healthcare & Public Health
Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

Manage Risks

Secure Medtech

Supplement to Health Industry Cybersecurity – Managing Legacy Technology Security (HIC-MaLTS)

A Quick Reference Guide

April 2023

Table of Contents

I. About this document

This is a supporting document of HSCC Cybersecurity Working Group's Healthcare Industry Security – Managing Legacy Technology Security[1] (HIC-MaLTS) which was released in March 2023. To aid the reader in better use of the HIC-MaLTS document depending on your persona, this document attempts to define different goals which may be applicable to you. Based on your specific role and relevant goal in legacy technology security risk management; you may have questions on how to address areas towards attaining this goal. This document provides a quick reference to relevant contents within the HIC-MaLTS document to address different questions which may arise towards attaining the goals.

II. The Goals

The following goals are identified as most common for persona within HDOs, MDMs and other stakeholders. Once you identify the goal which best aligns with your role, the table in section III can be used to identify content which could address the questions you may have to achieve this goal.

[1] https://healthsectorcouncil.org/wp-content/uploads/2023/03/Health-Industry-Cybersecurity-Managing-Legacy-Technology-Security-HIC-MaLTS.pdf

Goal 1: Avoid acquiring legacy technologies, or those that might become legacy quickly or unexpectedly

Goal 2: Manage my non-legacy technologies to keep them non-legacy as long as possible

Goal 3: Protect the legacy technologies that I already have

Goal 4: Make a smart, risk-informed decision about whether I need to replace a given legacy technology in my environment

Goal 5: Comply with SBOM Requirements (and take advantage of SBOM benefits)

Goal 6: Support my customers in managing technologies to keep them as non-legacy as long as possible

Goal 7: Design, deploy, and maintain secure and securable technologies

III. Quick Reference Guide

Questions	Document Section[2]	Page(s)
Goal 1: Avoid Acquiring Legacy Technologies, or Those That Might Become Legacy Quickly or Unexpectedly		
How do I determine whether a technology may be "legacy"?	*Identifying a Potential Legacy Technology*	11-12
How do I make sure I understand what terms/characteristics a technology may have, to know whether it might be "legacy"?	*Terminology*	8-9
How do I develop a strategy around my organization's technology acquisitions and maintenance?	*Defining a Legacy Technology Risk Management Strategy*	14
How do I draft and negotiate my contracts to address legacy technology risks?	*Considerations for Legacy Technology Communications*	19-26
How should I assess a technology for legacy risks?	*Recommendations to Address Legacy Risk Management*	33-34

[2] Section from HIC-MaLTS document published on HSCC website.

Questions	Document Section[2]	Page(s)
	throughout Technology Lifecycles: Product Assessment Stage	
How should I acquire technologies to avoid legacy risks?	*Recommendations to Address Legacy Risk Management throughout Technology Lifecycles: Acquisition Stage*	35
Goal 2: Manage my non-legacy technologies to keep them non-legacy as long as possible		
How do I make sure that I know, understand, and am acting on my technologies' various "ages"?	*Developing a Lifecycle Management Plan*	16
How do I manage my non-legacy technologies to keep them secure and securable for as long as possible?	*Managing Future Legacy Technologies*	31-40
How do I implement technologies in my environment to manage legacy risks?	*Recommendations to Address Legacy Risk Management throughout Technology Lifecycles: Implementation Stage*	36
How do I support technologies in my environment to manage legacy risks?	*Recommendations to Address Legacy Risk Management throughout Technology Lifecycles: Support/Maintenance Stage*	37
How can I keep up with patches?	*Patching Lifecycle Recommendations*	50-69
	Patching	101-107
Goal 3: Protect the Legacy Technologies I Already Have		
How do I identify a potential legacy technology?	*Identifying a Potential Legacy Technology*	11-12
How do I decide how much "risk" I can handle?	*Establishing a model and criteria for risk tolerance*	15
How do I manage the risks of my current legacy technologies?	*Managing Current Legacy Technologies*	28
Assess whether I can/should connect technologies to my network, that may not have been designed for that purpose?	*Connectivity*	80-84

Questions	Document Section[2]	Page(s)
Ensure that I understand, am prepared for, and appropriately manage my technologies as they age?	*End-of-Life/End-of-Support*	84-89
Understand how and when I may want to leverage third-party support servicers?	*Third Party Servicers*	89-91
Fully identify, track, and manage my inventory of digital technologies?	*Inventory/Asset Management*	91-95
Understand, produce, and effectively use SBOMs?	*SBOM*	95-101
Keep up with patches, and design my patching procedures to be as least burdensome and effective as possible?	*Patching*	101-107
Understand the benefits and risks that third-party components may pose, and what I may do to effectively manage them?	*Third-Party Component Risk Management*	107-112
Goal 4: Make a Smart, Risk-Informed Decision About Whether I Should Replace a Given Legacy Technology		
Legacy technologies exist in my environment, and I recognize that they should be replaced to mitigate or avoid potential cybersecurity risks, but I have very real and very significant competing organizational priorities. How do I make a smart, risk-informed decision about whether I should replace a given legacy technology?	*Responsibility Transfer Framework*	43-50
Goal 5: Comply with SBOM Requirements (and take advantage of SBOM benefits)		
My customers, the government, and my own organization are demanding that I use, produce, and/or consume SBOMs. How do I familiarize myself with what SBOMs are, what they are for, and how I can most effectively take advantage of them?	*Communications, SBOM*	22-23
	Challenges and Recommendations: SBOM	95-101
Goal 6: Support my customers in managing technologies to keep them as non-legacy as long as possible		

Questions	Document Section[2]	Page(s)
How do I understand what support expectations/needs my customers may have, and how to appropriately negotiate them?	*Considerations for Legacy Technology Communications*	19-26
Assess whether to connect technologies to networks, that may not have been designed for that purpose?	*Connectivity*	80-84
Ensure that I understand, am prepared for, and appropriately manage my technologies as they age?	*End-of-Life/End-of-Support*	84-89
Understand how and when I may want to leverage third-party support servicers?	*Third Party Servicers*	89-91
Make it easy for my customers to identify, track, and manage my technologies in their environments?	*Inventory/Asset Management*	91-95
Understand, produce, and effectively use SBOMs?	*SBOM*	95-101
Keep up with patches, and design my patching procedures to be as least burdensome and effective as possible?	*Patching*	101-107
Understand the benefits and risks that third-party components may pose, and what I may do to effectively manage them?	*Third-Party Component Risk Management*	107-112
Goal 7: Design, deploy, and maintain secure and securable technologies		
How may I design an effective, efficient cybersecurity risk management program?	*MDM Risk Management Considerations*	40-43
How do I proactively consider the potential legacy risks that my technologies may face, and how to design to control for those risks?	*Recommendations for Addressing Known Legacy Issues During Threat Modeling*	70-73
How may I design secure technologies that address legacy risks, including the criteria I use to select what software I may use in my technology?	*Recommendations for Secure Technology Design, Including Software Selection*	73-78
How may I facilitate my customers' secure deployment of my technologies?	*Recommendations to Facilitate Secure Technology Deployment*	78-80

Questions	Document Section[2]	Page(s)
Assess whether and how to connect technologies to networks, that may not have been designed for that purpose?	*Connectivity*	80-84
Ensure that I understand, am prepared for, and appropriately manage my technologies as they age?	*End-of-Life/End-of-Support*	84-89
Understand how and when I may want to leverage third-party support servicers?	*Third Party Servicers*	89-91
Make it easy for my customers to identify, track, and manage my technologies in their environments?	*Inventory/Asset Management*	91-95
Understand, produce, and effectively use SBOMs?	*SBOM*	95-101
Keep up with patches, and design my patching procedures to be as least burdensome and effective as possible?	*Patching*	101-107
Understand the benefits and risks that third-party components may pose, and what I may do to effectively manage them?	*Third-Party Component Risk Management*	107-112

IV. About the Health Sector Coordinating Council

The Healthcare and Public Health Sector Coordinating Council (HSCC) is a coalition of private-sector critical healthcare infrastructure entities organized under the National Infrastructure Protection Plan to partner with and advise the 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 300 industry and government organizations working together to develop strategies to address emerging and ongoing cybersecurity challenges to the health sector.