Contents

[1 Executive Summary 3](#_Toc95501622)

[2 Engagement and Training 4](#_Toc95501623)

[2.1 Why Security Matters 4](#_Toc95501624)

[2.2 Cultural Analysis 4](#_Toc95501625)

[2.3 Localization Requirements 5](#_Toc95501626)

[2.4 Branding and Imagery 5](#_Toc95501627)

[2.5 Training 6](#_Toc95501628)

[3 Metrics 7](#_Toc95501629)

[3.1 Impact Metrics 7](#_Toc95501630)

[4 Appendix A: Medical Device Security Topic and Operating Unit Department Matrix 8](#_Toc95501631)

[5 Appendix B: Learning Objectives 8](#_Toc95501632)

[5.1 Risk 8](#_Toc95501633)

[5.2 Goal 9](#_Toc95501634)

[5.3 Background 9](#_Toc95501635)

[5.4 Learning Objectives 9](#_Toc95501636)

# Executive Summary

The first tenant of our mission is to “extend the life of all patients.” This has guided our company since 1961. As our company and the devices that we engineer have grown more complex over the last 6 decades, we have never changed this or any other tenant of our mission statement. However, as the world and our industry have changed, we have adapted how we carry out these tenants of our mission to ensure we fulfill their original intent.

Tenant 3 of our mission requires us to “create the highest quality medical devices” and is central to supporting our first tenant. As our devices become more complex and more connected to fulfill the first tenant, we need to adapt how we ensure the greatest possible reliability and quality in our products as patient safety risk isn’t the only risk that we need to be managing in the future.

Security risks create safety risks for our patients. Managing security risks in our products is fast becoming as critical as managing safety risks because of the increased use of technology within our devices. Almost every medical device that was approved for Medical Marvels in calendar year 2021 had an embedded operating system and code running on that operating system that wasn’t developed at Medical Marvels. Conversely, the number of security vulnerabilities found in operating systems and application-level components continues to increase year-over-year. Our leveraging of software and firmware code created outside of Medical Marvels has enabled greater growth and capabilities than in the past, but it also comes with significant security risks that we have yet to truly understand and manage.

Regulators are also holding us accountable. Without their approval, the medical devices that we spend years engineering and getting ready for market can’t be sold. They recognize the increased risk that technology-enabled medical devices bring to patients that use them. As such, they have begun denying Medical Marvels submissions of new medical devices due to security concerns alone. Without broad awareness of this topic across the company as well as focused training within Operating Units, the security risks in our devices will continue to be unmanaged creating safety risks for our patients and business risk for our company.

A security awareness and training program is an organization-wide effort that enables us to effectively manage the security risks in our devices by changing our workforce’s behaviors through engagement and training. This program brings broad awareness to all of Medical Marvels on what medical device security is as well as brings focused training to Engineering, Quality, and Regulatory Affairs departments within each Operating Unit on how to integrate security into the design of new devices and manage the security risks of devices already in the marketplace.

This awareness and training program will enable our company to know how to effectively manage the security risks in our products throughout their lifecycle as well as convincingly present our management of security risks in our devices to our regulators across the globe.

# Engagement and Training

This Security Awareness Program’s objective is to help medical device development teams understand the relevant security risks for their new development projects as well as the current expectations for security controls from regulators. Many of our next-generation medical devices are enabled with increasingly complex technology and are becoming more connected with supporting ecosystem components in hospitals. The increasingly complex technology in devices compounded by the ecosystem of connected components presents a much greater attack surface which, if exploited, could lead to significant safety or privacy impacts. Continuous training on contemporary security threats and regulator expectations will reduce the likelihood of security, safety, or privacy risks being realized as well as accelerate the time to market for life-saving therapies by shortening the regulatory review process.

## Why Security Matters

Medical device development teams need to understand the necessity and value of security considerations throughout the lifecycle of their new development projects. Communication on necessity and value of security will occur through two methods:

* **Organizational**: The tenants of our Mission reinforce that we will always be focused on the development of increasingly complex medical devices to solve increasingly complex diseases and healthcare challenges. Security risks inherent in the medical devices we engineer could create patient safety issues, which means we must treat security risks with the same level of rigor we treat safety risks. Our organizational communication will ensure “We build Security into our DNA.”
* **Operating Unit**: Operating Units operate as almost independent companies within Medical Marvels. They are responsible for the development (pre-market) and maintenance (post-market) of all the medial devices that they engineer. Embedding security into the lifecycle of a new medical device requires following a framework of security activities during development as well as performing vulnerability monitoring, assessment, and field updates once the device is on the market. Primary groups within Operating Units that are predominantly responsible for identification and management of security risks in medical devices during pre-market and post-market include Engineering, Quality, and Regulatory Affairs. Each group has a specific responsibility for security risks, which will require a specific training curriculum for each group within each Operating Unit. The matrix of medical device security topics mapped to each target group within the Operating Unit can be found in Appendix A.

## Cultural Analysis

The nature of the medical device manufacturing industry is highly regulated and very conservative. Patient safety is paramount in everything that a medical device manufacturer does. This is reinforced by continuously sharing patient stories of how our medical devices extend the lives of our patients throughout the world. Employees work for this company because they believe in the mission and that our medical devices positively impact the world. Using humor or FUD (fear, uncertainty, and doubt) in our training program will go against the ideals of both employees and leadership.

Our training curriculums will capitalize on both the patient safety and regulated aspects of our company. Increased technology and connectivity will create safety risks that need to be understood and appropriately managed. This connection between security impacting safety will convey the criticality of this topic while also speaking in the language that the organization understands very well. Additionally, regulators around the world have and will continue to reject submissions of our new regulated devices to be sold in their geography’s marketplaces due to security concerns alone. Specifically, Operating Units need to understand what the current expectations are from regulators regarding relevant security risks as well as acceptable layers of security controls.

## Localization Requirements

We are a global organization with over 100 offices worldwide. Company policy dictates that organization-wide training content needs to be available in a certain set of languages. To support this requirement, there is a team of translation specialists available in the company. There is no policy requiring training content to be in certain languages if they are not delivered to the entire organization.

Our organization-wide training content will be delivered through our learning management system called Foundations, where we will leverage our translation specialists to make the content accessible and understood for all employees. The organizational training will be automatically assigned and tracked through Foundations.

Operating Units have employees across the world. However, our targeted departments of Quality, Engineering, and Regulatory Affairs in each Operating Unit are predominantly in America, Europe, Middle East, China, and Japan. Through feedback that our leadership has received from the President of each Operating Unit, training content should be delivered in just English. However, the training content should also be delivered live (in-person or over video conference) as to allow the opportunity for questions if something isn’t understood by the attendees because of a translation issue.

## Branding and Imagery

Our organization has a strong internal branding team. However, due to the size of our company, it is impractical for the branding team to review all content before it is delivered internally or externally. As such, they provide numerous templates, images, and icons that can be freely used by any Medical Marvels employee for any internal or external content that is prepared. However, the internal branding team is available for consultation when asked.

Our leadership has reaffirmed that there is no need for a formal review and approval by branding for creation of our Operating Unit curriculum content. However, our leadership has required us to receive review and approval on our organization-wide training content in Foundations before it is assigned to all company employees.

We will leverage all available templates, images, and icons as appropriate for both the organization-wide as well as the Operating Unit content to maintain the same format across all medical device security training and awareness efforts.

## Training

Our organization-wide training will be included in the annual Quality training where patient safety risk is already included. This way we will leverage the communication and translation plans already in place for this broader training. Our Operating Unit training will be delivered live through our virtual meeting software, WebEx.

**Primary Training**: The primary method we use to communicate our organization-wide training is Computer Based Training (CBT) through our internal learning management system called Foundations. This allows our employees to take the training on-demand as their schedule allows and is easy to implement in a way that can track participation and include evaluations as part of the training. During online training, all users also take an online quiz to test comprehension of the medical device security module of the overall Quality training. The goal of the annual training is to both set the baseline training for our organization and ensure we are compliant. The corporate Quality team assumes operational control of online awareness training and enforces this policy. However, our medical device security awareness team will assist corporate Quality in this awareness to ensure security is highlighted as a new module this year.

The primary method we use to communicate our Operating Unit training is through live Instructor Led Training (ILD) over WebEx video conferences. The smaller group sizes of either Engineering, Quality, or Regulatory Affairs in each Operating Unit will lend themselves to more audience interaction and questions on how the topic of medical device security applies to them as well as recommendations on how to implement both pre-market and post-market concepts in their departments going forward. This training will be mandatory and required by leadership of Engineering, Quality, and Regulatory Affairs within each Operating Unit. Attendance will be tracked through WebEx attendee listing that is automatically generated from attendees joining the scheduled WebEx teleconferences. Our leadership will work with the leadership teams in each Operating Unit to schedule and communicate the requirement of this training for their employees.

**Reinforcement Training and Awareness**: One instance of training our target stakeholders is not enough to change culture across a large company. We will reinforce key behaviors through the following methods throughout the year:

* **Medical Device Security Symposium**: An annual internal conference dedicated to this topic where we will have presentations and panels providing an update on trending topics of interest over the past year. Attendance will be optional but encouraged with recordings of all symposium sessions saved for later reference by internal employees.
* **Bi-Monthly** **Touchpoint:** A 90-minute meeting every other month where recent developments in regulator or customer expectations, external standards or guidance documents, or new company-wide projects on medical device security are shared and discussed. Attendance is optional with recordings saved of each meeting for reference.
* **Medical Device Security Advisory Council**: A quarterly meeting between leadership of corporate medical device security and leadership of each Operating Unit to cover recent external developments on this topic, decide on organizational-wide funding for resources, and agree on strategic direction for this topic across the company.

# Metrics

Metrics will be collected to allow for measuring and managing the training and awareness program. Further, these metrics will demonstrate the impact the program is having to Leadership. Two categories of metrics will be tracked:

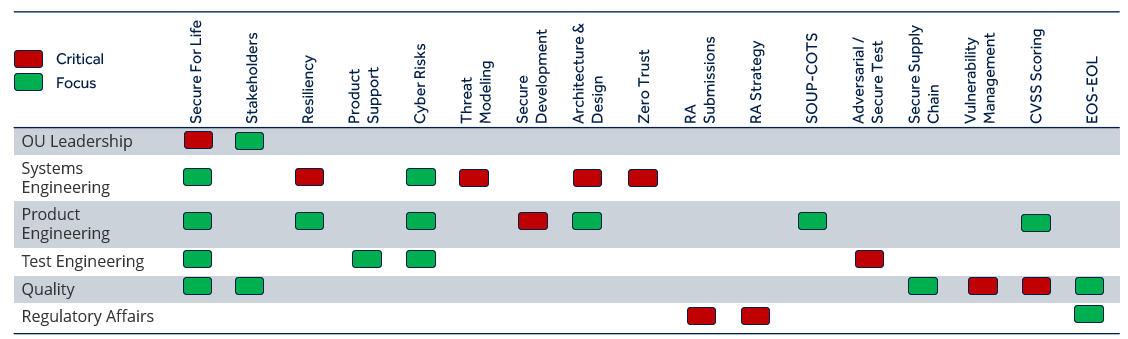
* **Compliance**: Ensure our organizational-wide content is being taken and understood by all company employees so that we can demonstrate results to our regulators. We will track completion of the quiz questions by all employees that take the Quality training in Foundations to ensure our entire organization meets the compliance standards established by global regulators. This metric will be tracked annually by the corporate Quality team who manage the completion of the entire Quality training of which medical device security is a discrete module.
* **Impact**: Measure the changes we’re having across the Operating Units with the inclusion of security risks in their development process as well as the continuous monitoring of security risks once medical devices are on the market. These metrics will be measured by each Operating Unit to maintain clear reporting lines to Operating Unit leadership.

## Impact Metrics

Our goals are to ensure appropriate security controls in our new products, maintained security of our devices in the market, and faster approval for our new devices due to less security deficiency comments from our regulators. We track the following metrics to measure the impact of our training and awareness program towards these goals.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Metric Name** | **What Is Measured?** | **How Is It Measured?** | **When Is It Measured?** | **Who Measures?** |
| Security Risks Mitigated | Number of security risks identified and mitigated through security control requirements during development of new medical devices. | Tracked by the number of security risks itemized with associated security risk requirements in the Security Risk Assessment Quality document required for every new medical device being developed. | Quarterly | Corporate Quality team |
| Regulator Security Deficiency Comments | Number of deficiency comments related to security across all our medical device regulatory submissions each fiscal year. | Tracking by the corporate Regulatory Affairs team who has visibility into all deficiency comments from all submissions. | Quarterly | Corporate Regulatory Affairs team |
| Security Bulletins | Number of Security Bulletins issued to the public on our corporate website advising on current vulnerabilities affecting our devices on the market as well as available mitigations. | Tracked by number of public security bulletins issued on our corporate website. | Quarterly | Medical device security team |

# Appendix A: Medical Device Security Topic and Operating Unit Department Matrix



# Appendix B: Learning Objectives

## Risk

Incomplete and inaccurate Security Risk Assessment.

## Goal

Participants will explain and demonstrate how executing a threat modeling methodology will lead to a complete identification of security risks and accurate assessment of those risks affecting their medical device. This more thorough identification and assessment of security risks will lead to more holistic management of security risks that could impact patient safety as well as create more defendable documentation for the device’s submission to regulators.

## Background

Incomplete identification and inaccurate assessment of security risks in a Security Risk Assessment document has been the primary source of regulator deficiency comments over the past two calendar years. As such, a focus on how to identify security risks more completely and assess them more accurately is needed. Industry collaboration with regulators over the past two calendar years has concluded that a structured threat modeling methodology leveraging frameworks like STRIDE is the standard for producing complete and accurate Security Risk Assessments of medical devices. This module teaches a structured threat modeling methodology using the STRIDE framework applied to medical devices.

## Learning Objectives

1. Learners can explain the steps of the threat modeling methodology: identify assets, identify threats, identify vulnerabilities, assess risks, and identify control requirements.
2. Learners can create a threat model architecture diagram for their medical device as a deliverable for the “identify assets” step in the threat modeling methodology.
3. Learners can prioritize security risks by correctly using the CVSS 3.0 scoring system while also leveraging the [MITRE Rubric](https://www.mitre.org/publications/technical-papers/rubric-for-applying-cvss-to-medical-devices) technical paper.