Medical Technology Company Security Procedure Template

The following Product Security Work Instruction (SWI) Template is provided below in furtherance of our commitment to transparency and collaboration with customers and industry stakeholders.

1.0 PURPOSE

1.1 The purpose of the [insert company name] SWI is to provide [insert company name] Business Units with the proper guidance for ensuring products and software enabled commercial offerings are secure by design, in use, and through partnership throughout the product lifecycle.

2.0 SCOPE

2.1 This SWI is applicable to [insert company name] functions that may take part in any aspect of the following:

2.1.1 Design, development, manufacturing, service and support of [insert company name] products that provide software or firmware solutions including medical devices, cloud-based solutions, and software-only products.

2.1.2 Third-party entities that [insert company name] collaborates with at any point in the product lifecycle including acquisition, development and servicing that does business with [insert company name] products or are in acquisition.

2.2 This document is not intended to provide guidance to update related business unit procedures and is exempt from:

2.2.1 Standards or practices regarding concept feasibility, technical development, or products intended without software.

2.2.2 Standards or practices regarding security of [insert company name] internal assets and infrastructure.

2.3 [insert company name] **Assets and Systems:** Includes, but not limited to, equipment used by any function in any aspect of day-to-day business operations that is owned by [insert company name]. Examples such as development **Common Vulnerability Scoring System (CVSS):** A security industry standard for prioritizing the severity of security issues.

2.4 **Controlled Risk:** Controlled risk is present when there is sufficiently low (acceptable) residual risk of patient harm due to a device's particular cybersecurity vulnerability.

2.5 **Critical Functions:** Any product functionality which impacts the clinical safety or significantly disrupts the business operations of customers.

2.6 **Hardening Standards:** A documented process or mechanism for securely configuring or implementing commonly used technologies.

2.7 **Incident Vulnerability and Patch Management:** The systematic monitoring, identification, assessment, remediation, deployment, and verification of operating system and application software code updates. These updates are known as patches, hot fixes, and service packs to operating systems, third-party products and components, and [insert company name] developed software.

2.8 **Penetration Testing:** A test methodology in which assessors, using all available documentation such as system design and working under specific constraints, attempt to circumvent the security features of an information system.

2.9 **Product Lifecycle:** Managing the entire lifecycle of a product from inception, through engineering design and manufacture, to service and disposal of manufactured products.

2.10 **Product Security:** Ensuring the adequate protection of product, customer and patient confidentiality, integrity, availability, and safety by design, in use, and through partnership with all stakeholders defined in the Responsibilities section below throughout the product lifecycle.

2.11 **Product Security Management Plan:** Used to document all Product Security Framework activities carried out through the design process and post commercialization. May also capture technical and process gaps, including exemptions. It is not intended to replace the Product Risk Management File or equivalent.

2.12 **Product Security Risk Assessment:** Overall process comprising a risk analysis and a risk evaluation for security issues found in [insert company name] products using impact to confidentiality, integrity, and availability to patients, customers, and [insert company name] to determine the acceptability of the risk.

2.13 **Removable Media:** Portable electronic storage media such as magnetic, optical, and solid-state devices, which can be inserted into and removed from a computing device, and that is used to store text, video, audio, and image information. Such devices have no independent processing capabilities. Examples include hard disks, floppy disks, zip drives, compact disks, thumb drives, pen drives, and similar USB storage devices.

2.14 **Robustness Testing:** A testing methodology to detect the vulnerabilities of a component under unexpected inputs or in a stressful environment.

2.15 **Secure Coding Standards:** Guidelines for writing software code which mitigates common security flaws specific to a programming language or in general to all software.

2.16 **Security Incident:** An event that may indicate that a device's data and security may have been compromised. This includes, but not limited to:

2.16.1 Attempt to gain unauthorized access to a system or its data

2.16.2 Unwanted disruption or denial of service

2.16.3 Unauthorized use of a system for the processing or storage of data

2.16.4 Changes to system hardware, firmware or software characteristics without owner's knowledge, instruction or consent

2.17 **Sensitive Information and Data:** Protected Health Information (PHI), Personally Identifiable Information (PII), proprietary software source code or business logic, configuration parameters, user credentials, cryptographic keys, quality control and calibration results.

2.18 **Static Code Analysis:** The automated analysis of software code for security flaws and adherence to a secure coding standard.

2.19 **Third-Party Entities:** External individuals and organizations such as vendor and suppliers that [insert company name] collaborate with at any point in the product lifecycle including acquisition,

development and servicing that does business with [insert company name] products or are in acquisition.

2.20 **Threat Source:** The intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally trigger a vulnerability.

2.21 **Uncontrolled Risk:** Uncontrolled risk is present when there is unacceptable residual risk of patient harm due to inadequate compensating controls and risk mitigations.

2.22 **Vulnerability:** A weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a Threat Source.

2.23 **Vulnerability Scanning:** The automated analysis and detection of vulnerabilities such as missing patches and misconfiguration in operating systems and other third-party software.

3.0 RESPONSIBILITIES

3.1 Product Security (PS):

3.1.1 Creation and maintenance of policies, procedures, tooling, guidance, training and awareness for product security across all [insert company name] business units and functions. PS will support product security risk assessments, automated security testing, penetration testing, remediation planning services for R&D and complaint handling.

3.2 Business Unit Product Security Officer:

3.2.1 Oversee and direct the adoption of the [insert company name] Product Security Policy within their business unit, reporting progress to their BU Leadership, and ensuring available PS expertise and resources are utilized.

3.3 Product Security Governance Committee:

3.3.1 Cross-Functional group responsible within each Business Unit providing oversight of [insert company name] Product Security Policy adoption and Exemptions documented in the Product Security Management Plan. This group shall include Product Security, Quality, PPM and other functions as required per Business Unit.

3.4 Corporate and Business Unit Quality:

3.4.1 Ensures the [insert company name] Product Security Policy is aligned and consistent with other [insert company name] corporate policies, as well as global regulations and standards, for product development, risk management, manufacturing, and support. Quality, jointly with PS, will ensure adherence to the [insert company name] Product Security Policy as with any other Quality policy, for example, risk management, supplier quality and reporting requirements for external agencies when applicable.

3.5 Research and Development (R&D):

3.5.1 Incorporates product security in the budgeting, resource planning, design requirements in the development process, and throughout the product lifecycle including post-commercialization maintainability. R&D will maintain record of security defects in accordance with the business unit quality management systems including design control and risk management procedures.

3.6 Product & Portfolio Management (PM, PPM, Core Team Lead or equivalent):

3.6.1 Responsible for ensuring product security is incorporated in budget, resource, project, and roadmap planning activities throughout the product lifecycle.

3.7 Complaint Handling Unit:

3.7.1 Responsible for identifying complaints that have a product security impact and reporting the complaint to PS.

3.8 Service and Support:

3.8.1 Ensure proper response to security incidents and events with products at customer sites, including proper documentation records as per business unit complaint handling procedures. Secure [insert company name] service assets, maintain validated security updates and ensure secure implementation, periodic reporting of security incident and events and security update tracking.

3.9 Business Unit and Regional Leadership:

3.9.1 Responsible for communication, compliance and adherence of the [insert company name] Product Security Policy at the Regional and local business levels. This may include the creation of local procedures that align with and supplement, where needed due to regional laws and regulation, the over-arching [insert company name] Product Security Policy.

3.10 Legal:

3.10.1 Provides Business Units with guidance on incident response, adherence to local security and privacy laws to ensure legal content meets [insert company name] policies.

3.11 Privacy:

3.11.1 Through the Central and Regional Privacy Councils, ensures the appropriate protection of data, such as information from or about our employees, our customers, and users of our products worldwide.

3.12 Regulatory:

3.12.1 Provides Business Units and the PS with guidance on product security and privacy regulation for medical devices including mobile applications and software only products.

3.13 Global Information Security (GIS):

3.13.1 Ensures [insert company name] managed assets, including but not limited to laptops, removable media, and networks that interact with [insert company name] products adhere to the [insert company name] Information Security Policy.

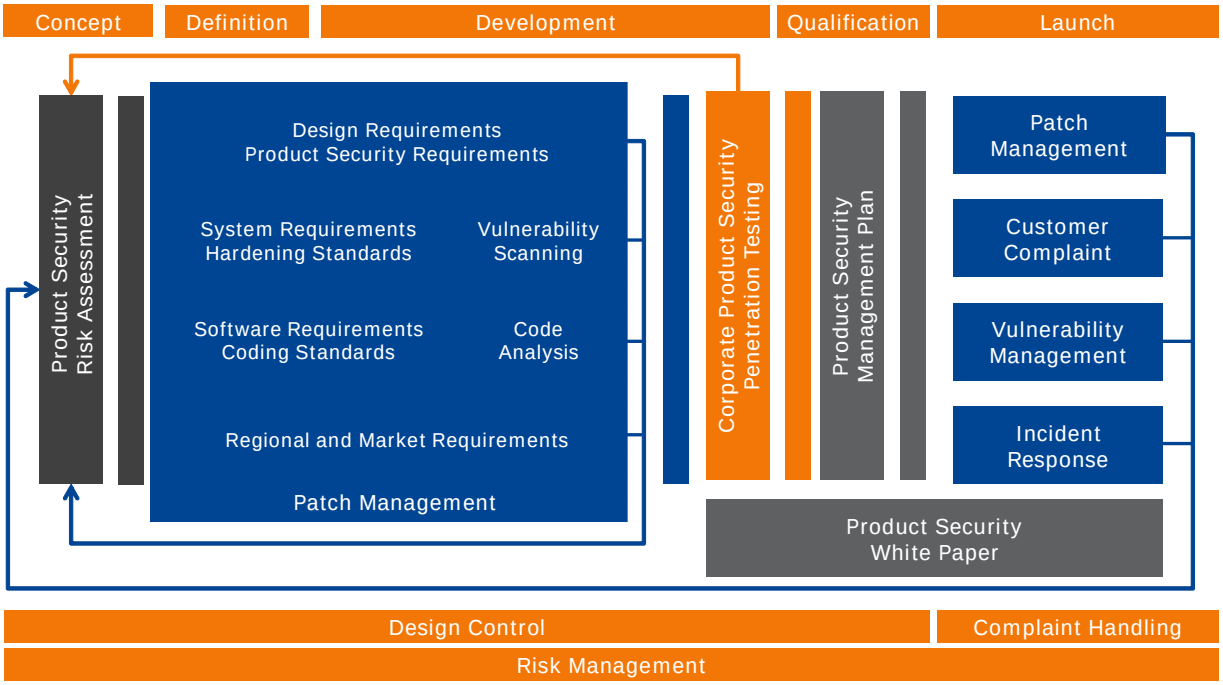
3.14 Third-Party Entities:

3.14.1 Adhere to requirements in the [insert company name] Product Security Policy and [insert company name] Information Security Procedure against entities external to [insert company name] .

4.0 REQUIREMENTS

4.1 The following requirements must be considered during any design, development, manufacturing, service and support of [insert company name] products that provide software or firmware solutions including medical devices, cloud-based solutions, and software-only products. Exemptions and vulnerabilities not being addressed will be documented in the Product Security Management Plan.

4.2 The flowchart below is used to illustrate how product security may be incorporated within existing [insert company name] design control, quality systems and release processes. Additional guidance and details are provided for each activity/process.



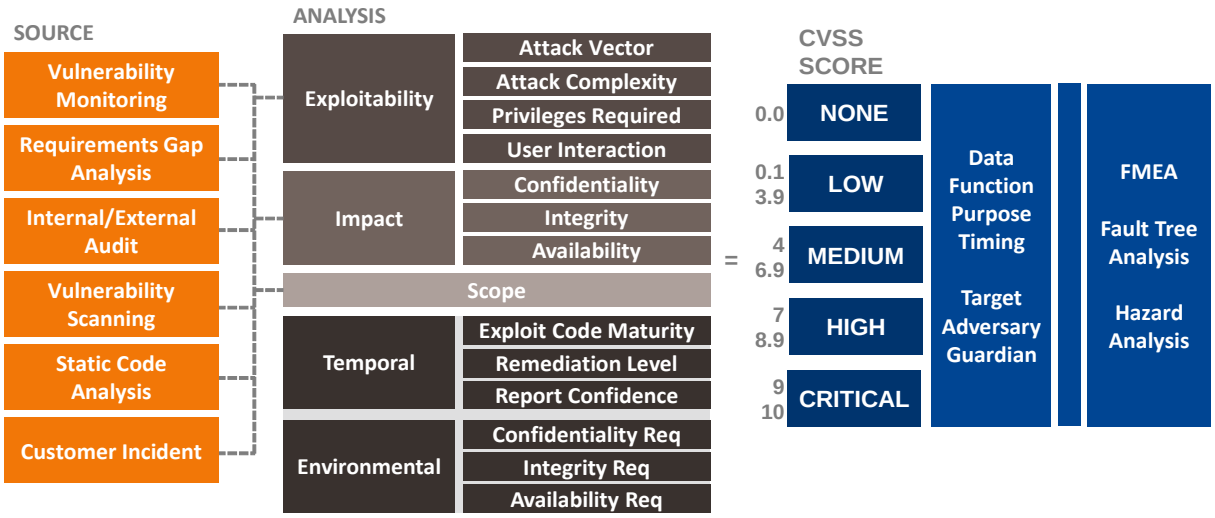
4.3 Risk Management for Product Security: There are specific considerations necessary for ensuring product security risks identified during Design Control and Complaint Handling are properly analyzed, evaluated, and documented.

Product Security Risk Assessment: Vulnerabilities identified in Design Control or complaint investigation must be analyzed and evaluated by PS and the corresponding project/product team using the Common Vulnerability Scoring System (CVSS) to derive the level of security risk.

PS shall review product security risk assessment outcome with Medical Affairs and Quality to determine if any security risk has a potential safety harm to the patient. At a minimum, security risk that impacts data integrity or device availability must be assessed for potential safety harm to the patient. If a security risk is determined to have a potential safety harm to the patient, it will be processed further as product safety risk in accordance with the business unit product risk management policy or procedure.

4.3.1 The diagram below is an example of the sources from which a vulnerability may be identified, the analysis categories used to score the vulnerability and the output of that analysis.

4.3.1.1 For examples of product security risks in reference to ISO14971, please see ..



4.3.1.2 None to Low Risk: Negligible or no impact to Confidentiality, Integrity, or Availability to the patient, user, [insert company name] or customer environment.

4.3.1.3 Medium to High Risk: Introduces potential vulnerabilities that may result in adverse events impacting Confidentiality, Integrity, or availability to the patient, user, [insert company name] or customer environment.

4.3.1.4 Critical Risk: Introduces potential for injury or harm to patients or users of [insert company name] products including impact to Sensitive Information and Data or Critical Functions.

4.3.2 Remediation Planning

4.3.2.1 Products In-Development: See the Design Control section below.

4.3.2.2 Products Commercialized: See the Complaint Handling section below.

4.3.2.3 Corrective and Preventative Action Plans: Evaluate the need to correct existing or potential quality issues that impact the security of [insert company name] products, and to develop actions to prevent their occurrence or recurrence in compliance with corporate or business unit CAPA policy/procedure.

4.3.3 Exemptions: A risk which is not addressed will require documentation of the risk assessment performed and the remediation planning that was not pursued.

4.4 Design Control for Product Security: Security vulnerabilities and controls shall be incorporated in the corporate or business unit design control policy/procedure. The following shall be used as additional requirements to be considered and implemented as part of product development.

4.4.1 Risk Assessment and Remediation: Throughout Design Control a product security risk assessment is necessary to determine the level of risk and subsequent actions for security requirements including remediation planning.

4.4.1.1 Low Risk: Address or document risk as an Exemption.

4.4.1.2 Medium to High and Critical Risk: Address as requirements for design input and mitigate accordingly.

4.4.2 Design Input: Includes applicable high-level security requirements for products based on authoritative sources as well as customer feedback.

4.4.3 Standards and Testing: The following standards and testing shall be applied to software code in development and components provided by third-party entities used in [insert company name] products.

4.4.3.1 Hardening Standards: For securely configuring all products and components used in the [insert company name] product, identify, apply, and maintain an available hardening standard provided by the component vendor or an authoritative source

4.4.3.2 System Patching: Throughout the product development process patches for system-level products and components, including those provided by third-party entities, must be identified, applied, and maintained. Remediation planning including an upgrade of the products and components must be considered if patching is no longer available. See the Incident Vulnerability and Patch Management section below.

4.4.3.3 Vulnerability Scanning: Periodically throughout product development automated testing must be performed to ensure secure system configuration and patching.

4.4.3.4 High-Level Secure Coding Standards: See internal Product Security Authoritative Sources and Guidance for examples of secure coding standards that are generic to any programming language used for the development of software.

4.4.3.5 Language-Specific Secure Coding Standards: See internal Product Security Authoritative Sources and Guidance for examples of secure coding standards that are specific to a programming language used for the development of software.

4.4.3.6 Static Code Analysis: Periodically throughout product development automated testing must be performed to ensure secure coding standards are followed.

4.4.3.7 Software Patching: Throughout the product development process product software must provide and maintain the capability to patch products and components, including those provided by third-party entities, with minimal

disruption to system operation. See the Incident Vulnerability and Patch Management section below.

4.4.3.8 Robustness Testing: During unit and interface testing of proprietary software in development, interfaces such as user interfaces, network protocols, and file inputs must be tested for ability to withstand and handle potentially malicious input.

4.4.4 Regional Requirements: Based on intended market for the product and in consultation with Legal, Regulatory, and Privacy identify regional security requirements that may apply to product.

4.4.5 Incident Vulnerability and Patch Management: Prior to release or commercialization a plan must be established to identify, evaluate, and respond to any incident or vulnerability including routine patching throughout the product lifecycle.

4.4.5.1 Monitor and Identify: Continuously track and plan for security incidents, vulnerabilities, patches, and end of support dates from predefined sources based on inventory of products and components including those provided by third-party entities.

4.4.5.2 Risk Assessment and Remediation Planning: Determine applicability of vulnerabilities and patches along with Product Security Risk Assessment to determine the level of risk and subsequent actions necessary.

4.4.5.2.1 Medium to High and Critical Risks: Patches must be applied or made available with at least one of the deployment methods within a maximum of 30 days after initial discovery.

4.4.5.2.2 Low Risks: May be addressed separately in a reasonable amount of time however at minimum during the next product or software update.

4.4.5.3 Validate: Remediation of vulnerabilities including patches shall be validated in compliance with [insert company name] internal Design Control Policy.

4.4.5.4 Deployment: At least one of the following methods will be made available for commercialized products to apply validated security patches.

4.4.5.4.1 Customer Administered: Validated patches will be made available for customer retrieval and installation from a [insert company name] source or direct download from the third-party entity that provides the product or component.

4.4.5.4.2 Ad-hoc Patching: Customers may accept risk for all other deployment mechanisms and/or application of security patches not validated by [insert company name] .

4.4.5.4.3 Remote Update: Patches applied via authorized remote service and support platforms.

4.4.5.4.4 Service Visit: Local service administered security patches.

4.4.5.5 Reporting: Customers shall be notified of security patches and upgrades for [insert company name] products through the public [insert company name] Product Security webpage. For [insert company name] managed remote updates and service visits, routine reporting of failures to patch products in the field is necessary including products and components provided by third-party entities that are no longer supported by their vendor.

4.4.6 Penetration Testing: PS will verify security testing performed and security controls implemented during Design Control near or at completion of Risk Remediation. In addition, PS will perform custom security testing methodologies to ensure comprehensive test case coverage.

4.4.7 Product Security White Paper: Any commercialized product must develop and maintain documentation internally and externally available which describes all pertinent security information related to the product.

4.4.8 Product Security Readiness: Prior to commercialization of a product, a Product Security Management Plan must be created by R&D, reviewed by the Product Security Governance Committee, and approved by the PPM and [insert company name] Product Security Officer.

4.5 Complaint Handling for Product Security:

4.5.1 Escalation: Complaint evaluation or investigation shall include steps to determine if there is a product security incident. PS will be notified if a complaint is determined to have a product security incident. The Business Product Security Officer may create a cross-functional task force to ensure a coordinated investigation and appropriate response. Service and Support must have adequate classification of potential security issues for their product to ensure effective escalation and triage.

4.5.1.1 PHI or PII: If the complaint is associated with protected health information or personally identifiable information then [insert company name] regional Privacy Officer must be notified to ensure applicable breach notification rules are followed.

4.5.1.2 [insert company name] Assets and Information: If the complaint is associated with [insert company name] assets then [insert company name] Global Information Security (GIS) must be notified in addition to the regional Privacy Officer.

4.5.2 Risk Assessment and Remediation Planning shall be performed as part of the complaint investigation.

4.5.2.1 Low Risks: May be addressed separately in a reasonable amount of time however at minimum during the next product or software update.

4.5.2.2 Medium to High and Critical Risks: Communicates with the customer and user community about the vulnerability, interim control and remediation plan within 30 days after learning of the vulnerability. Patches must be available with at least one of the deployment method within a maximum of 60 days after initial discovery. PHI or PII: Unauthorized disclosure of PHI or PII will require data breach investigation and potential notification to customers.

4.5.2.3 Other Sensitive Information and Data: Unauthorized disclosure of other Sensitive Information and Data such as intellectual property will require data breach investigation and potential notification to customers.

4.5.3 Reporting Requirements

4.5.3.1 Product security incidents determined to have controlled risk do not have to be reported per adverse event or corrections and removal procedures. However, they shall be remediated by routine updates and patches and/or device enhancements.

4.5.3.2 Product security incidents determined to have uncontrolled risk shall be reported per adverse event or corrections and removal procedures.

4.5.4 Response and Communication: Timely responses and communications must be provided to all stakeholders impacted by vulnerabilities and incidents for commercialized products as described below.

4.5.4.1 Internal: [insert company name] Product Security Officer and PPM must notify the Product Security Governance Committee of Medium to Critical Risks within three (3) days of initial discovery once it was determine to be a product security incident and provide an update every seven (7) days thereafter until closure.

4.5.4.2 Customers and Third-Parties: Targeted customer bulletins or notifications must be made available and posted to the public [insert company name] Product Security webpage or other available delivery mechanisms to customers within 30 days of initial discovery. Updates to related Product Security White Papers shall be evaluated and updated if required. Customers and third-parties reporting vulnerabilities and incidents shall be provided status updates in a routine cadence established by the cross-functional task force while complaint handling investigation is in progress.

4.6 Peripheral Factors Impacting Product Security

4.6.1 [insert company name] Assets and Systems: [insert company name] assets and/or infrastructure used to support R&D, Supply Chain, Manufacturing, Service and any other functions to produce and procure [insert company name] products and services must adhere to [insert company name] Information Security Policy and Standards. These may include personal computers and networks used during any stage of the products lifecycle.

4.6.2 [insert company name] Service and Support

4.6.2.1 Service Access: Remote and Local access of customer systems and products by [insert company name] Associates must maintain permissible security and privacy controls. Service and support shall ensure system security controls are always returned to intended use prior to completing any service visit. Service and support users must be uniquely identified upon authentication and authorization to a system, meaning shared or hardcoded credentials will require Exemptions documented in the Product Security Management Plan. Customers should also consider limiting access to [insert company name] products whenever possible.

4.6.2.2 Service Documentation: Product information used in documentations such as Service Manuals, shall not include any credentials which may allow other unauthorized access to the product. Default passwords or credentials may be documented when instructions are provided to make those credentials unique.

4.6.2.3 Customer Data Handling: Customer data may never leave the site without clear communication of use of data, such as troubleshooting, and approval from the customer.

4.6.2.4 Removable Media: Any use of removal storage devices shall be approved and adhere to existing [insert company name] Information Security Policy or Standards for potential harm before utilization with a [insert company name] product at any time. This includes during development, manufacturing and/or service and support.

4.6.2.5 Decommissioning: Products and components transferred or decommissioned from a customer facility, or removed for refurbishment must have any Sensitive Information and Data destroyed or transferred with reasonable and appropriate safeguards with the customer's written authorization.

4.6.2.5.1 Customer Destruction: Customers may accept responsibility to destroy Sensitive Information and Data from any [insert company name] product if they so wish to do so. The transfers of this data shall be clearly documented and follow any federal and local regulatory or legal procedures.

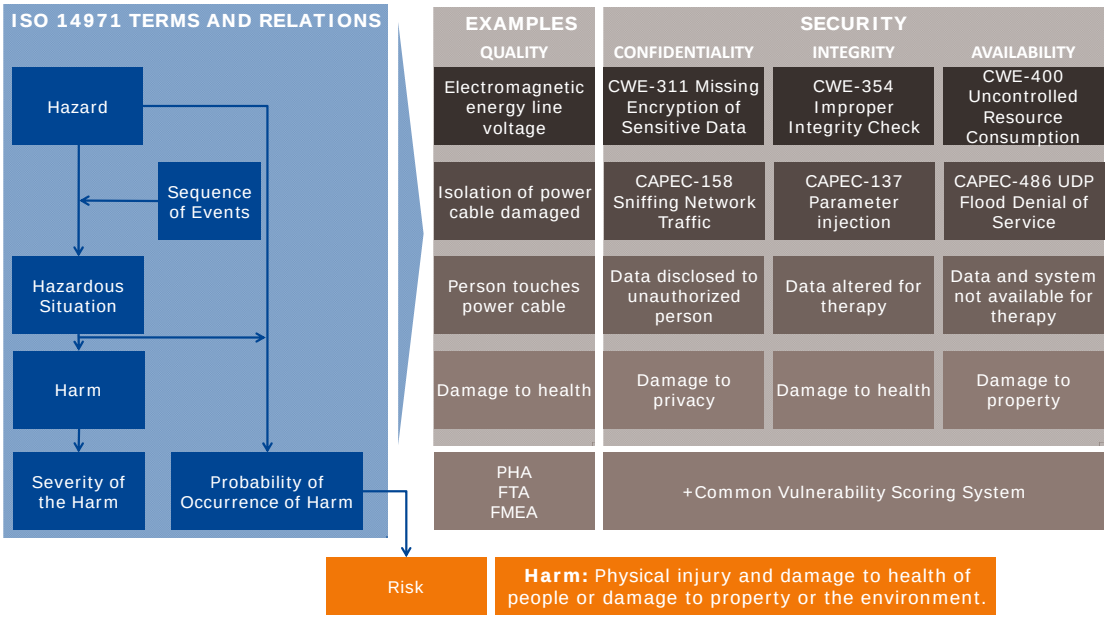
4.6.2.5.2 Field Destruction: Service organizations shall work with PS to determine approved manners in which to manage Sensitive Information and Data. The destruction of this data shall be clearly documented and follow any local regulatory or legal procedures.

4.6.3 [insert company name] IT: Infrastructure required by the business functions to develop, manufacture and support [insert company name] products must adhere to [insert company name] Information Security Policy and Standards.

4.6.4 Third-Party Entity Assets and Systems: Quality must assess and consult with GIS and or Supplier Management on a third-party entity adherence to [insert company name] Information Security Policy and Standards.

5.0 Appendix

5.1 Product Security Risk in comparison to ISO 14971


ISO 14971 TERMS AND RELATIONS
Hazard
Sequence of Events
Hazardous Situation
Harm
Severity of the Harm
Probability of Occurrence of Harm
EXAMPLES
QUALITY
SECURITY
CONFIDENTIALITY
INTEGRITY
AVAILABILITY
Electromagnetic energy line voltage
CWE-311 Missing Encryption of Sensitive Data
CWE-354 Improper Integrity Check
CWE-400 Uncontrolled Resource Consumption
Isolation of power cable damaged
CAPEC-158 Sniffing Network Traffic
CAPEC-137 Parameter injection
CAPEC-486 UDP Flood Denial of Service
Person touches power cable
Data disclosed to unauthorized person
Data altered for therapy
Data and system not available for therapy
Damage to health
Damage to privacy
Damage to health
Damage to property
PHA
FTA
FMEA
+Common Vulnerability Scoring System
Risk
Harm: Physical injury and damage to health of people or damage to property or the environment.