2024 Medical Device Cybersecurity Benchmarking Assessment

The benchmarking survey as well as the annual benchmarking report are offered as a collaborative effort between The Medical Device Innovation Consortium (MDIC), Apraciti and HSCC. The findings from the benchmarking assessment will help MDIC to create resources to measure maturity over time and enable industry growth through continuous product security enhancements.

The survey encompasses a number questions each drawn from the Medical Device and Health IT Joint Security Plan's (JSP) maturity assessment framework, along with basic demographic questions and should take approximately 15-30 minutes to complete (you can save your progress at any time to resume later). Previous or current use of the JSP is not a requirement for participation. Please answer each question to the best of your ability and revert to other colleagues for additional data, where relevant. You are strongly encouraged to refer to the JSP before answering each question. Specific line numbers of the JSP corresponding to each question have been added to help guide you.

We recommend a Senior-Level Product Security Officer, Risk Manager or Quality Manager complete this survey based on strong working knowledge of the organization's product portfolio and relative security posture. We also encourage connecting with colleagues across the organization's lines of business, where relevant, to ensure responses are as comprehensive and accurate as possible. Only one survey per company or organization is meant to be completed and submitted; duplicates will be discarded.

Please note:

- This survey does not provide a certification or attestation and should not be considered a substitute for completing a comprehensive security maturity assessment or for conducting a third-party security audit.
- Respondents may publicly disclose survey results for marketing purposes but by participating in this survey, each respondent acknowledges and agrees that (1) it will be clearly stated that these survey scores are based on a subjective self-assessment that yielded results which have not been certified by an objective third-party each and every time the respondent publicly discloses the survey scores in any and all media or discloses the scores to a third party, and (2) it will not indicate or imply that the Medical Device Innovation Consortium has certified or attested to the survey results.
- For your convenience, all survey questions are available as a PDF. This document may be freely shared with other members of your organization to assist with the survey process.
- All identifiable information provided by survey respondents will be kept confidential, withheld from any regulatory or governing bodies and not shared outside of MDIC.
- Only non-identifiable, anonymous summaries of the overall findings will be made public as part of the overarching benchmark study.
- Names of organizations participating in this survey will not be included in any public reports or summaries.
- Questions?
    - On the initiative - cybersecurity@mdic.org or info@apraciti.com
    - On the platform - info@productsecurityhub.com

ORGANIZATION > GOVERNANCE

Is an accountable leader with required resources, such as a Chief Product Security Officer (CPSO), designated as responsible for the Product Security Program?
[JSP, Section VII Organizational Governance to Support JSP Implementation, Page 12]
Select the answer that best applies.

- ☐ Nothing is in place
- ☐ Staffing or designating an individual is being discussed and socialized within the organization
- ☐ Organizational plans, including resources and structure are funded and approved but not yet finalized
- ☐ The CPSO role (or equivalent) has been staffed or designated
- ☐ The roles & responsibilities of the CPSO are documented in organization Policy and reporting lines have been updated and the CPSO reports directly or indirectly to the head of R&D
- ☐ Product Security performance is directly linked to organization leadership success goals.

Have capable and qualified individuals responsible for carrying out product security activities been identified with clear roles & responsibilities?
[JSP, Section VII Organizational Governance to Support JSP Implementation, Page 12]
Select the answer that best applies.

- ☐ Nothing is in place
- ☐ Staffing Product Security is being brainstormed
- ☐ Roles & responsibilities and job descriptions are fully drafted and approved
- ☐ Product Security roles have been staffed or designated
- ☐ Individuals responsible for Product Security have received appropriate training
- ☐ Effectiveness of individuals responsible for Product Security is managed during performance reviews

ORGANIZATION > PRODUCT SECURITY FRAMEWORK

Is a formal Product Security Program in place (e.g. structure, framework, product inventory, processes, metrics, etc.)?
[JSP, Section IX JSP Product Security Framework Implementation, Page 12-13]
Select the answer that best applies.

- ☐ No formal or documented program is in place
- ☐ Processes are being discussed and socialized throughout the organization
- ☐ Plans for the program are fully drafted and approved
- ☐ The program elements have been rolled out and implemented throughout the organization
- ☐ Metrics on the program are routinely reviewed to evaluate performance
- ☐ Performance improvement plans have been developed to optimize the program

Are Pre-Market Product Security Processes developed and fully integrated with Quality Management Systems (QMS)?
[JSP, Section IX JSP Product Security Framework Implementation, Page 12-13]
Select the answer that best applies.

- ☐ No process or standard is in place
- ☐ Processes are being discussed and socialized throughout the organization
- ☐ Processes aligned with regulatory guidance and/or an industry framework are fully drafted
- ☐ Processes are fully integrated with the QMS and required to be adhered to
- ☐ Metrics associated with the Processes are routinely reviewed to evaluate performance
- ☐ Performance improvement plans have been developed to optimize the Processes

Are Post Market Product Security Processes developed and fully integrated with Quality Management Systems (QMS) (e.g. threat/signal monitoring, triage risk assessment, CERT/ISAO/regulatory notification requirements, etc.)?
[JSP, Section IX JSP Product Security Framework Implementation, Page 12-13]
Select the answer that best applies.

- ☐ No process or standard is in place
- ☐ Processes are being discussed and socialized throughout the organization
- ☐ Processes aligned with regulatory guidance and/or an industry framework are fully drafted
- ☐ Processes are fully integrated with the QMS and required to be adhered to
- ☐ Metrics associated with the Processes are routinely reviewed to evaluate performance
- ☐ Performance improvement plans have been developed to optimize the Processes

CONCEPT > SECURITY MANAGEMENT PLANNING

Does the organization include cybersecurity considerations as part of product conceptualization and planning such that Product Security activities and deliverables are appropriately accounted for in project scope, schedule, and costs?
[JSP, Section IX, Section A.3. Security Management Planning, page 18-20]
Select the answer that best applies for each of the three categories, Frequency, Standards and Metrics, Audit & Input.

FREQUENCY

How often is this activity completed for products?

- ☐ Not done for any products
- ☐ Done for some products
- ☐ Done for all products

STANDARDS

Are formalized processes or standards followed?

- ☐ No process or standard is followed
- ☐ Different processes or standards are followed and/or output is inconsistent
- ☐ The same formalized process or standard is followed for all products with consistent output

METRICS, AUDIT & INPUT

Are metrics tracked, audits performed and performance improvement plans documented for this activity?

- ☐ Metrics are not developed and audits are not performed
- ☐ Metrics are developed and regularly reviewed
- ☐ Audits are regularly conducted to ensure activity is being executed to standard, outcomes from the audits are documented, and performance improvement plans are developed (as necessary)

Are cybersecurity risks, known vulnerabilities, and software anomalies identified throughout design and development (including testing) properly evaluated and managed (e.g., tracked in R&D defect tracking systems, design history or risk management files)?
[JSP, Section IX, Section A.3 Security Management Planning, Page 18-20]
Select the answer that best applies for each of the three categories, Frequency, Standards and Metrics, Audit & Input.

FREQUENCY

How often is this activity completed for products?

- Not done for any products
- Done for some products
- Done for all products

STANDARDS

Are formalized processes or standards followed?

- No process or standard is followed
- Different processes or standards are followed and/or output is inconsistent
- The same formalized process or standard is followed for all products with consistent output

METRICS, AUDIT & INPUT

Are metrics tracked, audits performed and performance improvement plans documented for this activity?

- Metrics are not developed and audits are not performed
- Metrics are developed and regularly reviewed
- Audits are regularly conducted to ensure activity is being executed to standard, outcomes from the audits are documented, and performance improvement plans are developed (as necessary)

Are cybersecurity plans implemented to manage cybersecurity activities throughout the product's lifecycle?
[JSP, Section IX. Section A.3. Security Management Planning, page 18-20]
Select the answer that best applies.

- No process or standard is in place
- Processes are being discussed and socialized throughout the organization
- Processes aligned with regulatory guidance and/or an industry framework are fully drafted
- Processes are fully integrated with the QMS and required to be adhered to
- Metrics associated with the processes are routinely reviewed to evaluate performance
- Performance improvement plans have been developed to optimize the processes

Does the organization or product maintain a coordinated vulnerability disclosure policy that is publicly shared?

[JSP, Section IX. Section A.3. Security Management Planning, page 18-20]

Select the answer that best applies for each of the three categories, Frequency, Standards and Metrics, Audit & Input.

FREQUENCY

How often is this activity completed for products?

- Not done for any products
- Done for some products
- Done for all products

STANDARDS

Are formalized processes or standards followed?

- No process or standard is followed
- Different processes or standards are followed and/or output is inconsistent
- The same formalized process or standard is followed for all products

METRICS, AUDIT & INPUT

Are metrics tracked, audits performed and performance improvement plans documented for this activity?

- Metrics are not developed and audits are not performed
- Metrics are developed and regularly reviewed
- Audits are regularly conducted to ensure activity is being executed to standard, outcomes from the audits are documented, and performance improvement plans are developed (as necessary)

RISK MANAGEMENT > RISK MANAGEMENT

Does the cybersecurity risk assessment process require the evaluation of exploitability as opposed to likelihood or probability for risk evaluation?
[JSP, Section IX, Section B. Risk Management, Page 20-22]
Select the answer that best applies for each of the three categories, Frequency, Standards and Metrics, Audit & Input.

FREQUENCY

How often is this activity completed for products?

- ☐ Not done for any products
- ☐ Done for some products
- ☐ Done for all products

STANDARDS

Are formalized processes or standards followed?

- ☐ No process or standard is followed
- ☐ Different processes or standards are followed and/or output is inconsistent
- ☐ The same formalized process or standard is followed for all products

METRICS, AUDIT & INPUT

Are metrics tracked, audits performed and performance improvement plans documented for this activity?

- ☐ Metrics are not developed and audits are not performed
- ☐ Metrics are developed and regularly reviewed
- ☐ Audits are regularly conducted to ensure activity is being executed to standard, outcomes from the audits are documented, and performance improvement plans are developed (as necessary)

Has Cybersecurity Risk acceptability criteria been defined for cybersecurity risks?
[JSP, Section IX, Section B.1. Security Design Risk Assessment, Page 23]
Select the answer that best applies.

- ☐ No process or standard is in place
- ☐ Processes are being discussed and socialized throughout the organization
- ☐ Processes aligned with regulatory guidance and/or an industry framework are fully drafted
- ☐ Processes are fully integrated with the QMS and required to be adhered to
- ☐ Metrics associated with the processes are routinely reviewed to evaluate performance
- ☐ Performance improvement plans have been developed to optimize the processes

RISK MANAGEMENT > RISK ASSESSMENT

Is a process defined to perform cybersecurity risk assessments, for both pre-market and released products, fully integrated with the Quality Management System (QMS)?
[JSP, Section IX, Section B.1. Security Design Risk Assessment, Page 14-25]
Select the answer that best applies for each of the three categories, Frequency, Standards and Metrics, Audit & Input.

FREQUENCY

How often is this activity completed for products?

- ☐ Not done for any products
- ☐ Done for some products
- ☐ Done for all products

STANDARDS

Are formalized processes or standards followed?

- ☐ No process or standard is followed
- ☐ Different processes or standards are followed and/or output is inconsistent
- ☐ The same formalized process or standard is followed for all products

METRICS, AUDIT & INPUT

Are metrics tracked, audits performed and performance improvement plans documented for this activity?

- ☐ Metrics are not developed and audits are not performed
- ☐ Metrics are developed and regularly reviewed
- ☐ Audits are regularly conducted to ensure activity is being executed to standard, outcomes from the audits are documented, and performance improvement plans are developed (as necessary)

RISK MANAGEMENT > SECURITY INTEGRATION INTO SAFETY RISK ASSESSMENT

Does the cybersecurity risk management process(es) include when security risk must be included in the safety risk assessment?
[JSP, Section IX, Section B.2. Security Integration into Safety Risk Assessment, Page 25-27]
Select the answer that best applies.

- ☐ No process or standard is in place
- ☐ Processes are being discussed and socialized throughout the organization
- ☐ Processes are fully drafted, and define when security risk must be included in the safety risk assessment
- ☐ Processes are fully integrated with the QMS and required to be adhered to defining when security risk must be included in the safety risk assessment
- ☐ Metrics associated with the Processes are routinely reviewed to evaluate performance
- ☐ Performance improvement plans have been developed to optimize the Processes

Is a process in place to determine if cybersecurity risks and vulnerabilities impacting patient harm are controlled or uncontrolled?
[JSP, Section IX, Section B.2. Security Integration into Safety Risk Assessment, Page 25-27]
Select the answer that best applies.

- ☐ No process or standard is in place
- ☐ Processes are being discussed and socialized throughout the organization
- ☐ Processes are drafted and define when vulnerabilities should be treated as controlled or uncontrolled risk
- ☐ Processes are fully integrated with the QMS and required to be adhered to and define when vulnerabilities should be treated as controlled or uncontrolled risk
- ☐ Metrics associated with the Processes are routinely reviewed to evaluate performance
- ☐ Performance improvement plans have been developed to optimize the Processes

RISK MANAGEMENT > SECURITY RISK MANAGEMENT SUMMARY AND APPROVAL

Are residual security risks and known, unresolved vulnerabilities (e.g., not remediated) summarized in a formal report, such as a Security Risk Management Summary Report?
[JSP, Section IX, Section B.3. Security Risk Management Summary and Approval, Page 27]
Select the answer that best applies for each of the three categories, Frequency, Standards and Metrics, Audit & Input.

FREQUENCY

How often is this activity completed for products?

- ☐ Not done for any products
- ☐ Done for some products
- ☐ Done for all products

STANDARDS

Are formalized processes or standards followed?

- ☐ No process or standard is followed
- ☐ Different processes or standards are followed and/or output is inconsistent
- ☐ The same formalized process or standard is followed for all products

METRICS, AUDIT & INPUT

Are metrics tracked, audits performed and performance improvement plans documented for this activity?

- ☐ Metrics are not developed and audits are not performed
- ☐ Metrics are developed and regularly reviewed
- ☐ Audits are regularly conducted to ensure activity is being executed to standard, outcomes from the audits are documented, and performance improvement plans are developed (as necessary)

SUPPLIER MANAGEMENT > SUPPLIER MANAGEMENT

Is a formal Cybersecurity Supply Chain Program in place, covering manufacturing, distribution environments?
[JSP, Section IX, Section C. Supplier Management, Page 28]
Select the answer that best applies.

- ☐ No process or standard is in place
- ☐ Processes are being discussed and socialized throughout the organization
- ☐ Plans for the program are fully drafted
- ☐ The program elements have been rolled out and implemented throughout the organization
- ☐ Metrics associated with the processes are routinely reviewed to evaluate performance
- ☐ Performance improvement plans have been developed to optimize the program

Has the organization implemented Cybersecurity Supply Chain processes?
[JSP, Section IX, Section C. Supplier Management, Page 28]
Select the answer that best applies.

- ☐ No process or standard is in place
- ☐ Processes are being discussed and socialized throughout the organization
- ☐ Processes aligned with regulatory guidance and/or an industry framework are fully drafted
- ☐ Processes are fully integrated with the QMS and required to be adhered to
- ☐ Metrics associated with the processes are routinely reviewed to evaluate performance
- ☐ Performance improvement plans have been developed to optimize the processes

Have necessary cybersecurity controls been established to manage risks within the supply chain environment?
[JSP, Section IX, Section C. Supplier Management, Page 31]
Select the answer that best applies for each of the three categories, Frequency, Standards and Metrics, Audit & Input.

FREQUENCY

How often is this activity completed for products?

- ☐ Not done for any products
- ☐ Done for some products
- ☐ Done for all products

STANDARDS

Are formalized processes or standards followed?

- ☐ No process or standard is followed
- ☐ Different processes or standards are followed and output is inconsistent
- ☐ The same formalized process or standard is followed for all products with consistent output

METRICS, AUDIT & INPUT

Are metrics tracked, audits performed and performance improvement plans documented for this activity?

- ☐ Metrics are not developed and audits are not performed
- ☐ Metrics are developed and regularly reviewed
- ☐ Audits are regularly conducted to ensure activity is being executed to standard, outcomes from the audits are documented, and performance improvement plans are developed (as necessary)

Are cybersecurity risks identified in the organization's Supply Chain Environment managed in alignment with the organization's risk management process?
[JSP, Section IX, Section C.2 Performance Management, Page 30-31]
Select the answer that best applies for each of the three categories, Frequency, Standards and Metrics, Audit & Input.

FREQUENCY

How often is this activity completed for products?

- Not done for any products
- Done for some products
- Done for all products

STANDARDS

Are formalized processes or standards followed?

- No process or standard is followed
- Different processes or standards are followed and output is inconsistent
- The same formalized process or standard is followed for all products with consistent output

METRICS, AUDIT & INPUT

Are metrics tracked, audits performed and performance improvement plans documented for this activity?

- Metrics are not developed and audits are not performed
- Metrics are developed and regularly reviewed
- Audits are regularly conducted to ensure activity is being executed to standard, outcomes from the audits are documented, and performance improvement plans are developed (as necessary)

Have Supply Chain Cybersecurity Processes been fully integrated with Quality Management Systems (QMS)?
[JSP, Section IX. Section C. Supplier Management, page 29]
Select the answer that best applies.

- No process or standard is in place
- Processes are being discussed and socialized throughout the organization
- Processes aligned with regulatory guidance and/or an industry framework are fully drafted
- Processes are fully integrated with the QMS and required to be adhered to
- Metrics associated with the processes are routinely reviewed to evaluate performance
- Performance improvement plans have been developed to optimize the processes

SUPPLIER MANAGEMENT > PURCHASING PROCESS

Does the organization maintain a supplier cybersecurity risk management program including which type of suppliers require an assessment and the frequency of assessment?
[JSP, Section IX. Section C.1 Purchasing Process, page 28-30]
Select the answer that best applies.

- ☐ No process or standard is in place
- ☐ Processes are being discussed and socialized throughout the organization
- ☐ Processes aligned with regulatory guidance and/or an industry framework are fully drafted
- ☐ Processes are fully integrated with the QMS and required to be adhered to
- ☐ Metrics associated with the processes are routinely reviewed to evaluate performance
- ☐ Performance improvement plans have been developed to optimize the processes

Have cybersecurity requirements been incorporated into supplier contractual agreements?
[JSP, Section IX. Section C.1. Purchasing Process, page 28-30]
Select the answer that best applies.

- ☐ There are no cybersecurity requirements in contract templates or supplier contracts
- ☐ Contractual requirements being discussed and socialized throughout the organization
- ☐ Contractual requirements, aligned with the supplier cybersecurity risk management process are fully drafted
- ☐ Contractual requirements are integrated in all contract templates
- ☐ Metrics associated with the requirements are routinely reviewed to evaluate performance
- ☐ Performance improvement plans have been developed to optimize the requirements

SUPPLIER MANAGEMENT > PERFORMANCE MANAGEMENT

Has the organization implemented Cybersecurity Supply Chain incident management processes?
[JSP, Section IX. Section C.2. Performance Management, Page 30-31]
Select the answer that best applies.

- No process or standard is in place
- Processes are being discussed and socialized throughout the organization
- Processes aligned with regulatory guidance and/or an industry framework are fully drafted
- Processes are fully integrated with the QMS and required to be adhered to
- Metrics associated with the processes are routinely reviewed to evaluate performance
- Performance improvement plans have been developed to optimize the processes

Is the performance of suppliers monitored including vulnerability monitoring, existence of and updates to a SBOM, and incident monitoring?
[JSP, Section IX. Section C.2. Performance Management, Page 30-31]
Select the answer that best applies for each of the three categories, Frequency, Standards and Metrics, Audit & Input.

FREQUENCY

How often is this activity completed for products?

- Not done for any products
- Done for some products
- Done for all products

STANDARDS

Are formalized processes or standards followed?

- No process or standard is followed
- Different processes or standards are followed and/or output is inconsistent
- The same formalized process or standard is followed for all products

METRICS, AUDIT & INPUT

Are metrics tracked, audits performed and performance improvement plans documented for this activity?

- Metrics are not developed and audits are not performed
- Metrics are developed and regularly reviewed
- Audits are regularly conducted to ensure activity is being executed to standard, outcomes from the audits are documented, and performance improvement plans are developed (as necessary)

DESIGN & DEVELOPMENT > SECURITY REQUIREMENTS DEVELOPMENT

Does the organization maintain information security policies that apply to any systems or software that are used in the development environment?
[JSP, Section IX, Section D.1 Security Requirements Development, Page 32-33]
Select the answer that best applies.

- No process or standard is in place
- Processes are being discussed and socialized throughout the organization
- Processes aligned with regulatory guidance and/or an industry framework are fully drafted
- Processes are referenced in the QMS and required to be adhered to
- Metrics associated with the processes are routinely reviewed to evaluate performance
- Performance improvement plans have been developed to optimize the processes

Have third party tools, including cloud tools, used in device development been documented and assessed for cybersecurity?
[JSP, Section IX, Section D.1 Security Requirements Development, Page 32-33]
Select the answer that best applies for each of the three categories, Frequency, Standards and Metrics, Audit & Input.

FREQUENCY

How often is this activity completed for products?

- Not done for any products
- Done for some products
- Done for all products

STANDARDS

Are formalized processes or standards followed?

- No process or standard is followed
- Different processes or standards are followed and output is inconsistent
- The same formalized process or standard is followed for all products with consistent output

METRICS, AUDIT & INPUT

Are metrics tracked, audits performed and performance improvement plans documented for this activity?

- Metrics are not developed and audits are not performed
- Metrics are developed and regularly reviewed
- Audits are regularly conducted to ensure activity is being executed to standard, outcomes from the audits are documented, and performance improvement plans are developed (as necessary)

Have cybersecurity requirements been established, following an industry recognized standard or guidance?
[JSP, Section IX, Section D.1 Security Requirements Development, Page 32-33]
Select the answer that best applies for each of the three categories, Frequency, Standards and Metrics, Audit & Input.

FREQUENCY

How often is this activity completed for products?

- Not done for any products
- Done for some products
- Done for all products

STANDARDS

Are formalized processes or standards followed?

- No process or standard is followed
- Different processes or standards are followed and output is inconsistent
- The same formalized process or standard is followed for all products with consistent output

METRICS, AUDIT & INPUT

Are metrics tracked, audits performed and performance improvement plans documented for this activity?

- Metrics are not developed and audits are not performed
- Metrics are developed and regularly reviewed
- Audits are regularly conducted to ensure activity is being executed to standard, outcomes from the audits are documented, and performance improvement plans are developed (as necessary)

Do cybersecurity requirements include secure-by-design principles, legal and regulatory security requirements, customer security requirements, requirements based on recognized security standards, and the organization's own security requirements?
[JSP, Section IX, Section D.1 Security Requirements Development, Page 32-33]
Select the answer that best applies for each of the three categories, Frequency, Standards and Metrics, Audit & Input.

FREQUENCY

How often is this activity completed for products?

- Not done for any products
- Done for some products
- Done for all products

STANDARDS

Are formalized processes or standards followed?

- No process or standard is followed
- Different processes or standards are followed and output is inconsistent
- The same formalized process or standard is followed for all products with consistent output

METRICS, AUDIT & INPUT

Are metrics tracked, audits performed and performance improvement plans documented for this activity?

- Metrics are not developed and audits are not performed
- Metrics are developed and regularly reviewed
- Audits are regularly conducted to ensure activity is being executed to standard, outcomes from the audits are documented, and performance improvement plans are developed (as necessary)

DESIGN & DEVELOPMENT > SECURE ARCHITECTURE AND DESIGN

Are accurate and comprehensive architecture views and data flow diagrams formally documented, including definition of the device, all hardware and software components, trust boundaries, security-relevant system elements, internal/external interfaces and how interactions occur (e.g. ports/protocols) ?

[JSP, Section IX. Section D.2. Secure Architecture and Design, Page 34]

Select the answer that best applies for each of the three categories, Frequency, Standards and Metrics, Audit & Input.

FREQUENCY

How often is this activity completed for products?

- ☐ Not done for any products
- ☐ Done for some products
- ☐ Done for all products

STANDARDS

Are formalized processes or standards followed?

- ☐ No process or standard is followed
- ☐ Different processes or standards are followed and/or output is inconsistent
- ☐ The same formalized process or standard is followed for all products with consistent output

METRICS, AUDIT & INPUT

Are metrics tracked, audits performed and performance improvement plans documented for this activity?

- ☐ Metrics are not developed and audits are not performed
- ☐ Metrics are developed and regularly reviewed
- ☐ Audits are regularly conducted to ensure activity is being executed to standard, outcomes from the audits are documented, and performance improvement plans are developed (as necessary)

Has threat modeling been performed, in alignment with an industry recognized threat modeling method and include all system elements (i.e. device, interactions, users, manufacturing, supply chain, development, deployment, interoperation with other devices, maintenance/update activities and decommissioning etc.)?

[JSP, Section IX. Section D.2. Secure Architecture and Design, Page 34]

Select the answer that best applies for each of the three categories, Frequency, Standards and Metrics, Audit & Input.

FREQUENCY

How often is this activity completed for products?

- Not done for any products
- Done for some products
- Done for all products

STANDARDS

Are formalized processes or standards followed?

- No process or standard is followed
- Different processes or standards are followed and/or output is inconsistent
- The same formalized process or standard is followed for all products with consistent output

METRICS, AUDIT & INPUT

Are metrics tracked, audits performed and performance improvement plans documented for this activity?

- Metrics are not developed and audits are not performed
- Metrics are developed and regularly reviewed
- Audits are regularly conducted to ensure activity is being executed to standard, outcomes from the audits are documented, and performance improvement plans are developed (as necessary)

DESIGN & DEVELOPMENT > CODE DEVELOPMENT AND TESTING

Has cybersecurity testing been defined and executed, based on a product's design and intended use environment (e.g., SAST, SCA, Vulnerability Scanning, etc.)?
[JSP, Section IX. Section D.3.Code Development and Testing, page 35-38]
Select the answer that best applies for each of the three categories, Frequency, Standards and Metrics, Audit & Input.

FREQUENCY

How often is this activity completed for products?

- ☐ Not done for any products
- ☐ Done for some products
- ☐ Done for all products

STANDARDS

Are formalized processes or standards followed?

- ☐ No process or standard is followed
- ☐ Different processes or standards are followed and/or output is inconsistent
- ☐ The same formalized process or standard is followed for all products with consistent output

METRICS, AUDIT & INPUT

Are metrics tracked, audits performed and performance improvement plans documented for this activity?

- ☐ Metrics are not developed and audits are not performed
- ☐ Metrics are developed and regularly reviewed
- ☐ Audits are regularly conducted to ensure activity is being executed to standard, outcomes from the audits are documented, and performance improvement plans are developed (as necessary)

Is Iterative Code Testing, such as code analysis and Static Analysis Security Testing (SAST), incorporated into code development?
[JSP, Section IX. Section D.3.Code Development and Testing, page 36-37]
Select the answer that best applies for each of the three categories, Frequency, Standards and Metrics, Audit & Input.

FREQUENCY

How often is this activity completed for products?

- ☐ Not done for any products
- ☐ Done for some products
- ☐ Done for all products

STANDARDS

Are formalized processes or standards followed?

- ☐ No process or standard is followed
- ☐ Different processes or standards are followed and/or output is inconsistent
- ☐ The same formalized process or standard is followed for all products

METRICS, AUDIT & INPUT

Are metrics tracked, audits performed and performance improvement plans documented for this activity?

- ☐ Metrics are not developed and audits are not performed
- ☐ Metrics are developed and regularly reviewed
- ☐ Audits are regularly conducted to ensure activity is being executed to standard, outcomes from the audits are documented, and performance improvement plans are developed (as necessary)

Is Iterative Integration Testing, such as vulnerability scanning and Dynamic Application Security Testing (DAST), incorporated into code development?

[JSP, Section IX. Section D.3.Code Development and Testing, page 37-38]

Select the answer that best applies for each of the three categories, Frequency, Standards and Metrics, Audit & Input.

FREQUENCY

How often is this activity completed for products?

- Not done for any products
- Done for some products
- Done for all products

STANDARDS

Are formalized processes or standards followed?

- No process or standard is followed
- Different processes or standards are followed and/or output is inconsistent
- The same formalized process or standard is followed for all products

METRICS, AUDIT & INPUT

Are metrics tracked, audits performed and performance improvement plans documented for this activity?

- Metrics are not developed and audits are not performed
- Metrics are developed and regularly reviewed
- Audits are regularly conducted to ensure activity is being executed to standard, outcomes from the audits are documented, and performance improvement plans are developed (as necessary)

DESIGN & DEVELOPMENT > PATCH/SOFTWARE UPDATE PLANNING

Are routine update and patch management plans established in support of product launch covering both product software and third-party components?
[JSP, Section IX, Section D.4. Patch/Software Update Planning, Page 38-47]
Select the answer that best applies for each of the three categories, Frequency, Standards and Metrics, Audit & Input.

FREQUENCY

How often is this activity completed for products?

- ☐ Not done for any products
- ☐ Done for some products
- ☐ Done for all products

STANDARDS

Are formalized processes or standards followed?

- ☐ No process or standard is followed
- ☐ Different processes or standards are followed and output is inconsistent
- ☐ The same formalized process or standard is followed for all products with consistent output

METRICS, AUDIT & INPUT

Are metrics tracked, audits performed and performance improvement plans documented for this activity?

- ☐ Metrics are not developed and audits are not performed
- ☐ Metrics are developed and regularly reviewed
- ☐ Audits are regularly conducted to ensure activity is being executed to standard, outcomes from the audits are documented, and performance improvement plans are developed (as necessary)

Do patch management plans differentiate between planned update cycles and updates to address emergencies and critical cybersecurity risks?
[JSP, Section IX, Section D.4. Patch/Software Update Planning, Page 38-47]
Select the answer that best applies.

- ☐ No process or standard is in place
- ☐ Processes are being discussed and socialized throughout the organization
- ☐ Processes aligned with regulatory guidance and/or an industry framework are fully drafted
- ☐ Processes are fully integrated with the QMS and required to be adhered to
- ☐ Metrics associated with the processes are routinely reviewed to evaluate performance
- ☐ Performance improvement plans have been developed to optimize the processes

Do products have anticipated end of life and/or end of support dates established with consideration to supporting third-party products and components?
[JSP, Section IX, Section D.4. Patch/Software Update Planning, Page 44-45]
Select the answer that best applies for each of the three categories, Frequency, Standards and Metrics, Audit & Input.

FREQUENCY

How often is this activity completed for products?

- Not done for any products
- Done for some products
- Done for all products

STANDARDS

Are formalized processes or standards followed?

- No process or standard is followed
- Different processes or standards are followed and/or output is inconsistent
- The same formalized process or standard is followed for all products with consistent output

METRICS, AUDIT & INPUT

Are metrics tracked, audits performed and performance improvement plans documented for this activity?

- Metrics are not developed and audits are not performed
- Metrics are developed and regularly reviewed
- Audits are regularly conducted to ensure activity is being executed to standard, outcomes from the audits are documented, and performance improvement plans are developed (as necessary)

DESIGN & DEVELOPMENT > SECURE TRANSFER TO MANUFACTURING PLANNING

Is a process defined to ensure the design transfer to manufacturing is repeatable and ensures the secure deployment of artifacts used to build the product?
[JSP, Section IX, Section D.5. Secure Transfer to Manufacturing Planning, Page 47-49]
Select the answer that best applies for each of the three categories, Frequency, Standards and Metrics, Audit & Input.

FREQUENCY

How often is this activity completed for products?

- ☐ Not done for any products
- ☐ Done for some products
- ☐ Done for all products

STANDARDS

Are formalized processes or standards followed?

- ☐ No process or standard is followed
- ☐ Different processes or standards are followed and/or output is inconsistent
- ☐ The same formalized process or standard is followed for all products

METRICS, AUDIT & INPUT

Are metrics tracked, audits performed and performance improvement plans documented for this activity?

- ☐ Metrics are not developed and audits are not performed
- ☐ Metrics are developed and regularly reviewed
- ☐ Audits are regularly conducted to ensure activity is being executed to standard, outcomes from the audits are documented, and performance improvement plans are developed (as necessary)

Is a Software Bill of Materials produced, maintained, and made available to customers?
[JSP, Section IX, Section D.5. Secure Transfer to Manufacturing Planning, Page 47-49]
Select the answer that best applies for each of the three categories, Frequency, Standards and Metrics, Audit & Input.

FREQUENCY

How often is this activity completed for products?

- ☐ Not done for any products
- ☐ Done for some products
- ☐ Done for all products

STANDARDS

Are formalized processes or standards followed?

- ☐ No process or standard is followed
- ☐ Different processes or standards are followed and output is inconsistent
- ☐ The same formalized process or standard is followed for all products

METRICS, AUDIT & INPUT

Are metrics tracked, audits performed and performance improvement plans documented for this activity?

- ☐ Metrics are not developed and audits are not performed
- ☐ Metrics are developed and regularly reviewed
- ☐ Audits are regularly conducted to ensure activity is being executed to standard, outcomes from the audits are documented, and performance improvement plans are developed (as necessary)

DESIGN & DEVELOPMENT > CUSTOMER SECURITY DOCUMENTATION

Has labeling for product security been defined and documented in customer facing documentation (e.g., IFU, user guide, SBOM) in alignment with regulatory guidance and/or industry best practices?

[JSP, Section IX, Section D.5. Secure Transfer to Manufacturing Planning, Page 48-49]

Select the answer that best applies for each of the three categories, Frequency, Standards and Metrics, Audit & Input.

FREQUENCY

How often is this activity completed for products?

- ☐ Not done for any products
- ☐ Done for some products
- ☐ Done for all products

STANDARDS

Are formalized processes or standards followed?

- ☐ No process or standard is followed
- ☐ Different processes or standards are followed and output is inconsistent
- ☐ The same formalized process or standard is followed for all products with consistent output

METRICS, AUDIT & INPUT

Are metrics tracked, audits performed and performance improvement plans documented for this activity?

- ☐ Metrics are not developed and audits are not performed
- ☐ Metrics are developed and regularly reviewed
- ☐ Audits are regularly conducted to ensure activity is being executed to standard, outcomes from the audits are documented, and performance improvement plans are developed (as necessary)

Are device instructions and product specifications related to recommended cybersecurity controls appropriate for the intended use environment (e.g., antimalware software, use of a firewall, password requirements) included in device labeling?
[JSP, Section IX, Section D.5. Secure Transfer to Manufacturing Planning, Page 48-49]
Select the answer that best applies for each of the three categories, Frequency, Standards and Metrics, Audit & Input.

FREQUENCY

How often is this activity completed for products?

- Not done for any products
- Done for some products
- Done for all products

STANDARDS

Are formalized processes or standards followed?

- No process or standard is followed
- Different processes or standards are followed and/or output is inconsistent
- The same formalized process or standard is followed for all products

METRICS, AUDIT & INPUT

Are metrics tracked, audits performed and performance improvement plans documented for this activity?

- Metrics are not developed and audits are not performed
- Metrics are developed and regularly reviewed
- Audits are regularly conducted to ensure activity is being executed to standard, outcomes from the audits are documented, and performance improvement plans are developed (as necessary)

Are sufficiently detailed diagrams for users that allow recommended cybersecurity controls to be implemented included in device labeling?
[JSP, Section IX, Section D.5. Secure Transfer to Manufacturing Planning, Page 48-49]
Select the answer that best applies for each of the three categories, Frequency, Standards and Metrics, Audit & Input.

FREQUENCY

How often is this activity completed for products?

- Not done for any products
- Done for some products
- Done for all products

STANDARDS

Are formalized processes or standards followed?

- No process or standard is followed
- Different processes or standards are followed and/or output is inconsistent
- The same formalized process or standard is followed for all products

METRICS, AUDIT & INPUT

Are metrics tracked, audits performed and performance improvement plans documented for this activity?

- Metrics are not developed and audits are not performed
- Metrics are developed and regularly reviewed
- Audits are regularly conducted to ensure activity is being executed to standard, outcomes from the audits are documented, and performance improvement plans are developed (as necessary)

Does product labeling describe the methods for updating the product and validating the integrity and authenticity of software updates and security patches?
[JSP, Section IX, Section D.5. Secure Transfer to Manufacturing Planning, Page 48-49]
Select the answer that best applies for each of the three categories, Frequency, Standards and Metrics, Audit & Input.

FREQUENCY

How often is this activity completed for products?

- ☐ Not done for any products
- ☐ Done for some products
- ☐ Done for all products

STANDARDS

Are formalized processes or standards followed?

- ☐ No process or standard is followed
- ☐ Different processes or standards are followed and output is inconsistent
- ☐ The same formalized process or standard is followed for all products

METRICS, AUDIT & INPUT

Are metrics tracked, audits performed and performance improvement plans documented for this activity?

- ☐ Metrics are not developed and audits are not performed
- ☐ Metrics are developed and regularly reviewed
- ☐ Audits are regularly conducted to ensure activity is being executed to standard, outcomes from the audits are documented, and performance improvement plans are developed (as necessary)

Is a list of network ports and other interfaces that are expected to receive and/or send data provided in customer documentation? This list should include a description of port functionality and indicate whether the ports are incoming, outgoing, or both, along with approved destination end-points.
[JSP, Section IX, Section D.5. Secure Transfer to Manufacturing Planning, Page 48-49]
Select the answer that best applies for each of the three categories, Frequency, Standards and Metrics, Audit & Input.

FREQUENCY

How often is this activity completed for products?

- ☐ Not done for any products
- ☐ Done for some products
- ☐ Done for all products

STANDARDS

Are formalized processes or standards followed?

- ☐ No process or standard is followed
- ☐ Different processes or standards are followed and/or output is inconsistent
- ☐ The same formalized process or standard is followed for all products

METRICS, AUDIT & INPUT

Are metrics tracked, audits performed and performance improvement plans documented for this activity?

- ☐ Metrics are not developed and audits are not performed
- ☐ Metrics are developed and regularly reviewed
- ☐ Audits are regularly conducted to ensure activity is being executed to standard, outcomes from the audits are documented, and performance improvement plans are developed (as necessary)

Is a MDS2 form produced, maintained and included in product labeling?
[JSP, Section IX, Section D.5. Secure Transfer to Manufacturing Planning, Page 48-49]
Select the answer that best applies for each of the three categories, Frequency, Standards and Metrics, Audit & Input.

FREQUENCY

How often is this activity completed for products?

- Not done for any products
- Done for some products
- Done for all products

STANDARDS

Are formalized processes or standards followed?

- No process or standard is followed
- Different processes or standards are followed and output is inconsistent
- The same formalized process or standard is followed for all products

METRICS, AUDIT & INPUT

Are metrics tracked, audits performed and performance improvement plans documented for this activity?

- Metrics are not developed and audits are not performed
- Metrics are developed and regularly reviewed
- Audits are regularly conducted to ensure activity is being executed to standard, outcomes from the audits are documented, and performance improvement plans are developed (as necessary)

Is information on securely decommissioning devices by sanitizing the product of sensitive, confidential, and proprietary data and software included in device labeling?
[JSP, Section IX, Section D.5. Secure Transfer to Manufacturing Planning, Page 48-49]
Select the answer that best applies for each of the three categories, Frequency, Standards and Metrics, Audit & Input.

FREQUENCY

How often is this activity completed for products?

- Not done for any products
- Done for some products
- Done for all products

STANDARDS

Are formalized processes or standards followed?

- No process or standard is followed
- Different processes or standards are followed and/or output is inconsistent
- The same formalized process or standard is followed for all products

METRICS, AUDIT & INPUT

Are metrics tracked, audits performed and performance improvement plans documented for this activity?

- Metrics are not developed and audits are not performed
- Metrics are developed and regularly reviewed
- Audits are regularly conducted to ensure activity is being executed to standard, outcomes from the audits are documented, and performance improvement plans are developed (as necessary)

Is information, if known or anticipated, concerning device cybersecurity end of support and end of life included in device labeling?

[JSP, Section IX, Section D.5. Secure Transfer to Manufacturing Planning, Page 48-49]

Select the answer that best applies for each of the three categories, Frequency, Standards and Metrics, Audit & Input.

FREQUENCY

How often is this activity completed for products?

- Not done for any products
- Done for some products
- Done for all products

STANDARDS

Are formalized processes or standards followed?

- No process or standard is followed
- Different processes or standards are followed and/or output is inconsistent
- The same formalized process or standard is followed for all products

METRICS, AUDIT & INPUT

Are metrics tracked, audits performed and performance improvement plans documented for this activity?

- Metrics are not developed and audits are not performed
- Metrics are developed and regularly reviewed
- Audits are regularly conducted to ensure activity is being executed to standard, outcomes from the audits are documented, and performance improvement plans are developed (as necessary)

Does product labeling describe the methods to identify and report security events, incidents and suspected vulnerabilities?

[JSP, Section IX, Section D.5. Secure Transfer to Manufacturing Planning, Page 48-49]

Select the answer that best applies for each of the three categories, Frequency, Standards and Metrics, Audit & Input.

FREQUENCY

How often is this activity completed for products?

- Not done for any products
- Done for some products
- Done for all products

STANDARDS

Are formalized processes or standards followed?

- No process or standard is followed
- Different processes or standards are followed and output is inconsistent
- The same formalized process or standard is followed for all products

METRICS, AUDIT & INPUT

Are metrics tracked, audits performed and performance improvement plans documented for this activity?

- Metrics are not developed and audits are not performed
- Metrics are developed and regularly reviewed
- Audits are regularly conducted to ensure activity is being executed to standard, outcomes from the audits are documented, and performance improvement plans are developed (as necessary)

VERIFICATION & VALIDATION > VERIFY SECURITY CONTROLS

Has verification testing been executed, ensuring all planned cybersecurity requirements have been appropriately implemented and are effective?
[JSP, Section IX. Section E.1. Verify Security Controls, page 50]
Select the answer that best applies for each of the three categories, Frequency, Standards and Metrics, Audit & Input.

FREQUENCY

How often is this activity completed for products?

- ☐ Not done for any products
- ☐ Done for some products
- ☐ Done for all products

STANDARDS

Are formalized processes or standards followed?

- ☐ No process or standard is followed
- ☐ Different processes or standards are followed and/or output is inconsistent
- ☐ The same formalized process or standard is followed for all products with consistent output

METRICS, AUDIT & INPUT

Are metrics tracked, audits performed and performance improvement plans documented for this activity?

- ☐ Metrics are not developed and audits are not performed
- ☐ Metrics are developed and regularly reviewed
- ☐ Audits are regularly conducted to ensure activity is being executed to standard, outcomes from the audits are documented, and performance improvement plans are developed (as necessary)

VERIFICATION & VALIDATION > SECURITY VALIDATION TESTING

Has validation testing been executed, ensuring all implemented cybersecurity requirements are functioning as intended and without uncontrolled or unacceptable vulnerabilities (e.g., penetration testing, vulnerability scanning, fuzz testing, robustness testing, SBOM scanning, etc.)?

[JSP, Section IX. Section E.3.Security Validation Testing, page 51-54]

Select the answer that best applies for each of the three categories, Frequency, Standards and Metrics, Audit & Input.

FREQUENCY

How often is this activity completed for products?

- ☐ Not done for any products
- ☐ Done for some products
- ☐ Done for all products

STANDARDS

Are formalized processes or standards followed?

- ☐ No process or standard is followed
- ☐ Different processes or standards are followed and/or output is inconsistent
- ☐ The same formalized process or standard is followed for all products with consistent output

METRICS, AUDIT & INPUT

Are metrics tracked, audits performed and performance improvement plans documented for this activity?

- ☐ Metrics are not developed and audits are not performed
- ☐ Metrics are developed and regularly reviewed
- ☐ Audits are regularly conducted to ensure activity is being executed to standard, outcomes from the audits are documented, and performance improvement plans are developed (as necessary)

Are cybersecurity verification and validation test failures properly managed (e.g., failed requirements, patching failures, etc.)?

[JSP, Section IX. Section E.3.Security Validation Testing, page 51-54]

Select the answer that best applies for each of the three categories, Frequency, Standards and Metrics, Audit & Input.

FREQUENCY

How often is this activity completed for products?

- Not done for any products
- Done for some products
- Done for all products

STANDARDS

Are formalized processes or standards followed?

- No process or standard is followed
- Different processes or standards are followed and output is inconsistent
- The same formalized process or standard is followed for all products with consistent output

METRICS, AUDIT & INPUT

Are metrics tracked, audits performed and performance improvement plans documented for this activity?

- Metrics are not developed and audits are not performed
- Metrics are developed and regularly reviewed
- Audits are regularly conducted to ensure activity is being executed to standard, outcomes from the audits are documented, and performance improvement plans are developed (as necessary)

MAINTENANCE > SURVEILLANCE

Are Complaint Handling systems capturing and tracking cybersecurity risks and are they periodically monitored for potential vulnerabilities that may impact on-market products?
[JSP, Section IX. Section F.1. Surveillance, page 55]
Select the answer that best applies for each of the three categories, Frequency, Standards and Metrics, Audit & Input.

FREQUENCY

How often is this activity completed for products?

- ☐ Not done for any products
- ☐ Done for some products
- ☐ Done for all products

STANDARDS

Are formalized processes or standards followed?

- ☐ No process or standard is followed
- ☐ Different processes or standards are followed and output is inconsistent
- ☐ The same formalized process or standard is followed for all products with consistent output

METRICS, AUDIT & INPUT

Are metrics tracked, audits performed and performance improvement plans documented for this activity?

- ☐ Metrics are not developed and audits are not performed
- ☐ Metrics are developed and regularly reviewed
- ☐ Audits are regularly conducted to ensure activity is being executed to standard, outcomes from the audits are documented, and performance improvement plans are developed (as necessary)

Is a Product Security Impact Assessment performed on vulnerabilities that may potentially be applicable to an on-market product?
[JSP, Section IX. Section F.1. Surveillance, page 55]
Select the answer that best applies for each of the three categories, Frequency, Standards and Metrics, Audit & Input.

FREQUENCY

How often is this activity completed for products?

- ☐ Not done for any products
- ☐ Done for some products
- ☐ Done for all products

STANDARDS

Are formalized processes or standards followed?

- ☐ No process or standard is followed
- ☐ Different processes or standards are followed and output is inconsistent
- ☐ The same formalized process or standard is followed for all products with consistent output

METRICS, AUDIT & INPUT

Are metrics tracked, audits performed and performance improvement plans documented for this activity?

- ☐ Metrics are not developed and audits are not performed
- ☐ Metrics are developed and regularly reviewed
- ☐ Audits are regularly conducted to ensure activity is being executed to standard, outcomes from the audits are documented, and performance improvement plans are developed (as necessary)

MAINTENANCE > VULNERABILITY & EOL/EOS MANAGEMENT

Is a Cybersecurity Risk Assessment performed on all identified vulnerabilities potentially impacting an on-market product?
[JSP, Section IX. Section F.2 Vulnerability & EOL/EOS Management, page 55-57]
Select the answer that best applies for each of the three categories, Frequency, Standards and Metrics, Audit & Input.

FREQUENCY

How often is this activity completed for products?

- ☐ Not done for any products
- ☐ Done for some products
- ☐ Done for all products

STANDARDS

Are formalized processes or standards followed?

- ☐ No process or standard is followed
- ☐ Different processes or standards are followed and output is inconsistent
- ☐ The same formalized process or standard is followed for all products with consistent output

METRICS, AUDIT & INPUT

Are metrics tracked, audits performed and performance improvement plans documented for this activity?

- ☐ Metrics are not developed and audits are not performed
- ☐ Metrics are developed and regularly reviewed
- ☐ Audits are regularly conducted to ensure activity is being executed to standard, outcomes from the audits are documented, and performance improvement plans are developed (as necessary)

Are uncontrolled vulnerabilities required to be remediated to an acceptable level within 60 days of learning of the vulnerability, including the fix, validation of the fix, and distribution of the fix?
[JSP, Section IX. Section F.2 Vulnerability & EOL/EOS Management, page 55-57]
Select the answer that best applies for each of the three categories, Frequency, Standards and Metrics, Audit & Input.

FREQUENCY

How often is this activity completed for products?

- ☐ Not done for any products
- ☐ Done for some products
- ☐ Done for all products

STANDARDS

Are formalized processes or standards followed?

- ☐ No process or standard is followed
- ☐ Different processes or standards are followed and output is inconsistent
- ☐ The same formalized process or standard is followed for all products

METRICS, AUDIT & INPUT

Are metrics tracked, audits performed and performance improvement plans documented for this activity?

- ☐ Metrics are not developed and audits are not performed
- ☐ Metrics are developed and regularly reviewed
- ☐ Audits are regularly conducted to ensure activity is being executed to standard, outcomes from the audits are documented, and performance improvement plans are developed (as necessary)

Are uncontrolled vulnerabilities required to be reported to the FDA when the exception criteria is not met, specifically: 1) There are no known serious adverse events or deaths associated with the vulnerability 2) The manufacturer communicates with its customers and user community regarding the vulnerability within 30 days 3) The manufacturer identifies interim compensating controls, and develops a remediation plan to bring the residual risk to an acceptable level within 30 days 4) The manufacturer fixes the vulnerability within 60 days 5) The manufacturer actively participates as a member of an ISAO that shares vulnerabilities and threats that impact medical devices?

[JSP, Section IX. Section F.2 Vulnerability & EOL/EOS Management, page 55-57]

Select the answer that best applies for each of the three categories, Frequency, Standards and Metrics, Audit & Input.

FREQUENCY

How often is this activity completed for products?

- Not done for any products
- Done for some products
- Done for all products

STANDARDS

Are formalized processes or standards followed?

- No process or standard is followed
- Different processes or standards are followed and output is inconsistent
- The same formalized process or standard is followed for all products

METRICS, AUDIT & INPUT

Are metrics tracked, audits performed and performance improvement plans documented for this activity?

- Metrics are not developed and audits are not performed
- Metrics are developed and regularly reviewed
- Audits are regularly conducted to ensure activity is being executed to standard, outcomes from the audits are documented, and performance improvement plans are developed (as necessary)

Are uncontrolled vulnerabilities communicated to customers and ISAO community with the following metadata in 30 days or less: 1) Information on the vulnerability itself including an impact assessment 2) Interim compensating controls 3) Remediation plan to bring the risk down to an acceptable level 4) Timeline rationale for remediation plan?

[JSP, Section IX. Section F.2 Vulnerability & EOL/EOS Management, page 55-57]

Select the answer that best applies for each of the three categories, Frequency, Standards and Metrics, Audit & Input.

FREQUENCY

How often is this activity completed for products?

- Not done for any products
- Done for some products
- Done for all products

STANDARDS

Are formalized processes or standards followed?

- No process or standard is followed
- Different processes or standards are followed and output is inconsistent
- The same formalized process or standard is followed for all products

METRICS, AUDIT & INPUT

Are metrics tracked, audits performed and performance improvement plans documented for this activity?

- Metrics are not developed and audits are not performed
- Metrics are developed and regularly reviewed
- Audits are regularly conducted to ensure activity is being executed to standard, outcomes from the audits are documented, and performance improvement plans are developed (as necessary)

MAINTENANCE > SECURITY INCIDENT RESPONSE

Are product security incidents managed, and are plans periodically tested?
[JSP, Section IX. Section F.3. Security Incident Response, page 57]
Select the answer that best applies for each of the three categories, Frequency, Standards and Metrics, Audit & Input.

FREQUENCY

How often is this activity completed for products?

- ☐ Not done for any products
- ☐ Done for some products
- ☐ Done for all products

STANDARDS

Are formalized processes or standards followed?

- ☐ No process or standard is followed
- ☐ Different processes or standards are followed and output is inconsistent
- ☐ The same formalized process or standard is followed for all products with consistent output

METRICS, AUDIT & INPUT

Are metrics tracked, audits performed and performance improvement plans documented for this activity?

- ☐ Metrics are not developed and audits are not performed
- ☐ Metrics are developed and regularly reviewed
- ☐ Audits are regularly conducted to ensure activity is being executed to standard, outcomes from the audits are documented, and performance improvement plans are developed (as necessary)

MAINTENANCE > PATCH/SOFTWARE UPDATE DEPLOYMENT

Are Cybersecurity Routine Updates & Patches properly managed in alignment with regulatory guidance and/or industry best practices (e.g. US FDA requirements for controlled/uncontrolled risk)?

[JSP, Section IX. Section F.4. Patch/Software Update Deployment, page 57-59]

Select the answer that best applies for each of the three categories, Frequency, Standards and Metrics, Audit & Input.

FREQUENCY

How often is this activity completed for products?

- Not done for any products
- Done for some products
- Done for all products

STANDARDS

Are formalized processes or standards followed?

- No process or standard is followed
- Different processes or standards are followed and output is inconsistent
- The same formalized process or standard is followed for all products with consistent output

METRICS, AUDIT & INPUT

Are metrics tracked, audits performed and performance improvement plans documented for this activity?

- Metrics are not developed and audits are not performed
- Metrics are developed and regularly reviewed
- Audits are regularly conducted to ensure activity is being executed to standard, outcomes from the audits are documented, and performance improvement plans are developed (as necessary)

Are validated patches deployed using an established method?

[JSP, Section IX. Section F.4. Patch/Software Update Deployment, page 57-59]

Select the answer that best applies for each of the three categories, Frequency, Standards and Metrics, Audit & Input.

FREQUENCY

How often is this activity completed for products?

- Not done for any products
- Done for some products
- Done for all products

STANDARDS

Are formalized processes or standards followed?

- No process or standard is followed
- Different processes or standards are followed and output is inconsistent
- The same formalized process or standard is followed for all products with consistent output

METRICS, AUDIT & INPUT

Are metrics tracked, audits performed and performance improvement plans documented for this activity?

- Metrics are not developed and audits are not performed
- Metrics are developed and regularly reviewed
- Audits are regularly conducted to ensure activity is being executed to standard, outcomes from the audits are documented, and performance improvement plans are developed (as necessary)

Is Cybersecurity Routine Updates & Patch deployment tracked and monitored for implementation status?

[JSP, Section IX. Section F.4. Patch/Software Update Deployment, page 57-59]

Select the answer that best applies for each of the three categories, Frequency, Standards and Metrics, Audit & Input.

FREQUENCY

How often is this activity completed for products?

- ☐ Not done for any products
- ☐ Done for some products
- ☐ Done for all products

STANDARDS

Are formalized processes or standards followed?

- ☐ No process or standard is followed
- ☐ Different processes or standards are followed and output is inconsistent
- ☐ The same formalized process or standard is followed for all products with consistent output

METRICS, AUDIT & INPUT

Are metrics tracked, audits performed and performance improvement plans documented for this activity?

- ☐ Metrics are not developed and audits are not performed
- ☐ Metrics are developed and regularly reviewed
- ☐ Audits are regularly conducted to ensure activity is being executed to standard, outcomes from the audits are documented, and performance improvement plans are developed (as necessary)

MAINTENANCE > CUSTOMER SECURITY COMMUNICATION

Are external communication plans developed for responding to vulnerabilities and/or incidents in alignment with regulatory guidance and/or industry best practices (e.g. US FDA requirements for controlled/uncontrolled risk)?

[JSP, Section IX. Section F.5. Customer Security Communication, page 59-60]

Select the answer that best applies for each of the three categories, Frequency, Standards and Metrics, Audit & Input.

FREQUENCY

How often is this activity completed for products?

- ☐ Not done for any products
- ☐ Done for some products
- ☐ Done for all products

STANDARDS

Are formalized processes or standards followed?

- ☐ No process or standard is followed
- ☐ Different processes or standards are followed and/or output is inconsistent
- ☐ The same formalized process or standard is followed for all products with consistent output

METRICS, AUDIT & INPUT

Are metrics tracked, audits performed and performance improvement plans documented for this activity?

- ☐ Metrics are not developed and audits are not performed
- ☐ Metrics are developed and regularly reviewed
- ☐ Audits are regularly conducted to ensure activity is being executed to standard, outcomes from the audits are documented, and performance improvement plans are developed (as necessary)

Are customer-facing security bulletins, notifications, and status updates made available for customers to review for product security information (e.g., routine update and patch information, bulletins and advisories related to vulnerabilities or incidents)?

[JSP, Section IX. Section F.5. Customer Security Communication, page 59-60]

Select the answer that best applies for each of the three categories, Frequency, Standards and Metrics, Audit & Input.

FREQUENCY

How often is this activity completed for products?

- Not done for any products
- Done for some products
- Done for all products

STANDARDS

Are formalized processes or standards followed?

- No process or standard is followed
- Different processes or standards are followed and output is inconsistent
- The same formalized process or standard is followed for all products with consistent output

METRICS, AUDIT & INPUT

Are metrics tracked, audits performed and performance improvement plans documented for this activity?

- Metrics are not developed and audits are not performed
- Metrics are developed and regularly reviewed
- Audits are regularly conducted to ensure activity is being executed to standard, outcomes from the audits are documented, and performance improvement plans are developed (as necessary)