Medical Device Cybersecurity

Joint Security Plan (JSP) Quick Reference Guide: Who Does What, When, and Why

Medcrypt

Objective

The Joint Security Plan (JSP) was created by the Health Sector Coordinating Council (HSCC) as an industry-wide framework to align people, processes and evidence across the medical device product lifecycle. This JSP Quick reference Guide (QRG), developed by Medcrypt, is designed to help medical device manufacturers put the JSP into practice. It breaks down complex regulatory requirements into four phases - Concept, Design & Development, Verification & Validation, and Maintenance - so everyone, from engineers to executives, can understand their role in building and sustaining secure products.

Note on alignment

This JSP QRG reflects the JSP structure, while other Medcrypt resources (such as the Pen Test Assurance Matrix) align more closely with IEC 81001-5-1 activities. The two views are complementary: the JSP provides the high-level “what and why,” while the 81001-aligned materials provide the detailed “how and when.”

Here’s what you’ll take away

- A clear picture of how the Joint Security Plan (JSP) organizes security work across the product lifecycle.
- An easy way to explain the house analogy — Foundation (Concept), Framing (Design & Development), Inspection (V&V), and Maintenance (Postmarket).
- The roles of Builders, Explainers, and Owners in keeping the cybersecurity house in order.
- Key outputs and evidence needed at each phase to meet FDA expectations and build trust with clients.
- A quick reference you can share with your team to align security responsibilities across functions.

What is the Joint Security Plan (JSP)?

The JSP is the medical technology industry's secure product development framework (SPDF). It was created by the Healthcare and Public Health Sector Coordinating Council (HSCC) to help medical device manufacturers (MDMs) and healthcare IT suppliers embed cybersecurity across the total product lifecycle (TPLC).

It is a total product lifecycle reference for developing, deploying, and supporting cybersecure technology solutions in healthcare.

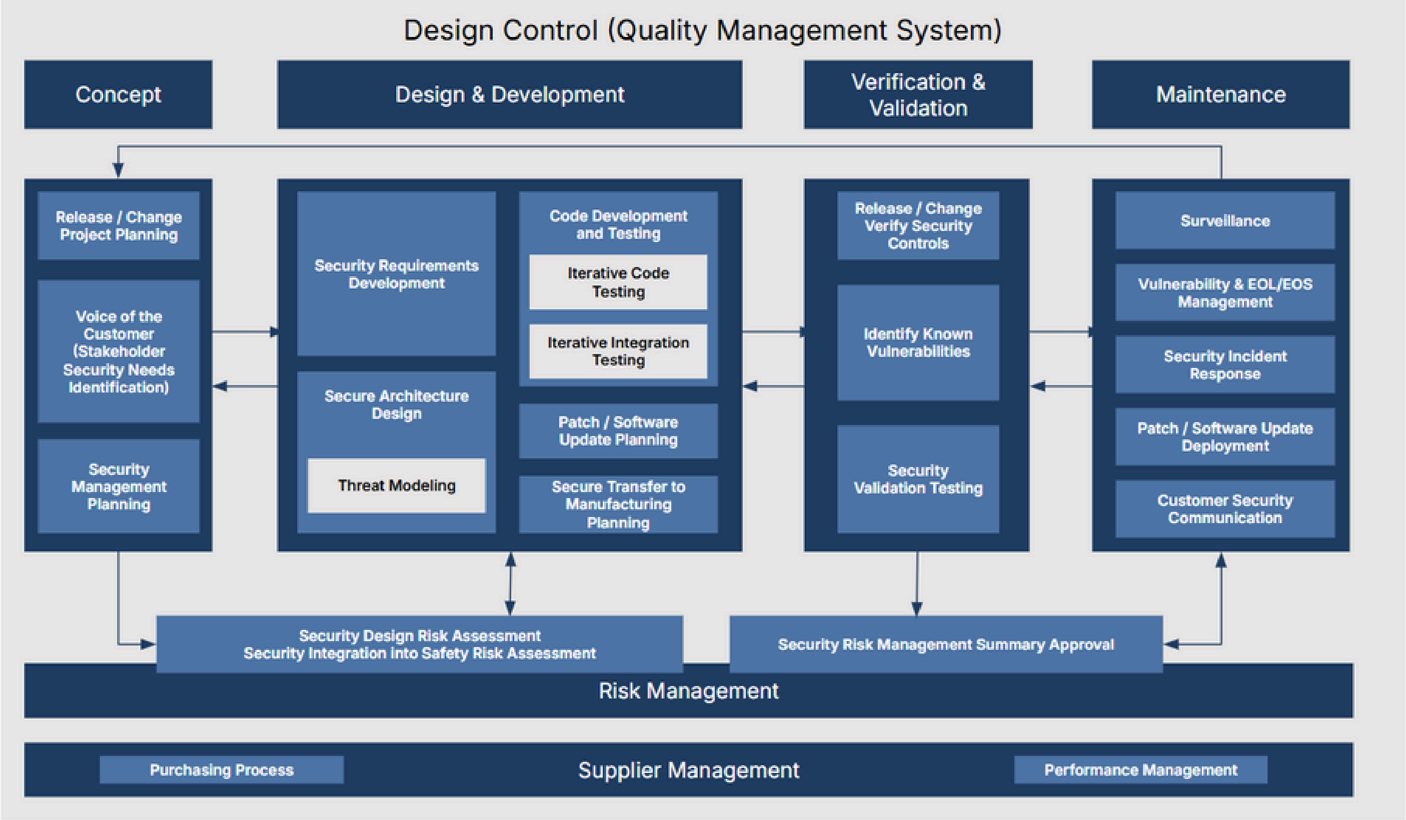
Design Control (Quality Management System)
Concept
Design & Development
Verification & Validation
Maintenance
Release / Change Project Planning
Voice of the Customer (Stakeholder Security Needs Identification)
Security Management Planning
Security Requirements Development
Secure Architecture Design
Threat Modeling
Code Development and Testing
Iterative Code Testing
Iterative Integration Testing
Patch / Software Update Planning
Secure Transfer to Manufacturing Planning
Release / Change Verify Security Controls
Identify Known Vulnerabilities
Security Validation Testing
Surveillance
Vulnerability & EOL/EOS Management
Security Incident Response
Patch / Software Update Deployment
Customer Security Communication
Security Design Risk Assessment
Security Integration into Safety Risk Assessment
Security Risk Management Summary Approval
Risk Management
Purchasing Process
Supplier Management
Performance Management

Figure 1: (Figure 1 from Health Sector Coordinating Council (HSCC) - Medical Device and Health IT Joint Security Plan Version 2.0)

The JSP as Your Cybersecurity House

Think of the JSP as the security process blueprint for your cybersecurity house:

- **Foundation** = Concept Phase (early decisions set stability for everything that follows)
- **Framing** = Design & Development (requirements and code turn into structure)
- **Inspection** = Verification & Validation (prove security works - FDA is the final inspector)
- **Maintenance** = Postmarket (monitor, communicate, patch to keep the house secure)

Each role contributes differently and palys a part in keeping the house standing strong:

- **Builders** = product managers, engineers, RA/QA
- **Explainers** = sales, marketing, service, even legal
- **Owners** = executives and incident response

The JSP as Your Cybersecurity House by Phase

Phase 1: Concept - Ask Early, Decide Early *(This is the foundation of your cybersecurity house.)*	
Focus	Lay the foundation.
Key Activities	Define security objectives, decide maintenance strategy, capture misuse cases, plan for security documentation (e.g., SBOM)
Who Does What	• **PMs:** Drive conversations, capture decisions, represent voice of the customer and maintenance strategy. • **Engineering:** Assess feasibility, define design constraints, tooling, and change control. • **Execs:** Approve strategy, allocate resources. • **Clinicians:** Flag usability/safety concerns.
Outputs	Security objectives doc, coding standards and training logs, maintenance plan, design constraints, and misuse case list.
Regulatory Context	This phase satisfies FDA and 524B design input expectations, AAMI SW 96 for risk management, and IEC 81001-5-1 secure development lifecycle.

Phase 2: Design & Development - Bake It In *(This is the framing stage - turning requirements into structure.)*	
Focus	Establish security requirements and develop code.
Key Activities	Document traceable security requirements, threat modeling, adopt secure coding standards, define crypto design, supply chain risk management (SBOM and scans).
Who Does What	• **Engineering:** Define requirements, threat modeling, code securely, and design crypto architecture. Develop traceable evidence through documentation. • **QA:** Verify requirements are testable. • **RA/QA:** Maintain evidence repository. • **PMs:** Keep requirements prioritized and visible. • **Execs:** Provide resources for tooling and training.
Outputs	Threat model, traceability matrix, crypto doc, supply chain risk management (SBOM reports), code review and early testing, and updated risk register.
Regulatory Context	Activities here support FDA and 524B secure design and coding requirements, IEC 81001-5-1 secure lifecycle standards, and ISO/IEC 27036 for supplier risk management.

The JSP as Your Cybersecurity House by Phase cont.

Phase 3: Verification & Validation – Prove It Works

(This is inspection time - FDA is the final inspector.)

Focus	Demonstrate secure design and document evidence of security controls effectiveness.
Key Activities	Execute test plans, run fuzz and other automated tests, conduct pen testing, triage vulnerabilities, and document residual risk.
Who Does What	• **QA:** Own test plan and execution. • **Test Team:** Deliver pen/fuzz results. • **Engineering:** Fix findings, update QMS. • **RA/QA:** Store evidence, log residual risk rationale. • **Executives:** Determine acceptability of residual risks. • **PMs:** Document and track closure of findings. • **Clinicians/Usability Experts:** Validate security doesn't disrupt workflows.
Outputs	Test reports, vulnerability triage report, and residual risk rationale.
Regulatory Context	These activities align with IEC 62304 for V&V, FDA premarket cybersecurity guidance.

Phase 4: Postmarket (Maintenance) – Launch Isn't the Finish Line

(This is ongoing maintenance - keeping the house secure after move-in.)

Focus	Keep devices secure after release, gather metrics and evidence, and vulnerability communication.
Key Activities	Postmarket surveillance: vulnerability intake and disclosure, patch/update processes, ongoing monitoring, and SBOM updates with EOL/EOS.
Who Does What	• **Product Security:** Manage disclosure and intake. • **Engineering/DevOps:** Assess new vulnerabilities, and build/verify patches. • **QA:** Validate and approve updates. • **RA/QA:** Archive evidence (reports and logs), and monitor compliance. • **Service/Field Teams:** Communicate updates to hospitals, and support rollout. • **Execs:** Ensure resource availability, budgets, and transparency.
Outputs	Evidence: patch/update logs, monitoring reports, surveillance logs, updated SBOMs with EOL/EOS status.
Regulatory Context	This phase satisfies FDA and 524B postmarket expectations, ISO/IEC 29147 and 30111 for vulnerability handling, and IEC 81001-5-1 maintenance requirements.

Conclusion

The JSP is more than a checklist - it's the security process blueprint that ensures your cybersecurity house stands strong. By breaking the lifecycle into four phases and clarifying who is responsible for what, you can create traceability for regulators, build confidence with customers, and ensure every team member knows their role in keeping your house in order.

This isn't just a checklist for security teams - it's a roadmap for the entire organization to build a security program that results in products that are not only innovative but also resilient against cyber threats.

Medcrypt

Medcrypt, Inc. is a San Diego-based cybersecurity provider for the healthcare industry, specializing in Software Bill of Materials (SBOM) and risk management solutions. By offering cutting-edge encryption, vulnerability analysis, and monitoring services, Medcrypt empowers medical device manufacturers to secure their products throughout the device lifecycle.

For more information: **website:** www.medcrypt.com **email:** info@medcrypt.com