Integrating Cybersecurity in the QMS

Leveraging a Cybersecurity Framework

CEO MedWare Cyber

Linkedin: *https://www.linkedin.com/in/joseph-silvia-mba-180a98/*

Website: *https://www.medwarecyber.com*

Security Must be Built In

- **Focus on a safety risk-based QMS**
  - ICH Q10: “When the term “risk” is used, the application of the term within the scope of this guideline pertains to safety or performance requirements of the pharmaceutical product or meeting applicable regulatory requirements.”
- **Cybersecurity Introduces a parallel requirement**
  - A secure QMS that protects systems and data
  - Security directly supports:
    - Data Integrity (ALCOA+)
    - Electronic records compliance (21 CFR/Annex 11)
    - System reliability and traceability

Pharmaceutical Cybersecurity Standards

- **Secure Product Development Framework**
  - NIST SP 800-82 Rev. 3
- **Cybersecurity Risk Management**
  - 21 CFR Part 11 / EU Annex 11
  - ISO 15189
  - GAMP 5 (2nd Ed.) & ICH Q10

Cybersecurity expectations are embedded across pharmaceutical regulations and must be integrated into the QMS, Validation, and data integrity controls.

NIST Cybersecurity Framework 2.0

Recover from the impacts of a cybersecurity event (Disaster Recovery, Report Correction

Establish the cybersecurity risk management strategy, expectations and policy; ongoing monitoring (QMS governance, Management Review)

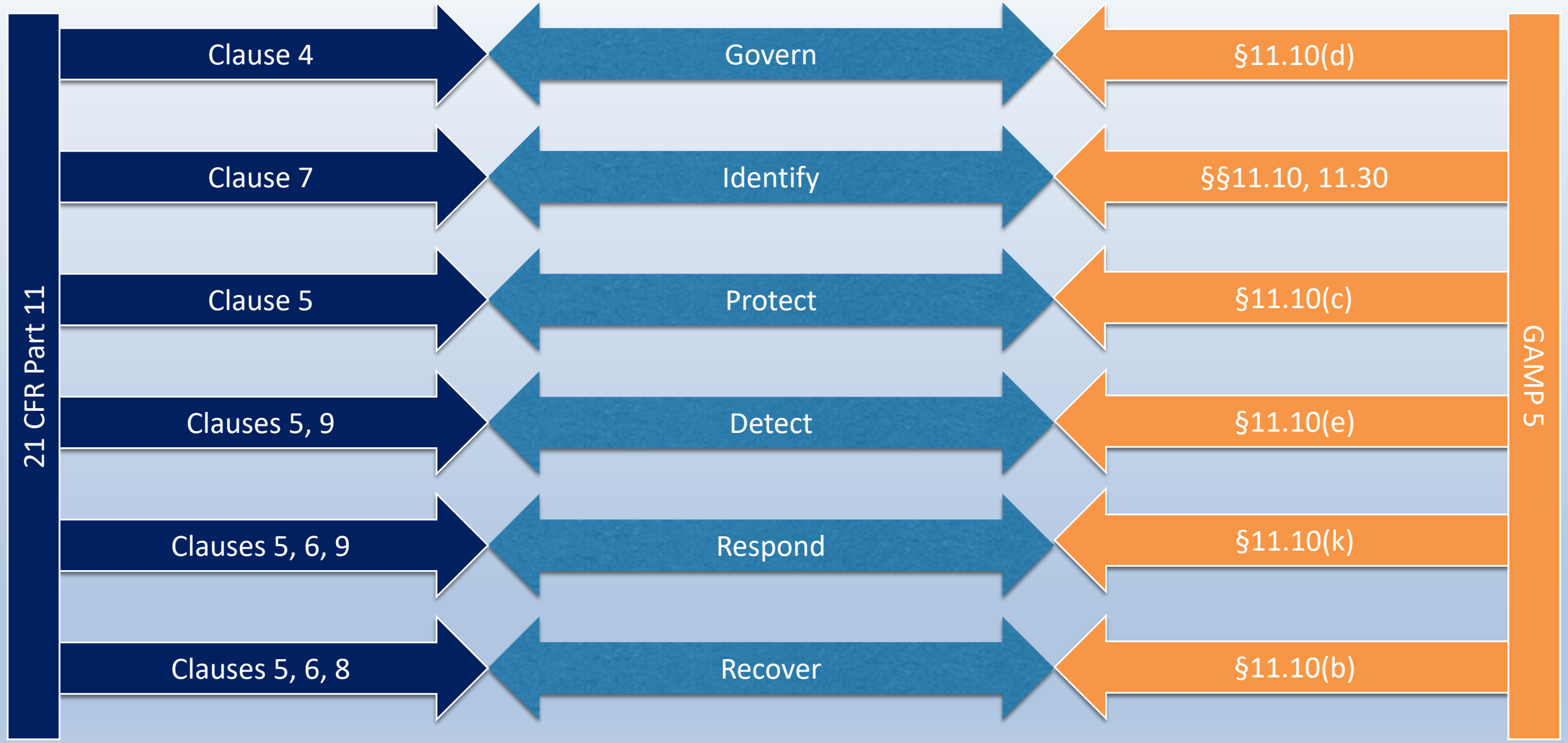
Determine cybersecurity risk throughout the product lifecycle (System Inventory, Risk Classification)

Prevent or reduce cybersecurity risk(Access Control, Encryption

Act on a detected cybersecurity event (Nonconformance/CAPA)

Detect a security event (Audit Trails, System Monitoring)

NIST CSF 2.0


21 CFR Part 11
Clause 4
Govern
§11.10(d)
Clause 7
Identify
§§11.10, 11.30
Clause 5
Protect
§11.10(c)
Clauses 5, 9
Detect
§11.10(e)
Clauses 5, 6, 9
Respond
§11.10(k)
Clauses 5, 6, 8
Recover
§11.10(b)
GAMP 5

Govern

- **Organizational context; policy; responsibilities:**
  - Quality policy and oversight
- **Oversight:**
  - Tracking & trending
  - Management review (QMR)
  - Periodic system review
- **Risk management strategy:**
  - Risk acceptance policies
- **Supply chain management:**
  - Supplier qualification and audit

Govern Example

Impact Severity	CVSS 4.0 Score			
	Low	Medium	High	Critical
Low	AC	AC	AC	NAC
Medium	AC	AC	NAC	NAC
High	AC	NAC	NAC	NAC

Risk Based on:

- Impact Severity
  - Patient Safety
  - Product Quality
  - Data Integrity
  - Align with GAMP5

In Pharma (Risk Impact):

- Data Integrity /Patient Results
- Vulnerabilities on GxP Systems

Pharma Impact

- Risks impacting data integrity or patient results are typically Not Acceptable
- Even moderate vulnerabilities may require action if they affect GxP systems
- All decisions must be:
  - Documented
  - Justified
  - Traceable to actions such as CAPA or mitigation

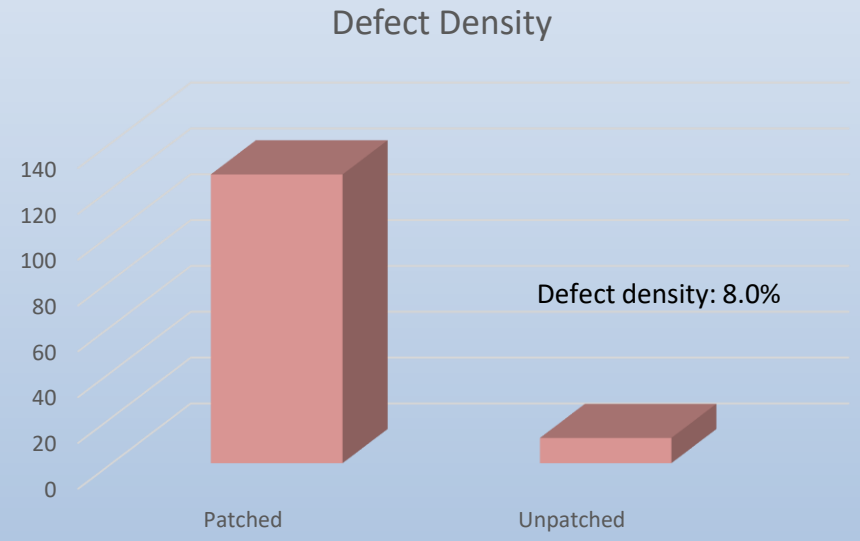
Identify

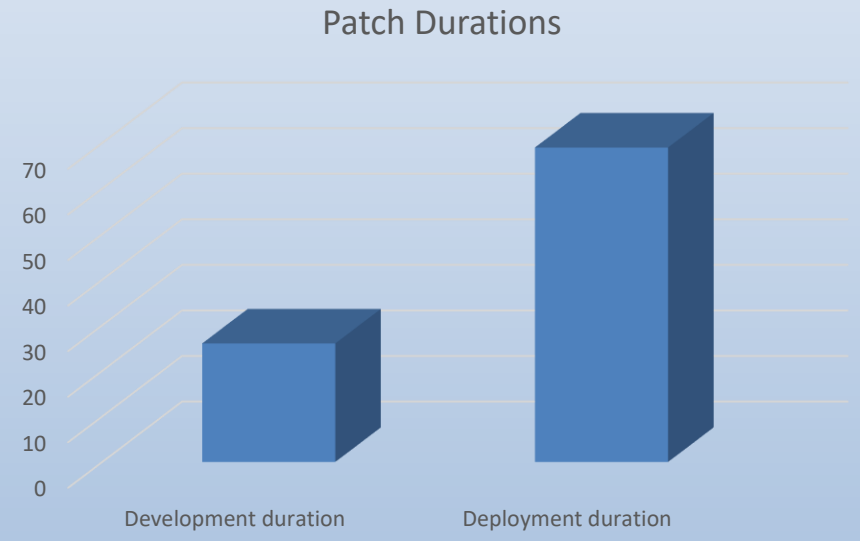
- **Function**
  - What systems exist
  - Their intended use
  - Their risk level
- **Pharma requirement**
  - Complete GxP system inventory/risk assessed
  - Classification
    - GxP
    - non-GxP
  - Identify
    - Interfaces
    - Data Flows

Forms the foundation for: Validation, Risk Assessment, Ongoing monitoring

Identify Example: Tracking & Trending

- **FDA security metrics:**





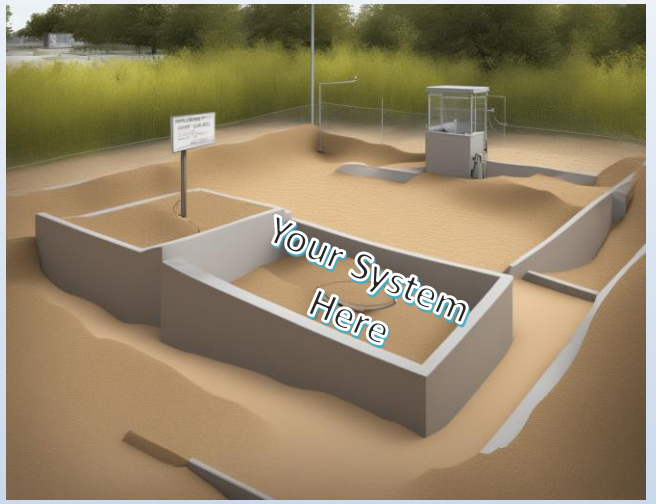
US FDA guidance: Cybersecurity in Pharmaceutical Operations: Quality System Considerations and Computerized System Controls, 2023

Protect

- **Identity management:**
  - Role-Based Access Controls
- **Controls must be:**
  - Defined in procedures
  - Validated or verified
  - Align with user roles & responsibilities
- **Awareness and training:**
  - Cybersecurity in training
  - Develop internal talent
- **Data security:**
  - At rest, in transit
- **Platform security:**
  - Manufacturing systems and platforms
- **Technology infrastructure resilience:**
  - IT infrastructure

Protect Example: Returned Equipment Handling

- **Protect your organization from infiltration**
  - Collect forensic evidence from returned samples and equipment in a sandboxed environment
- **Protect confidential information**
  - Sanitize returned equipment to avoid exposure of patient, batch, or user information



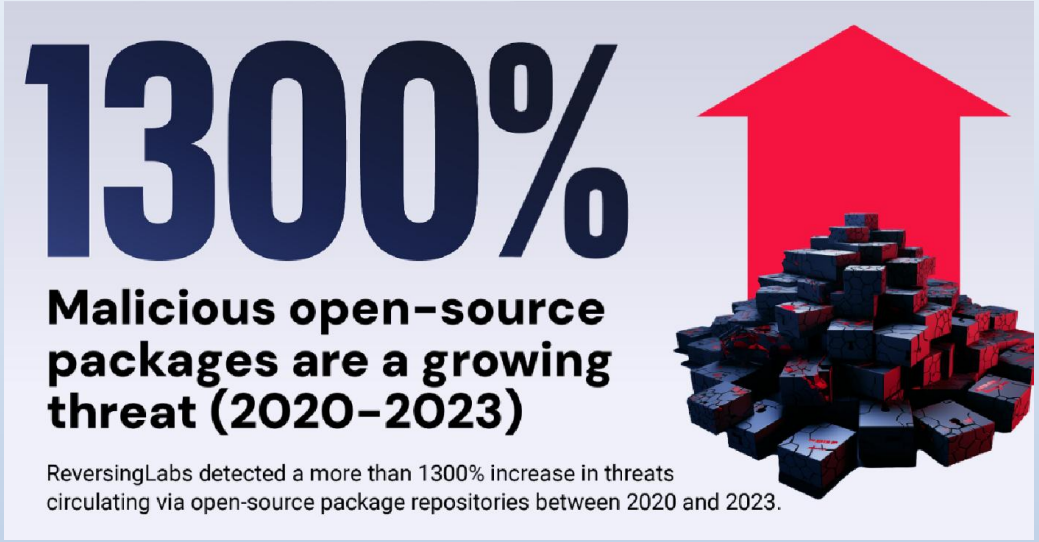
Detect

- **Continuous monitoring:**
  - Inspection and test
  - Asset monitoring
  - Event logging
  - Customer feedback
- **Event analysis:**
  - Nonconformances
  - Failure analysis
  - Tracking and trending
  - Complaint handling

Security events must be evaluated for GxP impact and documented as deviations/NCRs where applicable

Detect Example: Supply Chain Monitoring

https://www.reversinglabs.com/blog/the-state-of-software-supply-chain-security-2024-key-takeaways



https://www.wsj.com/articles/chip-shortage-has-spawned-a-surplus-of-fraudsters-and-fake-parts-11626255002

https://www.geckoandfly.com/22803/detect-fake-usb-flash-drives-sd-cards-ssd-disk/

https://openssf.org/blog/2024/04/15/open-source-security-openssf-and-openjs-foundations-issue-alert-for-social-engineering-takeovers-of-open-source-projects/

Supply Chain Risks

- **In pharma, this includes:**
  - Software suppliers
  - Cloud providers
  - Third-party integrations
- **Supplier Risk Management**
  - Supplier qualification
  - Ongoing monitoring
  - Integration into the QMS

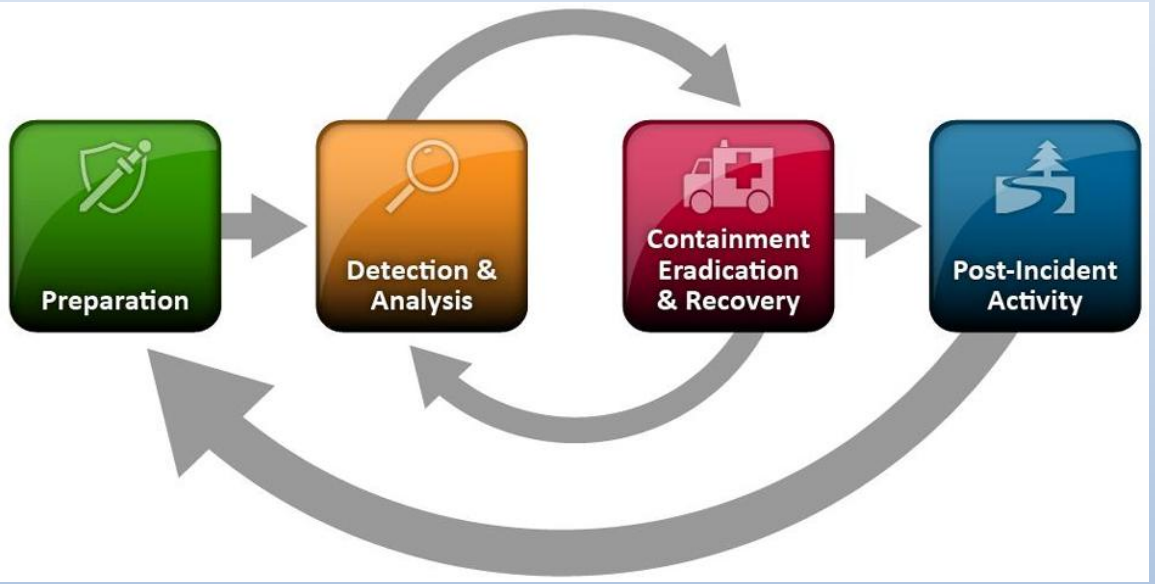
Respond

- **QMS Processes**
  - Deviation or NCR processes
  - Investigation and RCA
  - CAPA Implementation
- **Impact Assessments**
  - Patient Safety
  - Product Quality
  - Data Integrity

Respond Example: Incident Response Planning

- **Leverage QMS processes:**
  - risk management to determine applicability and impact
  - CAPA to formulate corrections and corrective actions
  - field notifications to customers, suppliers and regulators
  - Change control linkage
  - Validation impact assessment

NIST SP 800-61
ISO/IEC 27035-1
ISO/IEC 27035-2



Incident response must be structured, documented, traceable and cross-functional

Recover

- **Incident response reporting & communication:**
  - Notify affected customers
  - Review similar products
  - Issue patches/updates
  - Submit regulatory notifications if required (e.g., FDA, EMA)

- **In pharma:**
  - Systems must be restored to a validated state
  - Data must be verified for accuracy and completeness
  - Any impacted reports or records must be corrected
- **Recovery must ensure:**
  - Continued compliance
  - No impact to patient safety or product quality

Recover Example: Responding to Incidents

- **Incident recovery plan execution:**
  - CAPA to formulate preventive actions
  - Field action process to deploy the patch or update
  - Supplier management to fix any supply chain issues
  - Lessons learned to improve incident response
    - Risk Management
    - Process Improvements
    - Future prevention strategies

Summary: QMS-Cybersecurity Integration (Pharma)

- **Integrated Across Core Processes**
  - Risk Management
  - System Validation
  - Data Integrity
  - CAPA & Continuous Improvement
- **Organizations Must Demonstrate**
  - Documented & controlled processes
  - Validated and secure systems
  - End-to-end traceability
  - Cybersecurity is a Quality (QMS) & IT responsibility
- **Continuous monitoring & Risk Management**
  - Business & Patient Impact
  - Ensures product quality
  - Safeguards patient safety
  - Supports regulatory compliance