System Life Cycle Planning: NIST SP 800-160 V1 R1

Acquisition Process Priority

Strategy & Requirements

Establish acquisition strategy (AQ.1.1) and define system requirements (AQ.1.2).

Supplier Management

Identify potential suppliers (AQ.1.3) and develop solicitation package (AQ.1.4).

Selection & Monitoring

Evaluate proposals (AQ.2.1), select suppliers (AQ.2.2), and award contracts (AQ.2.3).

Supplier Performance & Relationship Management

Monitor supplier performance (AQ.3.1) and manage supplier relationships (AQ.3.2).

Organizational Project Processes

1. **Project Planning (OP.1)**
   Establishes foundation for project scope, objectives, and deliverables.
2. **Risk Management (OP.2)**
   Identifies and analyzes potential security and operational risks.
3. **Infrastructure Management (OP.3)**
   Ensures necessary tools and resources are in place.
4. **Quality Management (OP.4)**
   Maintains compliance with security and performance standards.

Project Management Foundation

Decision Management (OP.5)

Applies logical decision-making principles to each project part.

Configuration Management (OP.6)

Controls versions and changes throughout development.

Information Management (OP.7)

Ensures secure handling of information throughout the system lifecycle.

Maintenance & Evaluation: Risk & Incidents

Risk Monitoring (RM.1)

Continuous threat identification

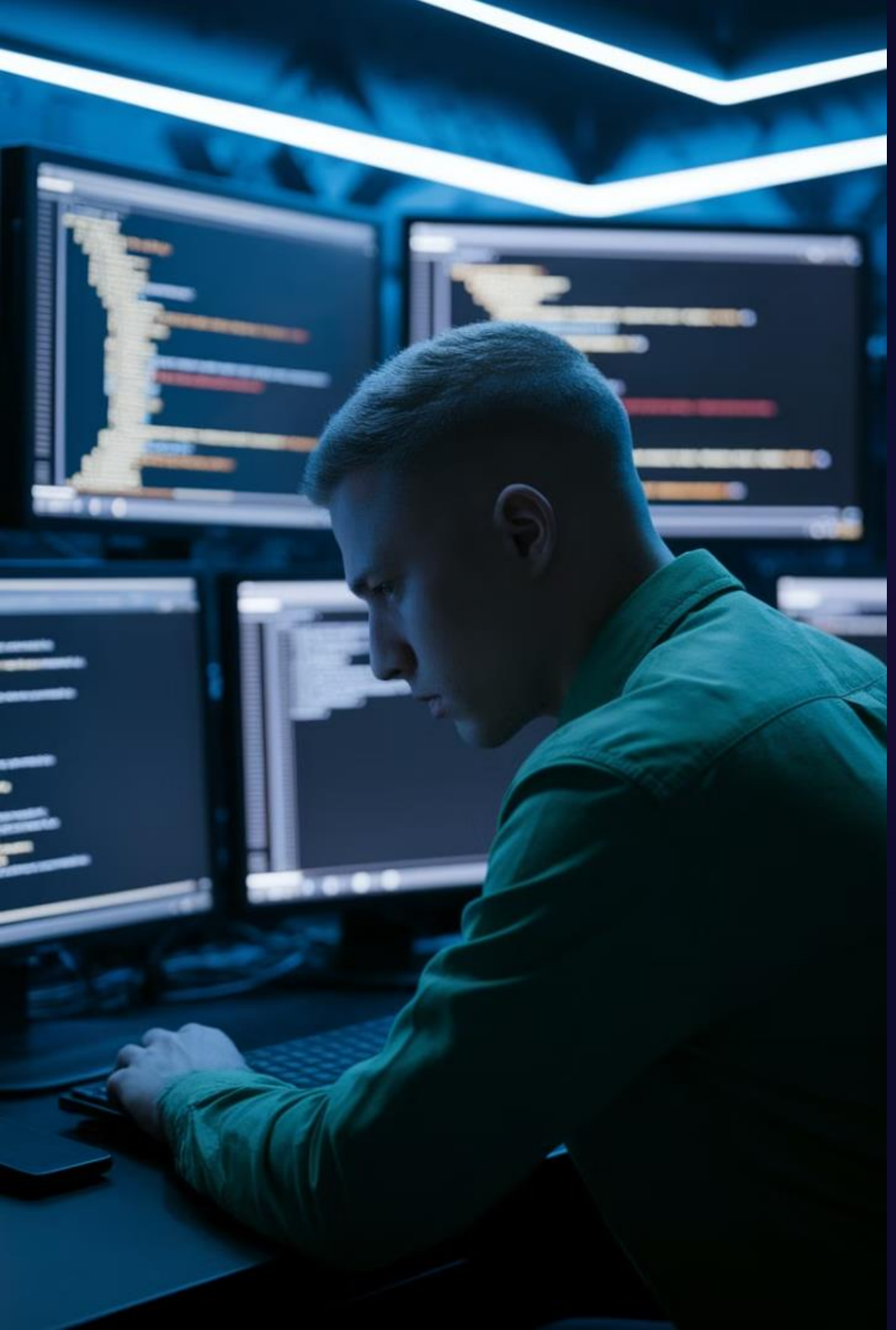
Incident Management (IM.1)

Swift response to breaches

Quality Assurance (QA.1)

Ongoing evaluation and improvement

This proactive approach keeps systems secure, minimizes downtime, and maintains high performance standards.



Technical Processes Priority

1

Verification (VE.1)

Confirm system security and functionality meet requirements.

2

Vulnerability Assessment (VA.2)

Identify and correct security weaknesses proactively.

3

Performance Optimization (OP.3)

Enhance efficiency while maintaining strong security measures.

4

Maintenance Actions (MA.4)

Implement updates and corrections for continuous improvement.

NIST 800-160 Framework Benefits

Security Integration

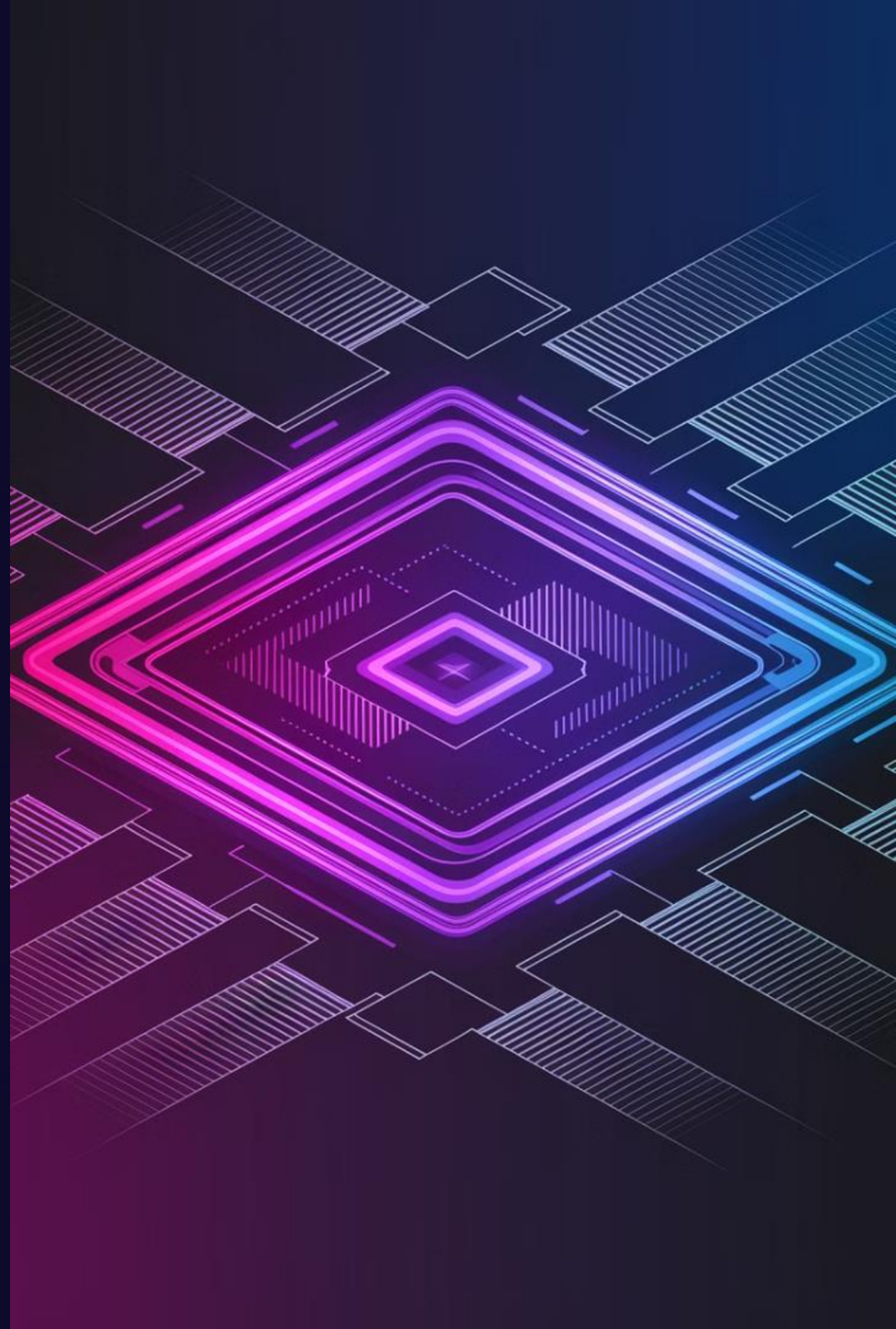
Embeds security from planning through maintenance, not as an afterthought.

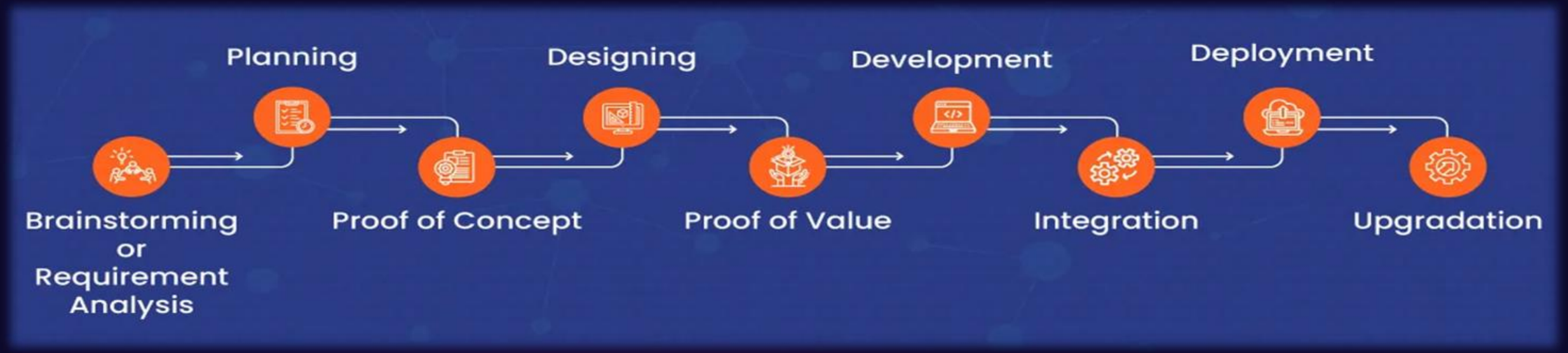
Regulatory Alignment

Supports industry regulations like PCI DSS for financial data handling.

Comprehensive Approach

Creates a security-focused culture throughout the entire development lifecycle.





9-Step SDLC Implementation

Early Risk Identification

Security issues are found and fixed early, not as emergency patches after release.

Continuous Monitoring

Ensures software remains strong against emerging threats.

Strategic Advantage

Improves operational efficiency and provides competitive edge in today's digital landscape.

Good Experiences | Challenges | What I learned

Thank You