FIRST.Org, Inc

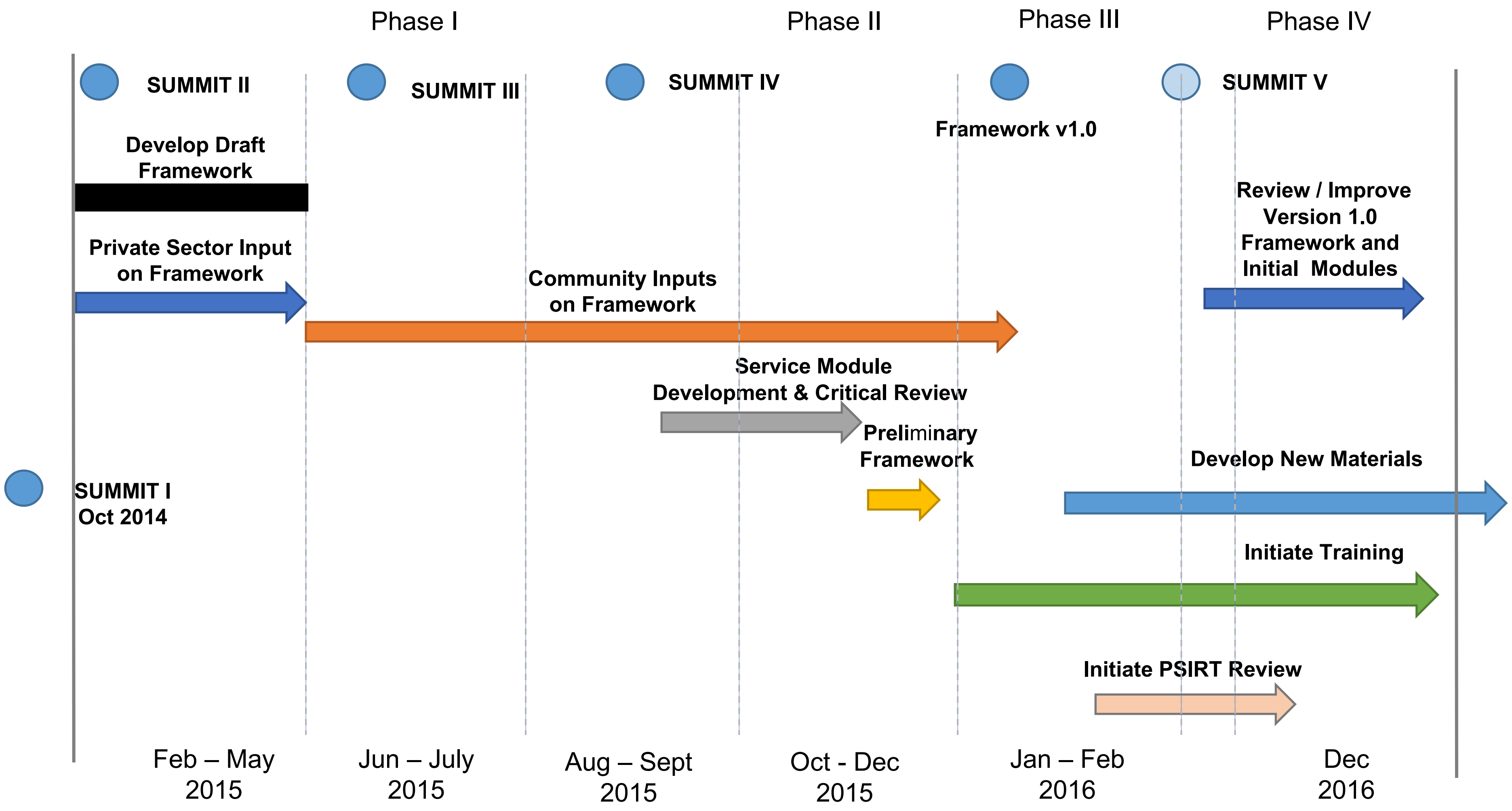
Incident Response Framework Journeys

Peter Allor
Education Advisory Board, Chair
FIRST.Org, Inc.

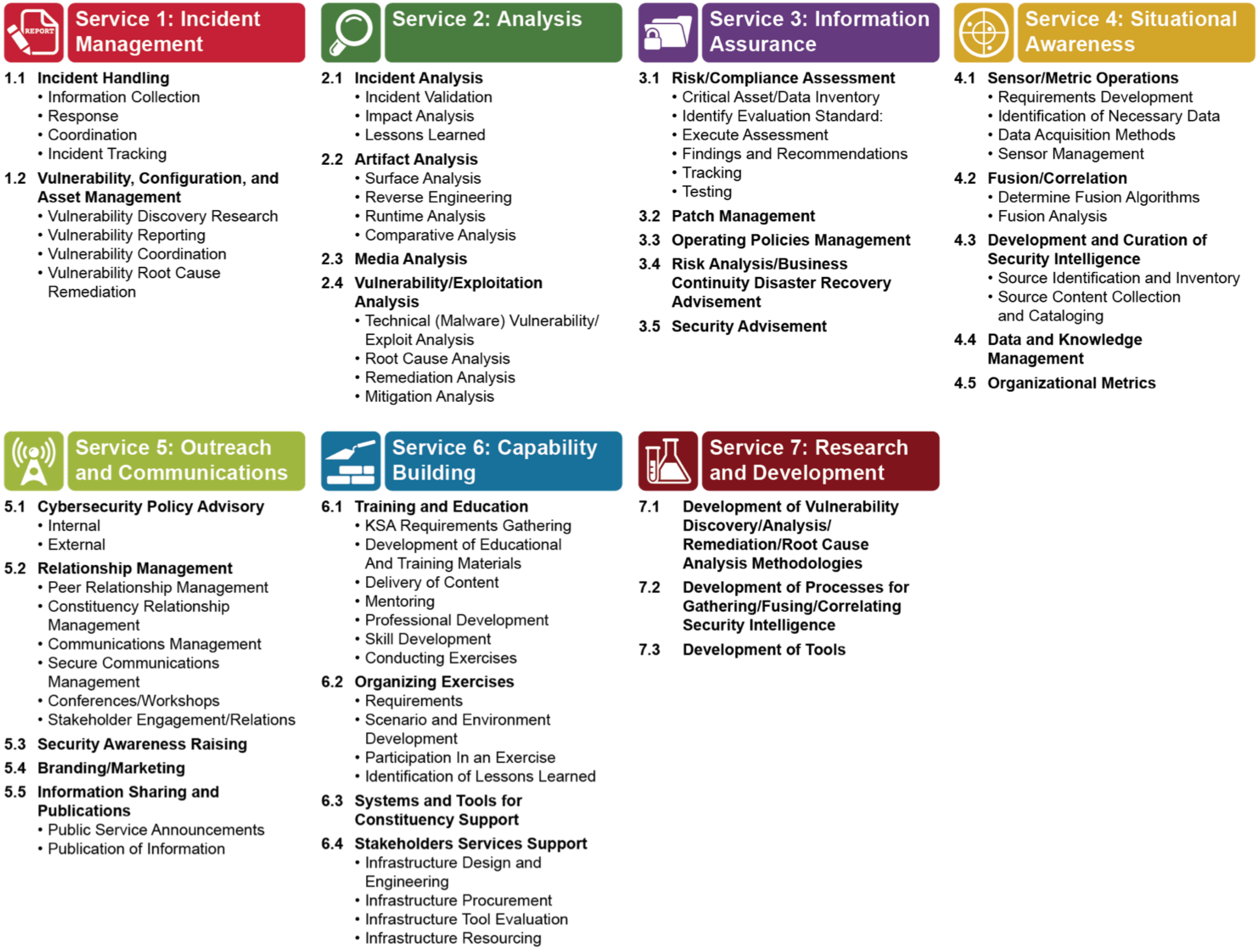
Education and Training

- It started with an idea…..it became a journey
- Then a Framework
- Then another
- Once upon a time CERT/CC

Program Timeline



CSIRT Services Framework v 1.0



Service 1: Incident Management

1.1 Incident Handling
- Information Collection
- Response
- Coordination
- Incident Tracking

1.2 Vulnerability, Configuration, and Asset Management
- Vulnerability Discovery Research
- Vulnerability Reporting
- Vulnerability Coordination
- Vulnerability Root Cause Remediation

Service 2: Analysis

2.1 Incident Analysis
- Incident Validation
- Impact Analysis
- Lessons Learned

2.2 Artifact Analysis
- Surface Analysis
- Reverse Engineering
- Runtime Analysis
- Comparative Analysis

2.3 Media Analysis

2.4 Vulnerability/Exploitation Analysis
- Technical (Malware) Vulnerability/ Exploit Analysis
- Root Cause Analysis
- Remediation Analysis
- Mitigation Analysis

Service 3: Information Assurance

3.1 Risk/Compliance Assessment
- Critical Asset/Data Inventory
- Identify Evaluation Standard:
- Execute Assessment
- Findings and Recommendations
- Tracking
- Testing

3.2 Patch Management

3.3 Operating Policies Management

3.4 Risk Analysis/Business Continuity Disaster Recovery Advisement

3.5 Security Advisement

Service 4: Situational Awareness

4.1 Sensor/Metric Operations
- Requirements Development
- Identification of Necessary Data
- Data Acquisition Methods
- Sensor Management

4.2 Fusion/Correlation
- Determine Fusion Algorithms
- Fusion Analysis

4.3 Development and Curation of Security Intelligence
- Source Identification and Inventory
- Source Content Collection and Cataloging

4.4 Data and Knowledge Management

4.5 Organizational Metrics

Service 5: Outreach and Communications

5.1 Cybersecurity Policy Advisory
- Internal
- External

5.2 Relationship Management
- Peer Relationship Management
- Constituency Relationship Management
- Communications Management
- Secure Communications Management
- Conferences/Workshops
- Stakeholder Engagement/Relations

5.3 Security Awareness Raising

5.4 Branding/Marketing

5.5 Information Sharing and Publications
- Public Service Announcements
- Publication of Information

Service 6: Capability Building

6.1 Training and Education
- KSA Requirements Gathering
- Development of Educational And Training Materials
- Delivery of Content
- Mentoring
- Professional Development
- Skill Development
- Conducting Exercises

6.2 Organizing Exercises
- Requirements
- Scenario and Environment Development
- Participation In an Exercise
- Identification of Lessons Learned

6.3 Systems and Tools for Constituency Support

6.4 Stakeholders Services Support
- Infrastructure Design and Engineering
- Infrastructure Procurement
- Infrastructure Tool Evaluation
- Infrastructure Resourcing

Service 7: Research and Development

7.1 Development of Vulnerability Discovery/Analysis/ Remediation/Root Cause Analysis Methodologies

7.2 Development of Processes for Gathering/Fusing/Correlating Security Intelligence

7.3 Development of Tools

Framework – hierarchical approach

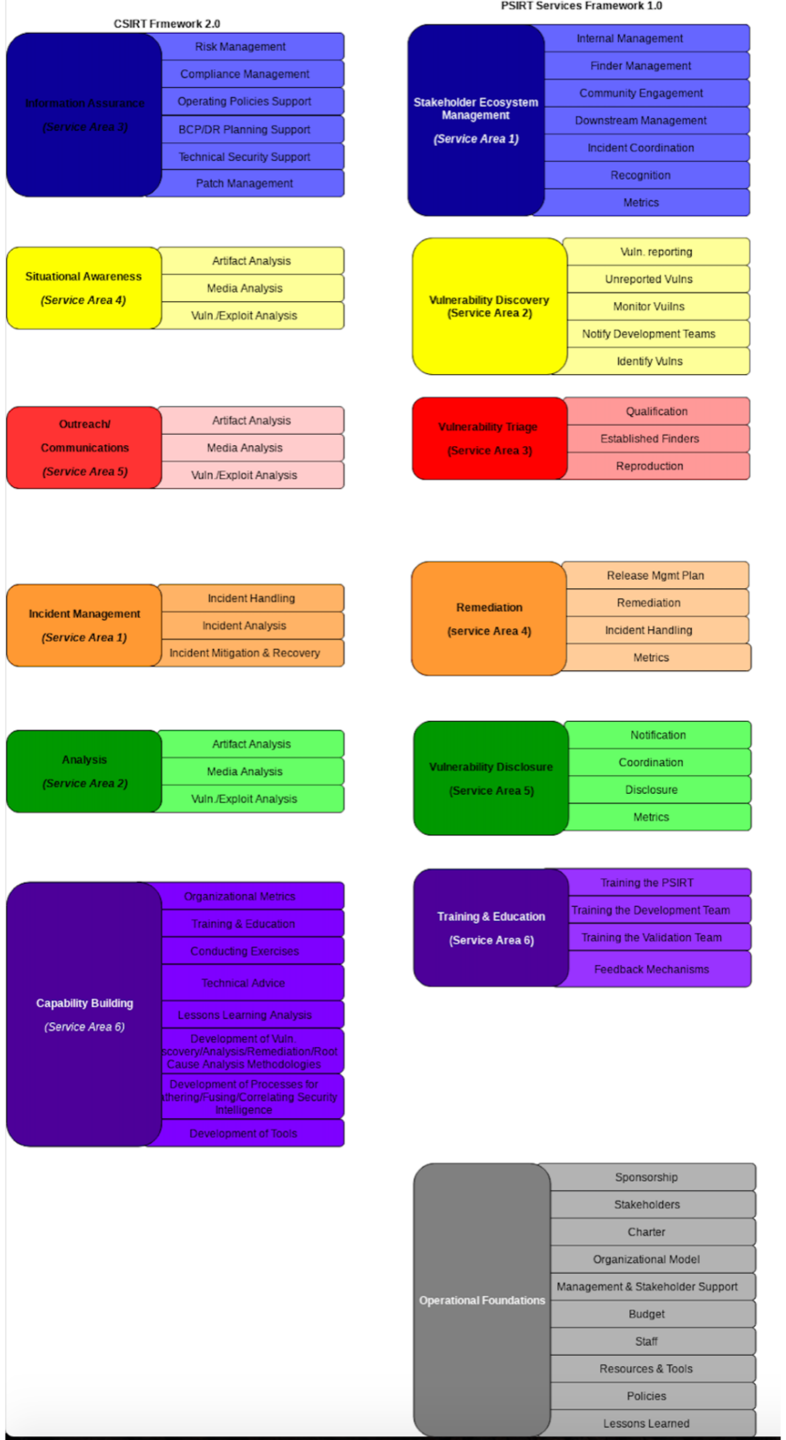
- Service Area
  - Service
    - Function
      - Sub-Function
        - Task
          - Sub-Task
            - Action

Simplified Definitions

- **Capability** – Can you do it?

- **Maturity** – How well can you do it?

- **Capacity** – How much can you do?



CSIRT Frmework 2.0

Information Assurance *(Service Area 3)*
- Risk Management
- Compliance Management
- Operating Policies Support
- BCP/DR Planning Support
- Technical Security Support
- Patch Management

Situational Awareness *(Service Area 4)*
- Artifact Analysis
- Media Analysis
- Vuln./Exploit Analysis

Outreach/ Communications *(Service Area 5)*
- Artifact Analysis
- Media Analysis
- Vuln./Exploit Analysis

Incident Management *(Service Area 1)*
- Incident Handling
- Incident Analysis
- Incident Mitigation & Recovery

Analysis *(Service Area 2)*
- Artifact Analysis
- Media Analysis
- Vuln./Exploit Analysis

Capability Building *(Service Area 6)*
- Organizational Metrics
- Training & Education
- Conducting Exercises
- Technical Advice
- Lessons Learning Analysis
- Development of Vuln. scovery/Analysis/Remediation/Root Cause Analysis Methodologies
- Development of Processes for athering/Fusing/Correlating Security Intelligence
- Development of Tools

PSIRT Services Framework 1.0

Stakeholder Ecosystem Management *(Service Area 1)*
- Internal Management
- Finder Management
- Community Engagement
- Downstream Management
- Incident Coordination
- Recognition
- Metrics

Vulnerability Discovery (Service Area 2)
- Vuln. reporting
- Unreported Vulns
- Monitor Vuilns
- Notify Development Teams
- Identify Vulns

Vulnerability Triage (Service Area 3)
- Qualification
- Established Finders
- Reproduction

Remediation (service Area 4)
- Release Mgmt Plan
- Remediation
- Incident Handling
- Metrics

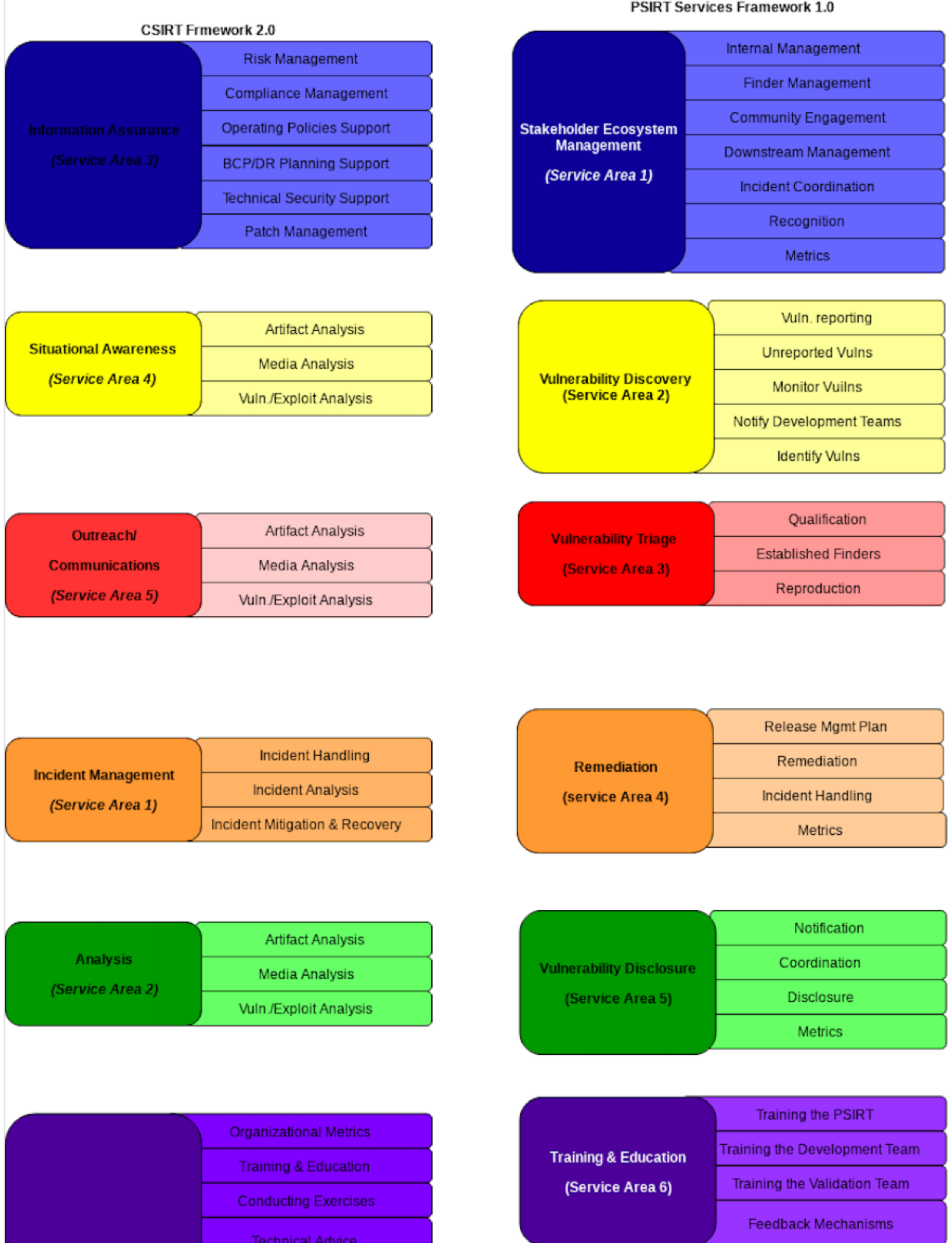
Vulnerability Disclosure (Service Area 5)
- Notification
- Coordination
- Disclosure
- Metrics

Training & Education (Service Area 6)
- Training the PSIRT
- Training the Development Team
- Training the Validation Team
- Feedback Mechanisms

Operational Foundations
- Sponsorship
- Stakeholders
- Charter
- Organizational Model
- Management & Stakeholder Support
- Budget
- Staff
- Resources & Tools
- Policies
- Lessons Learned

FIRST™

Improving Security Together



FIRST™

Improving Security Together

CSIRT Frmework 2.0

Information Assurance
(Service Area 3)
- Risk Management
- Compliance Management
- Operating Policies Support
- BCP/DR Planning Support
- Technical Security Support
- Patch Management

Situational Awareness
(Service Area 4)
- Artifact Analysis
- Media Analysis
- Vuln./Exploit Analysis

Outreach/ Communications
(Service Area 5)
- Artifact Analysis
- Media Analysis
- Vuln./Exploit Analysis

Incident Management
(Service Area 1)
- Incident Handling
- Incident Analysis
- Incident Mitigation & Recovery

Analysis
(Service Area 2)
- Artifact Analysis
- Media Analysis
- Vuln./Exploit Analysis

- Organizational Metrics
- Training & Education
- Conducting Exercises
- Technical Advice

PSIRT Services Framework 1.0

Stakeholder Ecosystem Management
(Service Area 1)
- Internal Management
- Finder Management
- Community Engagement
- Downstream Management
- Incident Coordination
- Recognition
- Metrics

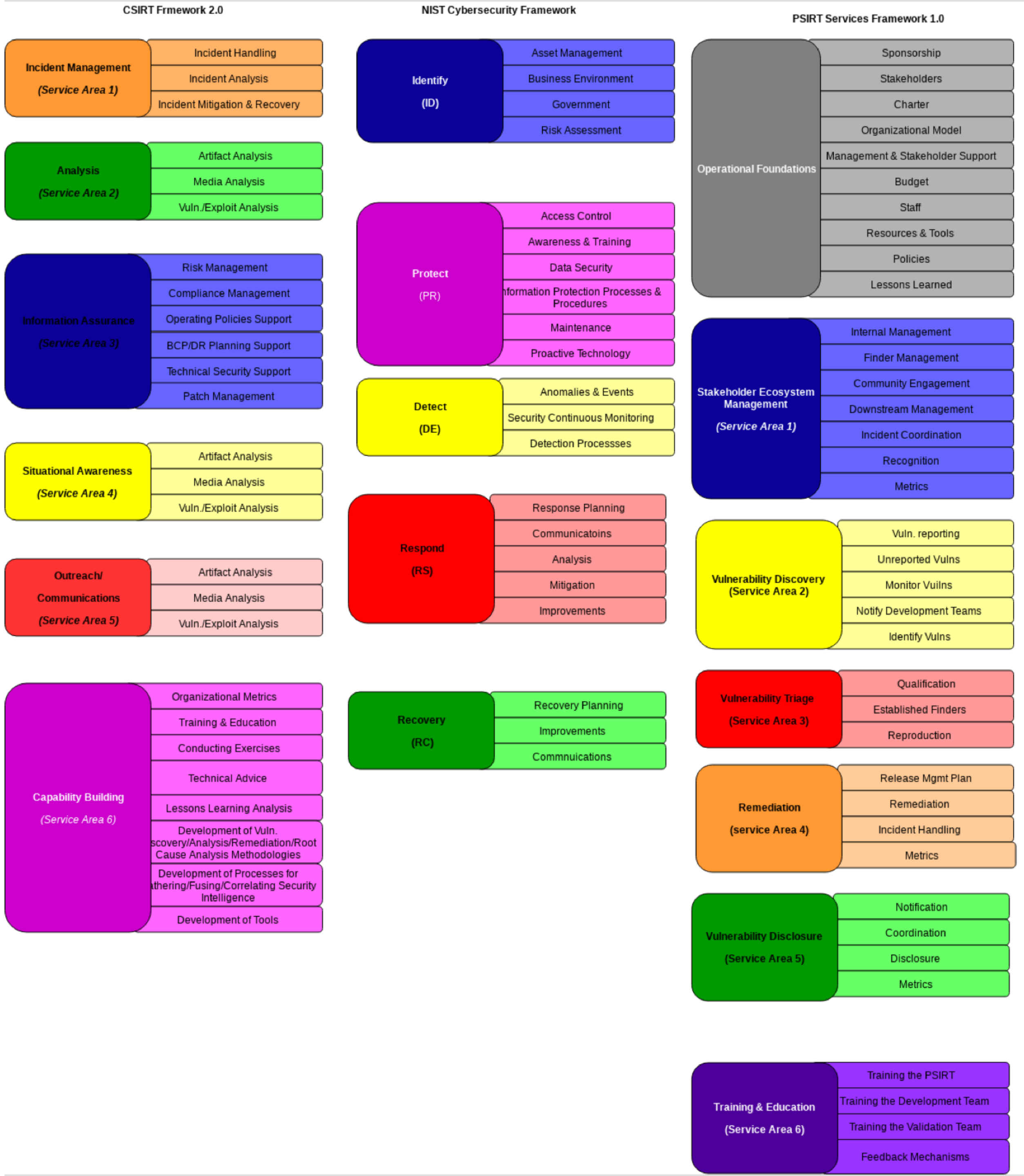
Vulnerability Discovery (Service Area 2)
- Vuln. reporting
- Unreported Vulns
- Monitor Vuilns
- Notify Development Teams
- Identify Vulns

Vulnerability Triage
(Service Area 3)
- Qualification
- Established Finders
- Reproduction

Remediation
(service Area 4)
- Release Mgmt Plan
- Remediation
- Incident Handling
- Metrics

Vulnerability Disclosure
(Service Area 5)
- Notification
- Coordination
- Disclosure
- Metrics

Training & Education
(Service Area 6)
- Training the PSIRT
- Training the Development Team
- Training the Validation Team
- Feedback Mechanisms



CSIRT Frmework 2.0

Incident Management *(Service Area 1)*
- Incident Handling
- Incident Analysis
- Incident Mitigation & Recovery

Analysis *(Service Area 2)*
- Artifact Analysis
- Media Analysis
- Vuln./Exploit Analysis

Information Assurance *(Service Area 3)*
- Risk Management
- Compliance Management
- Operating Policies Support
- BCP/DR Planning Support
- Technical Security Support
- Patch Management

Situational Awareness *(Service Area 4)*
- Artifact Analysis
- Media Analysis
- Vuln./Exploit Analysis

Outreach/ Communications *(Service Area 5)*
- Artifact Analysis
- Media Analysis
- Vuln./Exploit Analysis

Capability Building *(Service Area 6)*
- Organizational Metrics
- Training & Education
- Conducting Exercises
- Technical Advice
- Lessons Learning Analysis
- Development of Vuln. scovery/Analysis/Remediation/Root Cause Analysis Methodologies
- Development of Processes for thering/Fusing/Correlating Security Intelligence
- Development of Tools

NIST Cybersecurity Framework

Identify (ID)
- Asset Management
- Business Environment
- Government
- Risk Assessment

Protect (PR)
- Access Control
- Awareness & Training
- Data Security
- nformation Protection Processes & Procedures
- Maintenance
- Proactive Technology

Detect (DE)
- Anomalies & Events
- Security Continuous Monitoring
- Detection Processses

Respond (RS)
- Response Planning
- Communicatoins
- Analysis
- Mitigation
- Improvements

Recovery (RC)
- Recovery Planning
- Improvements
- Commnuications

PSIRT Services Framework 1.0

Operational Foundations
- Sponsorship
- Stakeholders
- Charter
- Organizational Model
- Management & Stakeholder Support
- Budget
- Staff
- Resources & Tools
- Policies
- Lessons Learned

Stakeholder Ecosystem Management *(Service Area 1)*
- Internal Management
- Finder Management
- Community Engagement
- Downstream Management
- Incident Coordination
- Recognition
- Metrics

Vulnerability Discovery (Service Area 2)
- Vuln. reporting
- Unreported Vulns
- Monitor Vuilns
- Notify Development Teams
- Identify Vulns

Vulnerability Triage (Service Area 3)
- Qualification
- Established Finders
- Reproduction

Remediation (service Area 4)
- Release Mgmt Plan
- Remediation
- Incident Handling
- Metrics

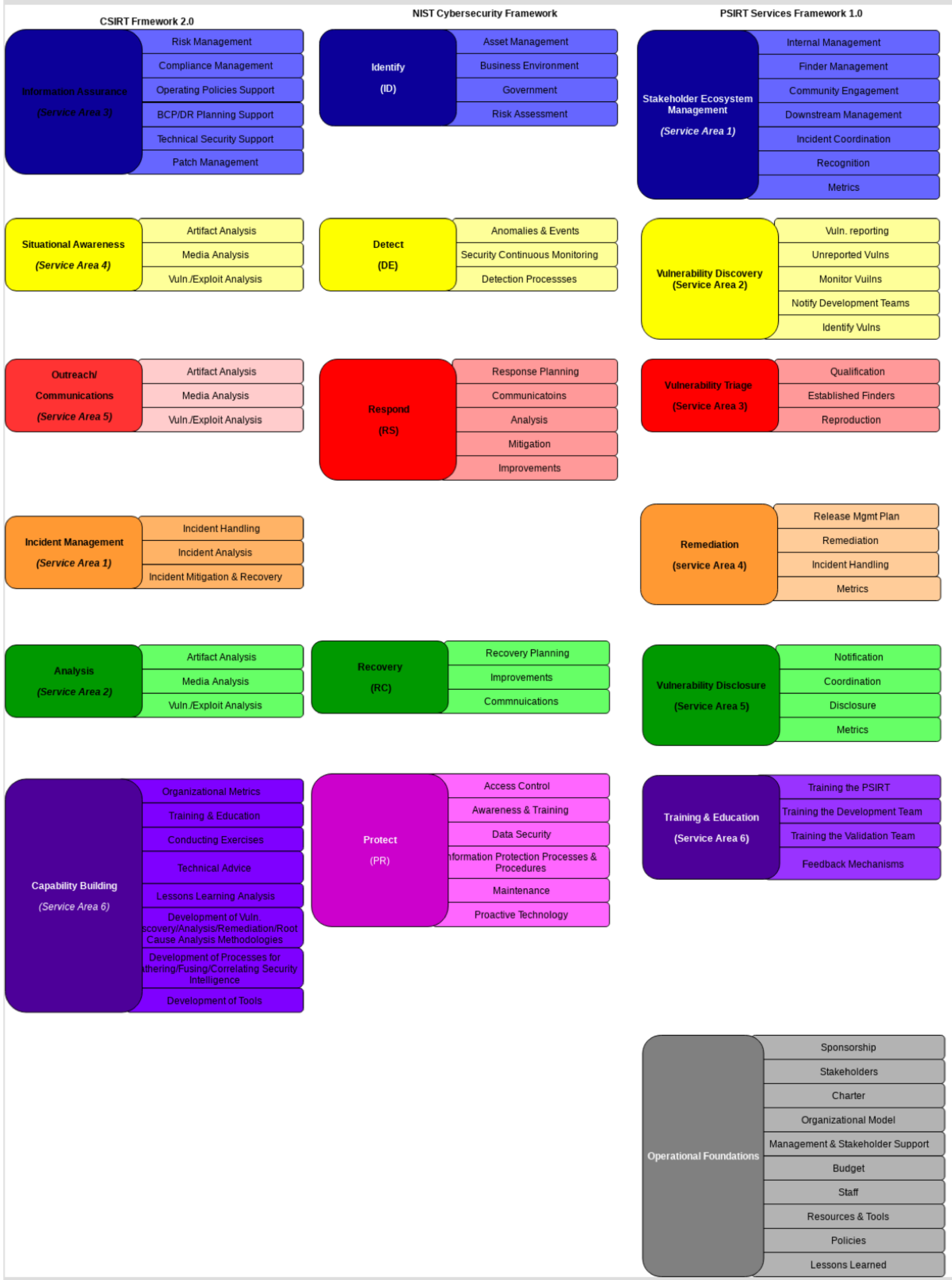
Vulnerability Disclosure (Service Area 5)
- Notification
- Coordination
- Disclosure
- Metrics

Training & Education (Service Area 6)
- Training the PSIRT
- Training the Development Team
- Training the Validation Team
- Feedback Mechanisms

FIRST™

Improving Security Together

FIRST™
Improving Security Together



CSIRT Frmework 2.0

Information Assurance *(Service Area 3)*: Risk Management; Compliance Management; Operating Policies Support; BCP/DR Planning Support; Technical Security Support; Patch Management

Situational Awareness *(Service Area 4)*: Artifact Analysis; Media Analysis; Vuln./Exploit Analysis

Outreach/ Communications *(Service Area 5)*: Artifact Analysis; Media Analysis; Vuln./Exploit Analysis

Incident Management *(Service Area 1)*: Incident Handling; Incident Analysis; Incident Mitigation & Recovery

Analysis *(Service Area 2)*: Artifact Analysis; Media Analysis; Vuln./Exploit Analysis

Capability Building *(Service Area 6)*: Organizational Metrics; Training & Education; Conducting Exercises; Technical Advice; Lessons Learning Analysis; Development of Vuln. scovery/Analysis/Remediation/Root Cause Analysis Methodologies; Development of Processes for athering/Fusing/Correlating Security Intelligence; Development of Tools

NIST Cybersecurity Framework

Identify (ID): Asset Management; Business Environment; Government; Risk Assessment

Detect (DE): Anomalies & Events; Security Continuous Monitoring; Detection Processses

Respond (RS): Response Planning; Communicatoins; Analysis; Mitigation; Improvements

Recovery (RC): Recovery Planning; Improvements; Commnuications

Protect (PR): Access Control; Awareness & Training; Data Security; nformation Protection Processes & Procedures; Maintenance; Proactive Technology

PSIRT Services Framework 1.0

Stakeholder Ecosystem Management *(Service Area 1)*: Internal Management; Finder Management; Community Engagement; Downstream Management; Incident Coordination; Recognition; Metrics

Vulnerability Discovery (Service Area 2): Vuln. reporting; Unreported Vulns; Monitor Vuilns; Notify Development Teams; Identify Vulns

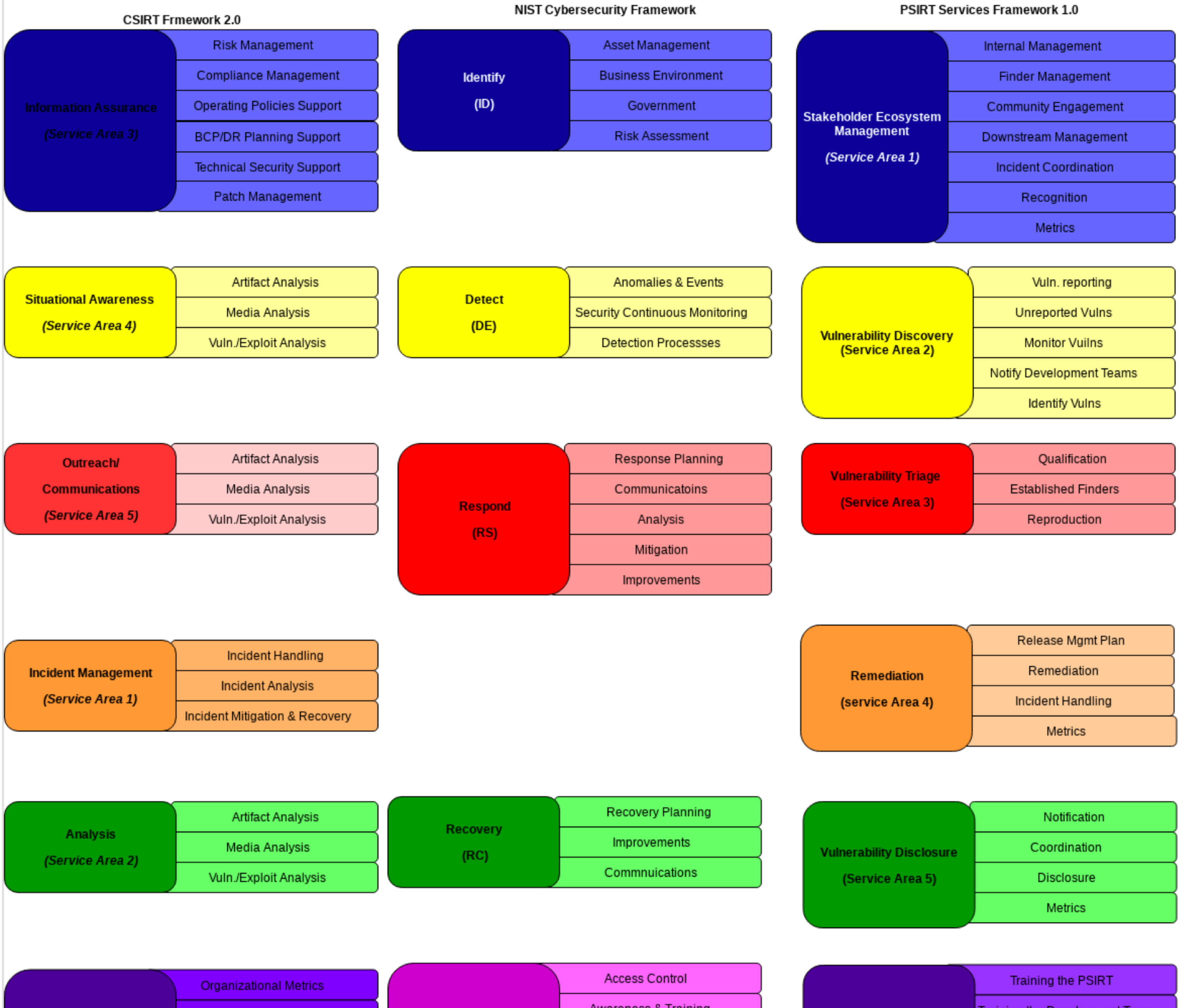
Vulnerability Triage (Service Area 3): Qualification; Established Finders; Reproduction

Remediation (service Area 4): Release Mgmt Plan; Remediation; Incident Handling; Metrics

Vulnerability Disclosure (Service Area 5): Notification; Coordination; Disclosure; Metrics

Training & Education (Service Area 6): Training the PSIRT; Training the Development Team; Training the Validation Team; Feedback Mechanisms

Operational Foundations: Sponsorship; Stakeholders; Charter; Organizational Model; Management & Stakeholder Support; Budget; Staff; Resources & Tools; Policies; Lessons Learned



CSIRT Frmework 2.0

- Information Assurance *(Service Area 3)*: Risk Management; Compliance Management; Operating Policies Support; BCP/DR Planning Support; Technical Security Support; Patch Management
- Situational Awareness *(Service Area 4)*: Artifact Analysis; Media Analysis; Vuln./Exploit Analysis
- Outreach/ Communications *(Service Area 5)*: Artifact Analysis; Media Analysis; Vuln./Exploit Analysis
- Incident Management *(Service Area 1)*: Incident Handling; Incident Analysis; Incident Mitigation & Recovery
- Analysis *(Service Area 2)*: Artifact Analysis; Media Analysis; Vuln./Exploit Analysis
- Organizational Metrics

NIST Cybersecurity Framework

- Identify (ID): Asset Management; Business Environment; Government; Risk Assessment
- Detect (DE): Anomalies & Events; Security Continuous Monitoring; Detection Processses
- Respond (RS): Response Planning; Communicatoins; Analysis; Mitigation; Improvements
- Recovery (RC): Recovery Planning; Improvements; Commnuications
- Access Control

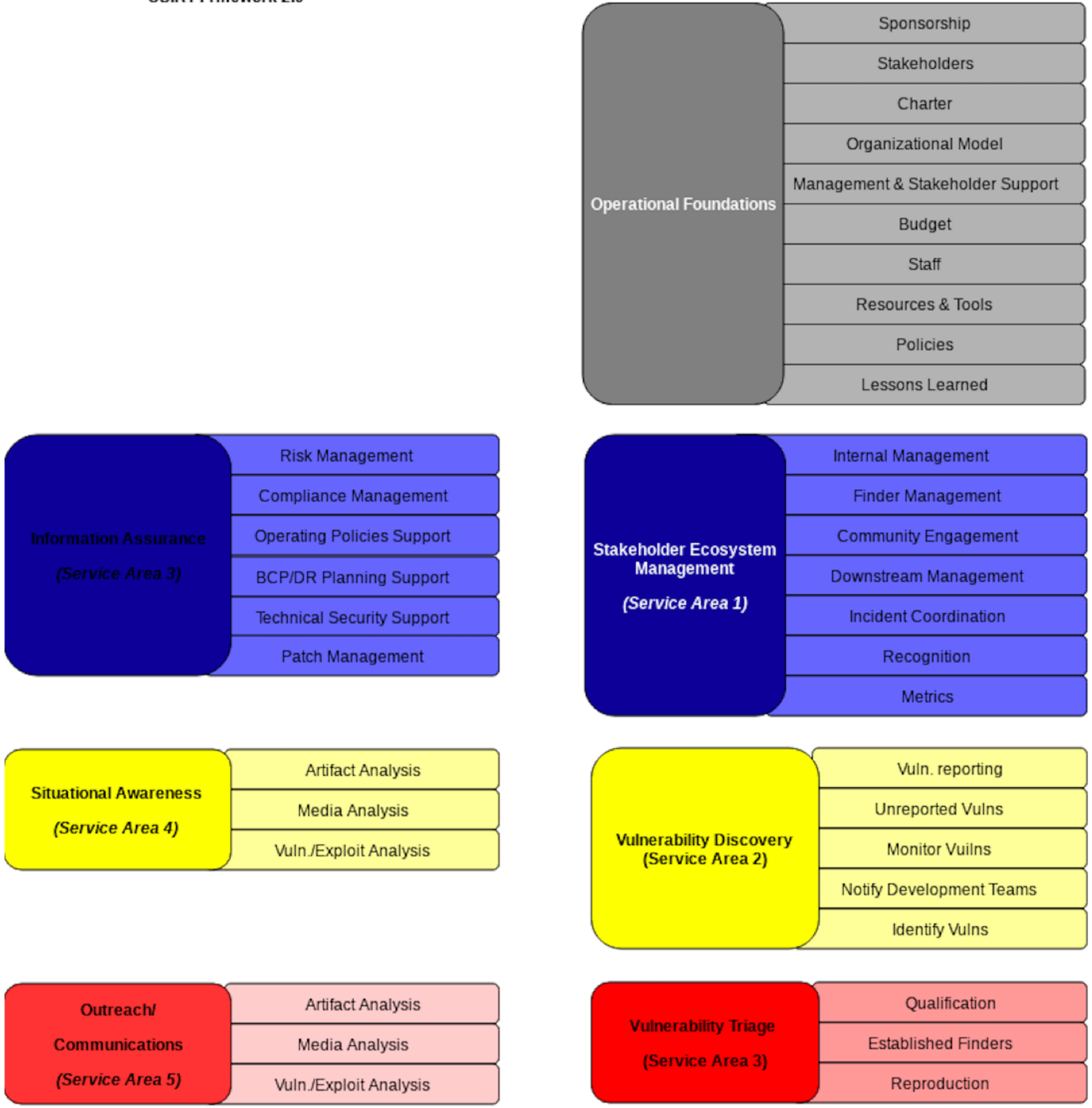
PSIRT Services Framework 1.0

- Stakeholder Ecosystem Management *(Service Area 1)*: Internal Management; Finder Management; Community Engagement; Downstream Management; Incident Coordination; Recognition; Metrics
- Vulnerability Discovery (Service Area 2): Vuln. reporting; Unreported Vulns; Monitor Vuilns; Notify Development Teams; Identify Vulns
- Vulnerability Triage (Service Area 3): Qualification; Established Finders; Reproduction
- Remediation (service Area 4): Release Mgmt Plan; Remediation; Incident Handling; Metrics
- Vulnerability Disclosure (Service Area 5): Notification; Coordination; Disclosure; Metrics
- Training the PSIRT

CSIRT Frmework 2.0

PSIRT Services Framework 1.0

FIRST
Improving Security Together



Operational Foundations
- Sponsorship
- Stakeholders
- Charter
- Organizational Model
- Management & Stakeholder Support
- Budget
- Staff
- Resources & Tools
- Policies
- Lessons Learned

Information Assurance
(Service Area 3)
- Risk Management
- Compliance Management
- Operating Policies Support
- BCP/DR Planning Support
- Technical Security Support
- Patch Management

Stakeholder Ecosystem Management
(Service Area 1)
- Internal Management
- Finder Management
- Community Engagement
- Downstream Management
- Incident Coordination
- Recognition
- Metrics

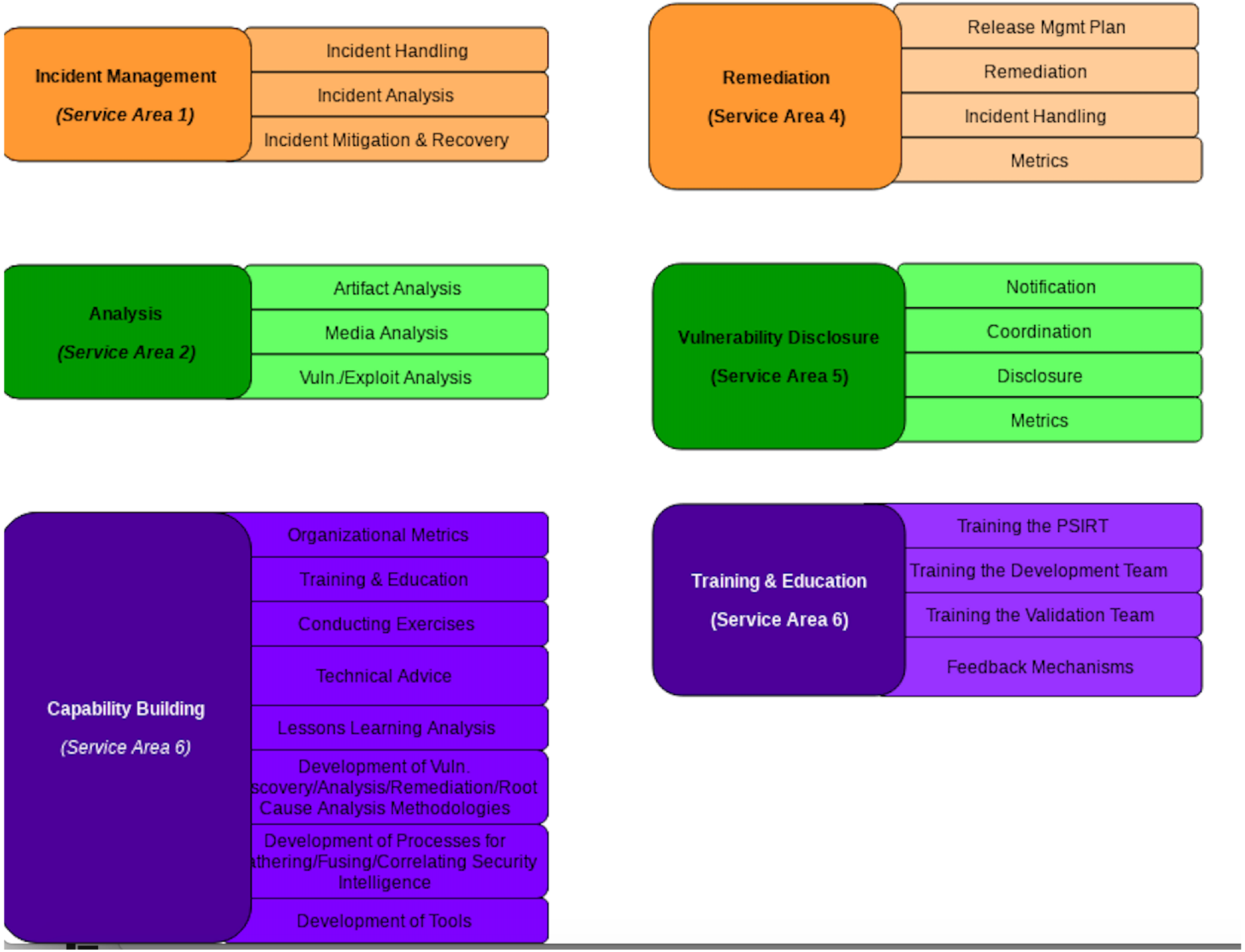
Situational Awareness
(Service Area 4)
- Artifact Analysis
- Media Analysis
- Vuln./Exploit Analysis

Vulnerability Discovery
(Service Area 2)
- Vuln. reporting
- Unreported Vulns
- Monitor Vuilns
- Notify Development Teams
- Identify Vulns

Outreach/
Communications
(Service Area 5)
- Artifact Analysis
- Media Analysis
- Vuln./Exploit Analysis

Vulnerability Triage
(Service Area 3)
- Qualification
- Established Finders
- Reproduction

FIRST™
Improving Security Together



Incident Management
(Service Area 1)

- Incident Handling
- Incident Analysis
- Incident Mitigation & Recovery

Remediation
(Service Area 4)

- Release Mgmt Plan
- Remediation
- Incident Handling
- Metrics

Analysis
(Service Area 2)

- Artifact Analysis
- Media Analysis
- Vuln./Exploit Analysis

Vulnerability Disclosure
(Service Area 5)

- Notification
- Coordination
- Disclosure
- Metrics

Capability Building
(Service Area 6)

- Organizational Metrics
- Training & Education
- Conducting Exercises
- Technical Advice
- Lessons Learning Analysis
- Development of Vuln. scovery/Analysis/Remediation/Root Cause Analysis Methodologies
- Development of Processes for thering/Fusing/Correlating Security Intelligence
- Development of Tools

Training & Education
(Service Area 6)

- Training the PSIRT
- Training the Development Team
- Training the Validation Team
- Feedback Mechanisms