

FIRST.Org, Inc

Incident Response Framework Journeys

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

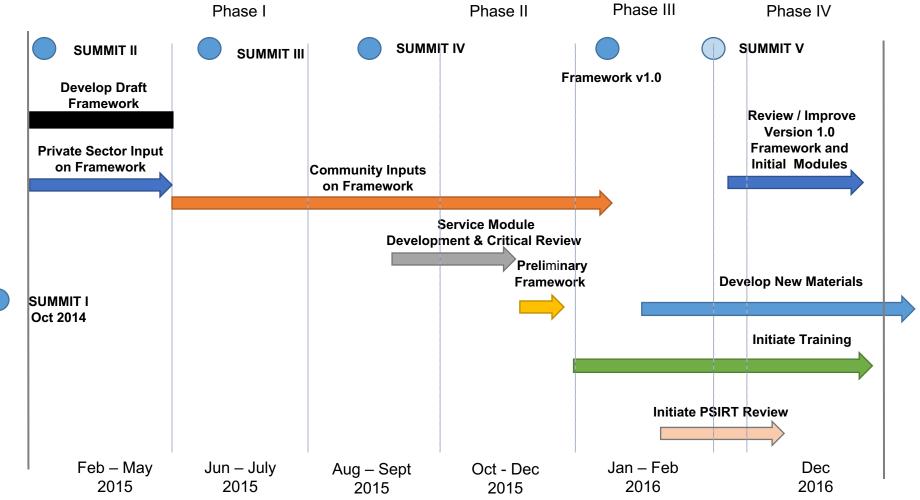
Education and Training



- 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 Service 2: Analysis **Service 3: Information** Service 4: Situational Management Assurance Awareness 1.1 Incident Handling 2.1 Incident Analysis 3.1 Risk/Compliance Assessment 4.1 Sensor/Metric Operations Information Collection Incident Validation Critical Asset/Data Inventory Requirements Development · Identify Evaluation Standard: Identification of Necessary Data Response Impact Analysis Coordination · Lessons Learned Execute Assessment Data Acquisition Methods Incident Tracking • Findings and Recommendations Sensor Management 2.2 Artifact Analysis Tracking 1.2 Vulnerability, Configuration, and Surface Analysis 4.2 Fusion/Correlation Testing Asset Management Reverse Engineering Determine Fusion Algorithms Vulnerability Discovery Research Runtime Analysis 3.2 Patch Management Fusion Analysis Vulnerability Reporting · Comparative Analysis 3.3 Operating Policies Management 4.3 Development and Curation of Vulnerability Coordination 2.3 Media Analysis Security Intelligence 3.4 Risk Analysis/Business Vulnerability Root Cause Source Identification and Inventory 2.4 Vulnerability/Exploitation **Continuity Disaster Recovery** Remediation Source Content Collection Analysis Advisement and Cataloging Technical (Malware) Vulnerability/ 3.5 Security Advisement 4.4 Data and Knowledge Exploit Analysis Root Cause Analysis Management Remediation Analysis 4.5 Organizational Metrics Mitigation Analysis Service 6: Capability

(w)) 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/WorkshopsStakeholder Engagement/Relations
- 5.3 Security Awareness Raising
- 5.4 Branding/Marketing
- 5.5 Information Sharing and Publications
 - Public Service Announcements
 Publication of Information

- Building
- 6.1 Training and Education
 KSA Requirements Gathering
 - Development of Educational
 - And Training Materials
 - Delivery of Content
 - Mentoring
 - Professional DevelopmentSkill 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



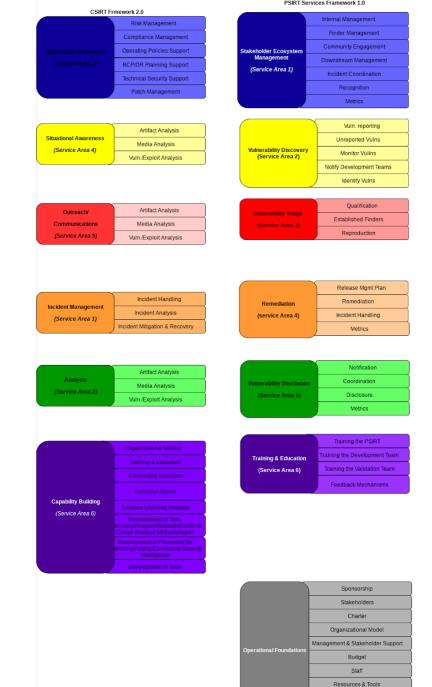
Framework – hierarchical approach

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

Simplified Definitions

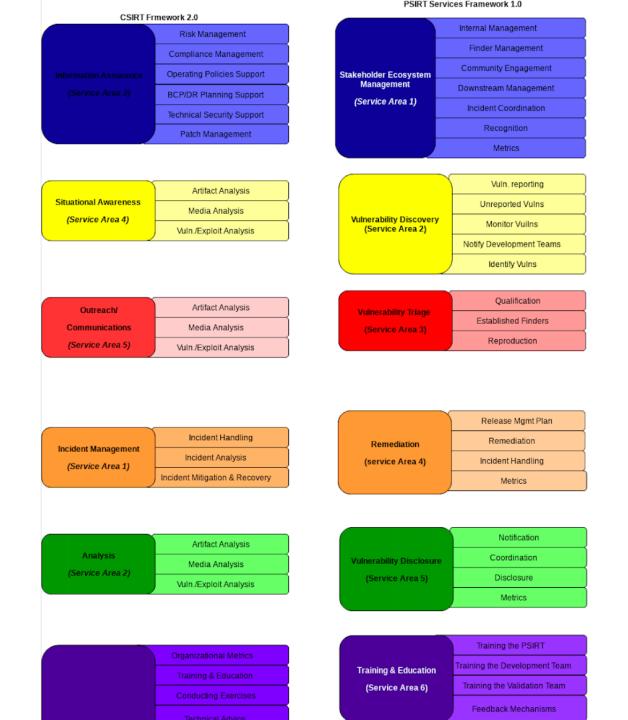


- Capability Can you do it?
- Maturity How well can you do it?
- **Capacity** How much can you do?



Policies Lessons Learned









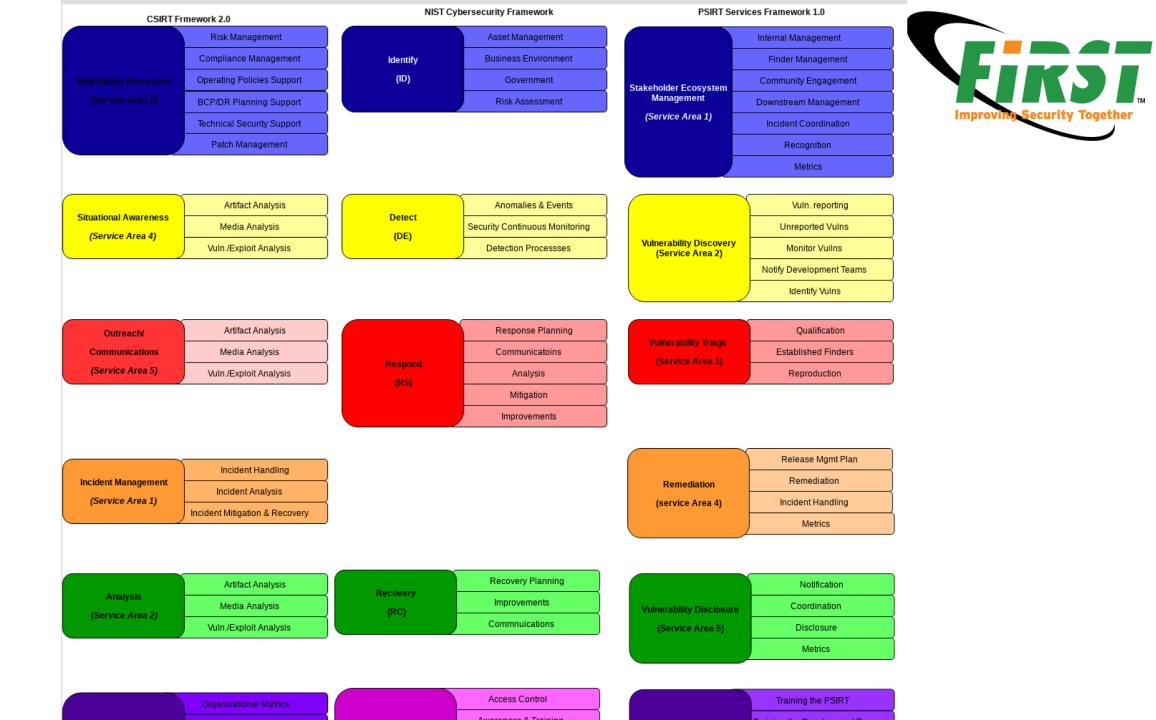
CSI	RT Frmework 2.0	NIST Cyberse	curity Framework	PSIRTS	Services Framework 1.0
	Incident Handling		Asset Management		Sponsorship
Incident Management	Incident Analysis	Identify	Business Environment		Stakeholders
(Service Area 1)	Incident Mitigation & Recovery	(ID)	Government		Charter
			Risk Assessment		Organizational Model
	Artifact Analysis				Management & Stakeholder Support
Analysis	Media Analysis			Operational Foundations	Budget
(Service Area 2)	Vuln./Exploit Analysis		Access Control		Staff
			Awareness & Training		Resources & Tools
	Risk Management		Data Security		Policies
	Compliance Management	Protect	formation Protection Processes &	ر آ	Lessons Learned
	Operating Policies Support	(PR)	Procedures		
	BCP/DR Planning Support		Maintenance		Internal Management
			Proactive Technology		Finder Management
	Technical Security Support Patch Management		Anomalies & Events	Stakeholder Ecosystem	Community Engagement
	Fach Management	Detect	Security Continuous Monitoring	Management	Downstream Management
		(DE)	Detection Processses	(Service Area 1)	Incident Coordination
Situational Awareness	Artifact Analysis				Recognition
(Service Area 4)	Media Analysis				Metrics
	Vuln./Exploit Analysis		Response Planning		
		Respond	Communicatoins		Vuln. reporting
Outreach/	Artifact Analysis	(RS)	Analysis		Unreported Vulns
Communications	Media Analysis		Mitigation	Vulnerability Discovery (Service Area 2)	Monitor Vuilns
(Service Area 5)	Vuln./Exploit Analysis		Improvements		Notify Development Teams
	VullizExploit Analysis				Identify Vulns
	Organizational Metrics			Vulnerability Triage	Qualification
	Training & Education	Recovery	Recovery Planning	(Service Area 3)	Established Finders
	Conducting Exercises	(RC)	Improvements		Reproduction
	Technical Advice		Commnuications		Release Mgmt Plan
Capability Building	Lessons Learning Analysis			Remediation	Remediation
(Service Area 6)	Development of Vuln.			(service Area 4)	Incident Handling
	scovery/Analysis/Remediation/Root Cause Analysis Methodologies				Metrics
	Development of Processes for thering/Fusing/Correlating Security				
	Intelligence Development of Tools				Notification
	2 Stelopinent of Tools			Vulnerability Disclosure	Coordination
				(Service Area 5)	Disclosure
					Metrics

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



CSIRTE	rmework 2.0	NIS	Cybersecurity Framework	PSIRT Servi	ICES FIAINEWOIK 1.0
	Risk Management		Asset Management		Internal Management
Compliance Management Information Assurance Operating Policies Support (Service Area 3) BCP/DR Planning Support Technical Security Support Patch Management	Identify	Business Environment		Finder Management	
	Operating Policies Support	(ID)	Government	Stakeholder Ecosystem	Community Engagement
	BCP/DR Planning Support		Risk Assessment	Management	Downstream Management
	Technical Security Support			(Service Area 1)	Incident Coordination
				Recognition	
					Metrics
	Artifact Analysis		Anomalies & Events		Vuln. reporting
Situational Awareness (Service Area 4)	Media Analysis	Detect	Security Continuous Monitoring		Unreported Vulns
(Service Area 4)	Vuln./Exploit Analysis	(DE)	Detection Processses	Vulnerability Discovery (Service Area 2)	Monitor Vuilns
				,	Notify Development Teams
					Identify Vulns
Outreach/	Artifact Analysis		Response Planning		Qualification
Communications	Media Analysis		Communicatoins	Vulnerability Triage	Established Finders
(Service Area 5)	Vuln./Exploit Analysis	Respond	Analysis	(Service Area 3)	Reproduction
		(RS)	Mitigation		
			Improvements		
					Deleges Marsh Diag
Incident Handling				Release Mgmt Plan	
Incident Management	Incident Handling			Remediation	Remediation
Incident Management (Service Area 1)	Incident Analysis			Remediation (service Area 4)	
				Remediation (service Area 4)	Remediation Incident Handling
	Incident Analysis				Remediation
	Incident Analysis				Remediation Incident Handling
	Incident Analysis	_	Recovery Planning		Remediation Incident Handling
(Service Area 1) Analysis	Incident Analysis Incident Mitigation & Recovery Artifact Analysis	Recovery	Recovery Planning	(service Area 4)	Remediation Incident Handling Metrics Notification
(Service Area 1)	Incident Analysis Incident Mitigation & Recovery Artifact Analysis Media Analysis	Recovery (RC)		(service Area 4) Vulnerability Disclosure	Remediation Incident Handling Metrics
(Service Area 1) Analysis	Incident Analysis Incident Mitigation & Recovery Artifact Analysis		Improvements	(service Area 4)	Remediation Incident Handling Metrics Notification Coordination Disclosure
(Service Area 1) Analysis	Incident Analysis Incident Mitigation & Recovery Artifact Analysis Media Analysis		Improvements	(service Area 4) Vulnerability Disclosure	Remediation Incident Handling Metrics Notification Coordination
(Service Area 1) Analysis	Incident Analysis Incident Mitigation & Recovery Artifact Analysis Media Analysis		Improvements Commnuications	(service Area 4) Vulnerability Disclosure	Remediation Incident Handling Metrics Notification Coordination Disclosure
(Service Area 1) Analysis	Incident Analysis Incident Mitigation & Recovery Artifact Analysis Media Analysis		Improvements Communications Access Control	(service Area 4) Vulnerability Disclosure	Remediation Incident Handling Metrics Notification Coordination Disclosure
(Service Area 1) Analysis	Incident Analysis Incident Mitigation & Recovery Artifact Analysis Media Analysis Vuln /Exploit Analysis		Improvements Commnuications	(service Area 4) Vulnerability Disclosure	Remediation Incident Handling Metrics Notfication Coordination Disclosure Metrics Training the PSIRT
(Service Area 1) Analysis	Incident Analysis Incident Mitigation & Recovery Artifact Analysis Media Analysis Vuln /Exploit Analysis Organizational Metrics		Improvements Communications Access Control Awareness & Training Data Security	(service Area 4) Vulnerability Disclosure (Service Area 5)	Remediation Incident Handling Metrics Notfication Coordination Disclosure Metrics Training the PSIRT Training the Development Tee
(Service Area 1) Analysis	Incident Analysis Incident Mitigation & Recovery Artifact Analysis Media Analysis Vuln /Exploit Analysis Organizational Metrics Training & Education	(RC)	Improvements Communications Access Control Awareness & Training	(service Area 4) Vuinerability Disclosure (Service Area 5) Training & Education	Remediation Incident Handling Metrics Notfication Coordination Disclosure Metrics Training the PSIRT Training the Development Tee
(Service Area 1) Analysis	Incident Analysis Incident Mitigation & Recovery Artifact Analysis Media Analysis Vuln /Exploit Analysis Organizational Metrics Training & Education Conducting Exercises Technical Advice	(RC) Protect	Improvements Communications Access Control Awareness & Training Data Security Information Protection Processes &	(service Area 4) Vuinerability Disclosure (Service Area 5) Training & Education	Remediation Incident Handling Metrics Notification Coordination Disclosure Metrics Training the PSIRT Training the Development Tea Training the Validation Team
(Service Area 1) Analysis (Service Area 2)	Incident Analysis Incident Mitigation & Recovery Artifact Analysis Media Analysis Vuln./Exploit Analysis Vuln./Exploit Analysis Organizational Metrics Training & Education Conducting Exercises Technical Advice Lessons Learning Analysis	(RC) Protect	Improvements Commulications Access Control Awareness & Training Data Security formation Protection Processes & Procedures Maintenance	(service Area 4) Vuinerability Disclosure (Service Area 5) Training & Education	Remediation Incident Handling Metrics Notification Coordination Disclosure Metrics Training the PSIRT Training the Development Tea Training the Validation Team
(Service Area 1) Analysis (Service Area 2) Capability Building	Incident Analysis Incident Mitigation & Recovery Artifact Analysis Media Analysis Vuln /Exploit Analysis Vuln /Exploit Analysis Organizational Metrics Training & Education Conducting Exercises Technical Advice Lessons Learning Analysis Development of Vuln Scorery/Analysis Remediation/Root	(RC) Protect	Improvements Commulications Access Control Awareness & Training Data Security Tormation Protection Processes & Procedures	(service Area 4) Vuinerability Disclosure (Service Area 5) Training & Education	Remediation Incident Handling Metrics Notification Coordination Disclosure Metrics Training the PSIRT Training the Development Tea Training the Ustidation Team
(Service Area 1) Analysis (Service Area 2) Capability Building	Incident Analysis Incident Mitigation & Recovery Artifact Analysis Media Analysis Vuln /Exploit Analysis Organizational Metrics Training & Education Conducting Exercises Technical Advice Lessons Learning Analysis Development of Vuin	(RC) Protect	Improvements Commulications Access Control Awareness & Training Data Security formation Protection Processes & Procedures Maintenance	(service Area 4) Vuinerability Disclosure (Service Area 5) Training & Education	Remediation Incident Handling Metrics Notification Coordination Disclosure Metrics Training the PSIRT Training the Development Tea Training the Ustidation Team

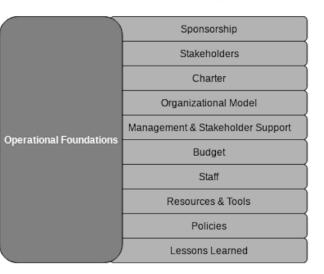
	Sponsorship	
	Stakeholders	
	Charter	
	Organizational Model	
Operational Foundations	Management & Stakeholder Support	
Operational Foundations	Budget	
	Staff	
	Resources & Tools	
	Policies	
	Lessons Learned	





PSIRT Services	Framework 1.0
----------------	---------------

CSIRT	Frmework	20



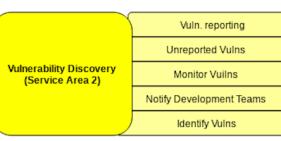


Operating Policies Support	Sta
BCP/DR Planning Support	
Technical Security Support	
Patch Management	

Risk Management

Compliance Management





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



