

Information Security Incident Management Program



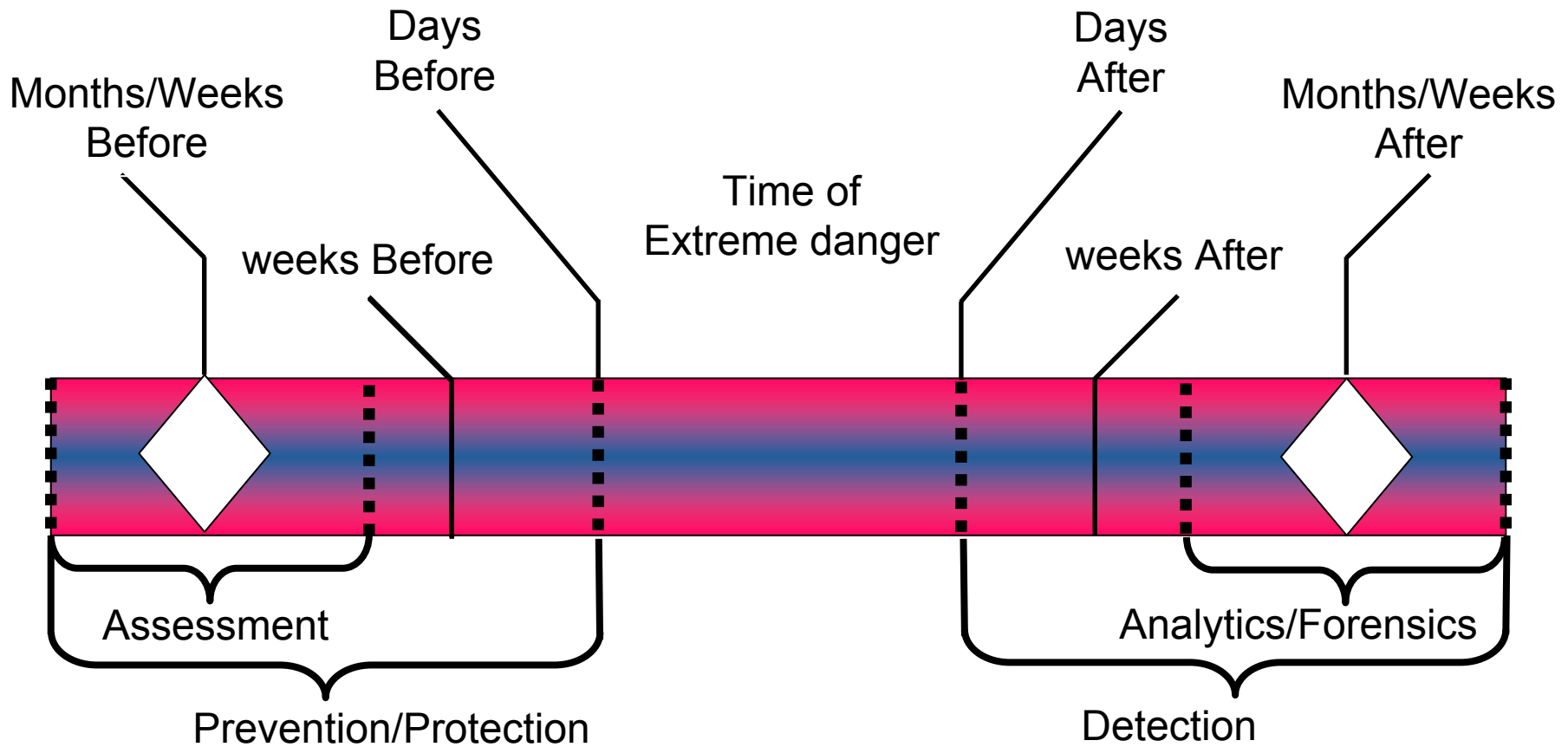
What is an Incident Management Program?

- It is a coordinated program of people, processes, tools and technology, which prevents and manages information security threats, vulnerabilities and incidents in order to minimize their impact on a company or organization.

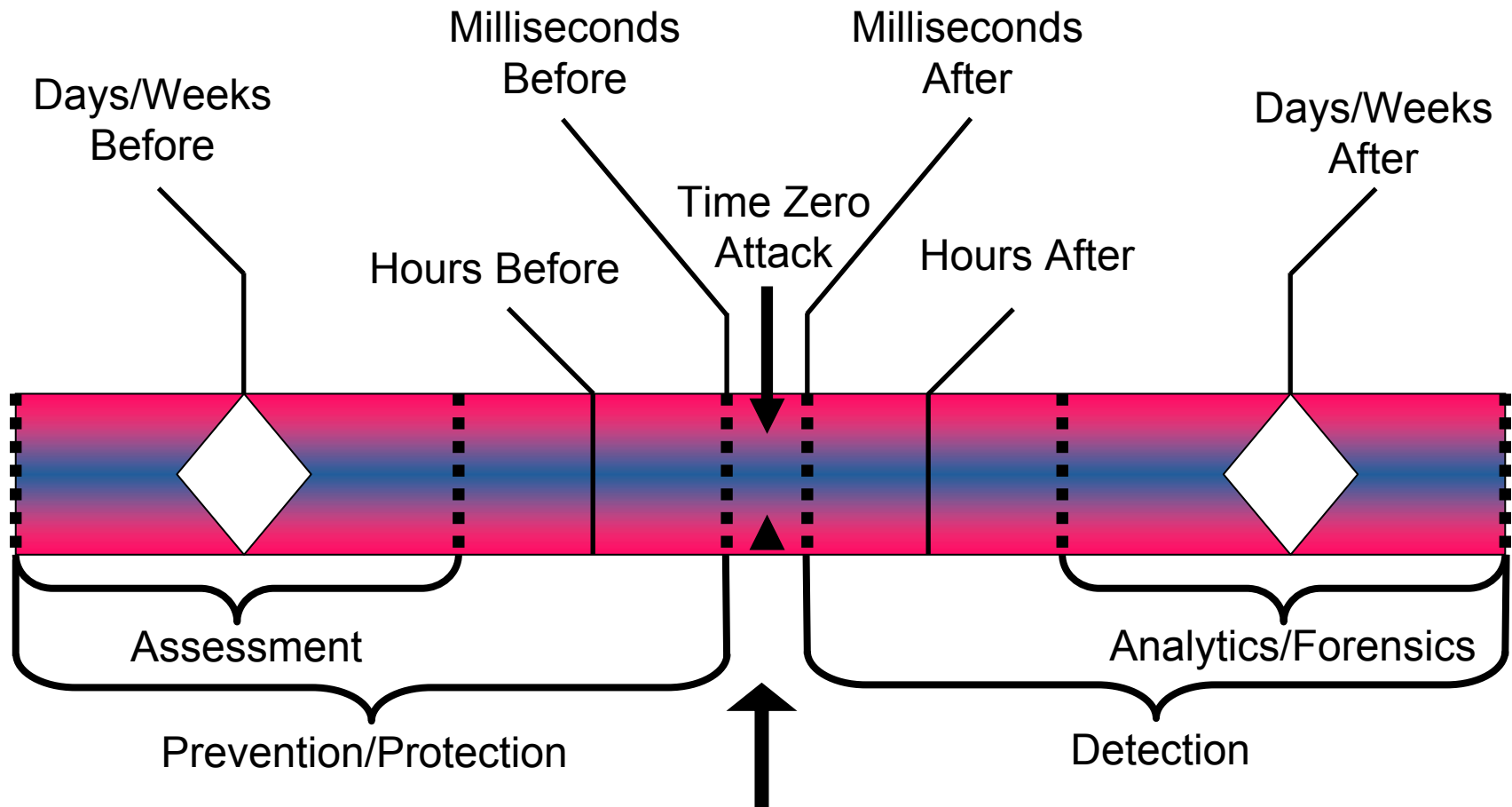
Why is it needed?

- To protect a company's brand and reputation
- To protect a company's intellectual property
- To ensure a company's uninterrupted ability to conduct business
- To avoid lost customers and revenue
- To avoid the cost of lost productivity
- To avoid the cost of cleaning up the effects of security incidents on the IT infrastructure

Normal Attack & Response Timeline

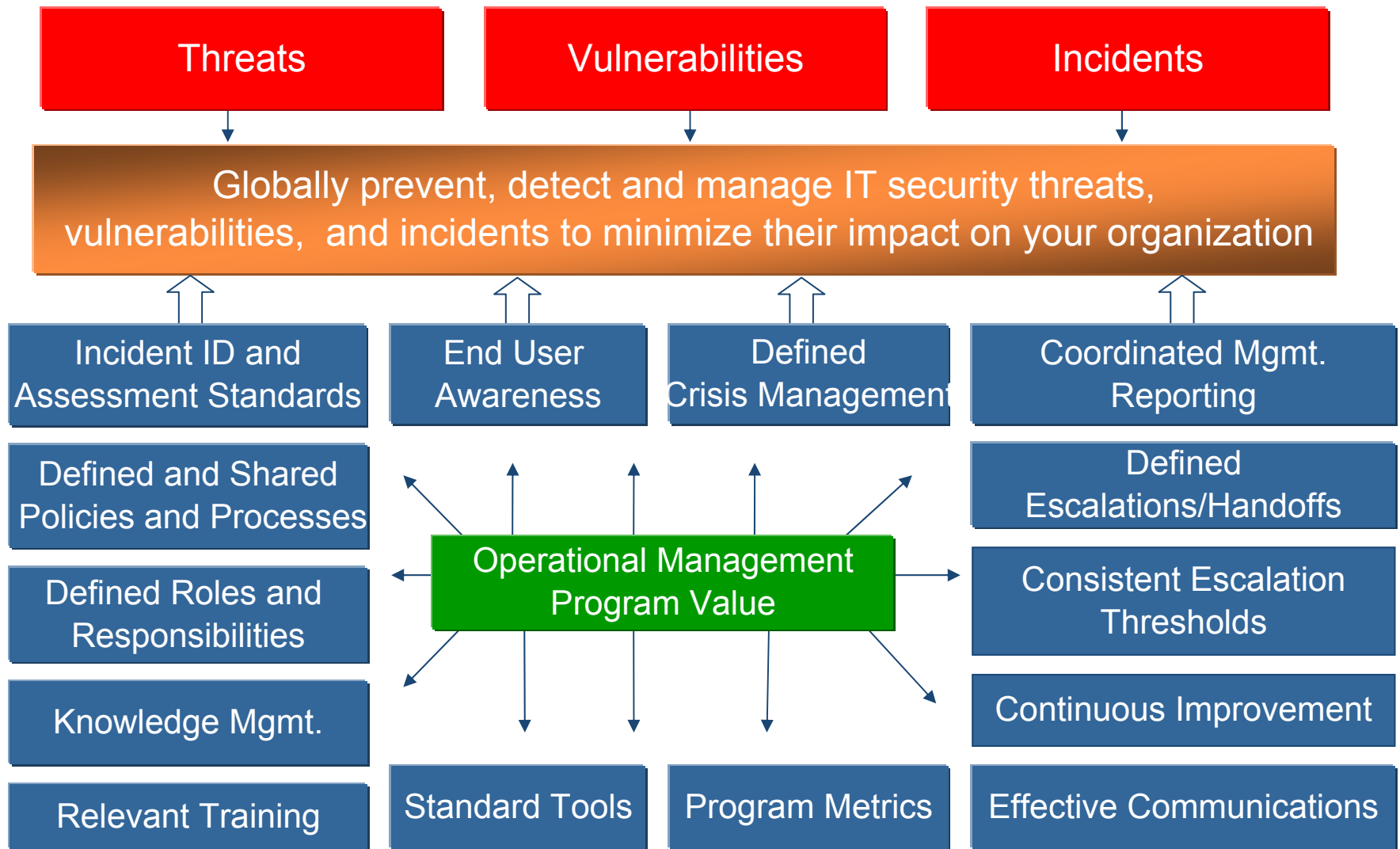


Ideal Attack & Response Timeline



**Small amount of
Danger time**

Operational Management Program Value



Operational Security Management

Information Flow



Employees **Management**
Customers **Businesses**
Vendors **Functions**

STAKEHOLDERS

Information Security	Public Relations
Physical Security	Legal
Information Technology	Help Desk
Privacy	Operations
Audit	Global Network Operations
Communications	HR / ER

PARTNERS

Citizens
 Law Enforcement
 Intelligence Sources
 Third-parties

OTHER



Functional Area's

Threat Analysis
Vulnerability Detection
Malware/AV
Compliance
Incident Response Team
Counter-measures
Investigations & Forensics
IDS/IPS
Security Operations, Escalation & Crisis Management
Program Administration & Analysis
Monitoring & Reporting
Program Rollout & Awareness



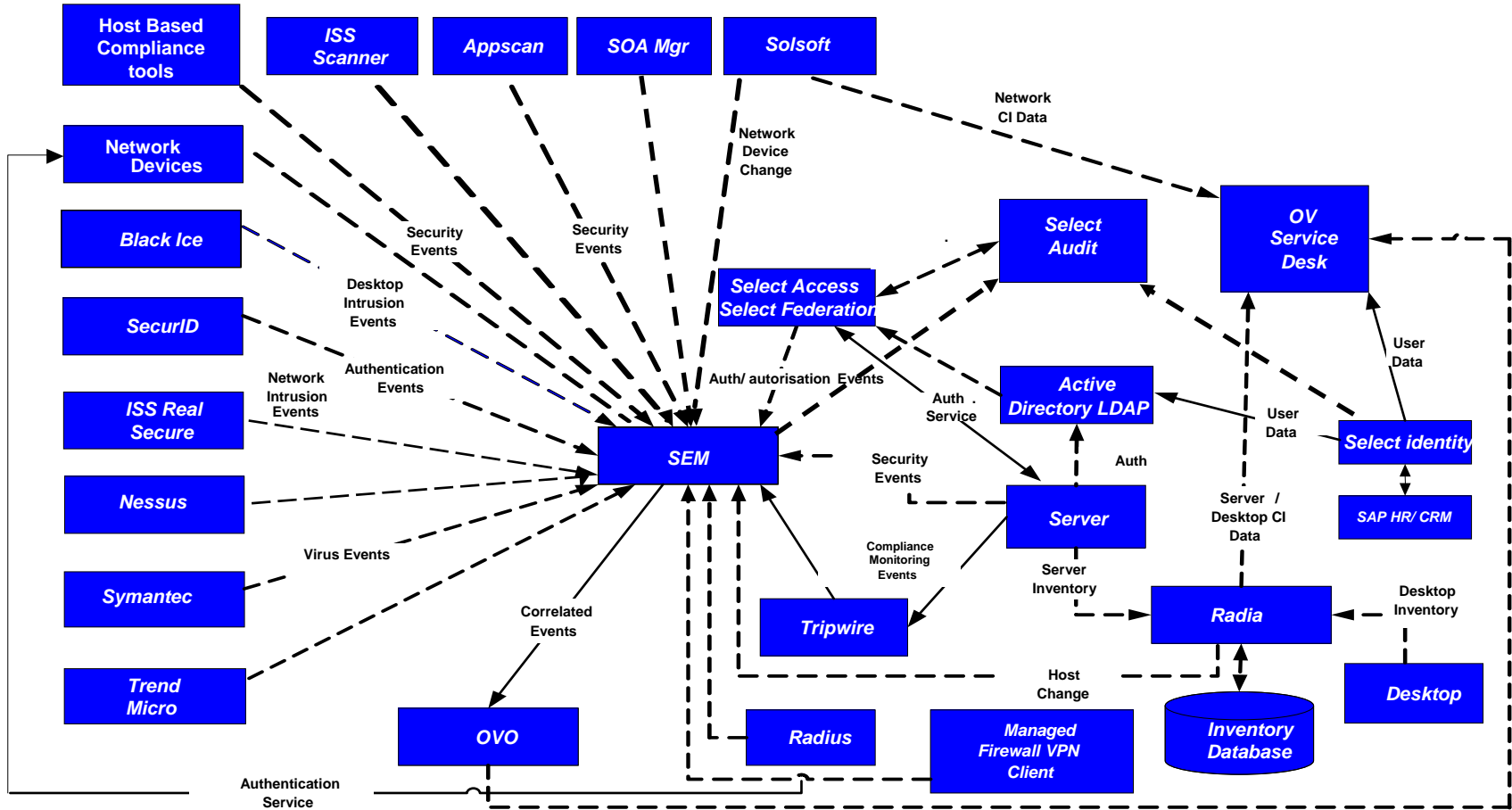
Corporate Crisis Management Team



IT & Information Security Management Teams



Security Management Technical Architecture

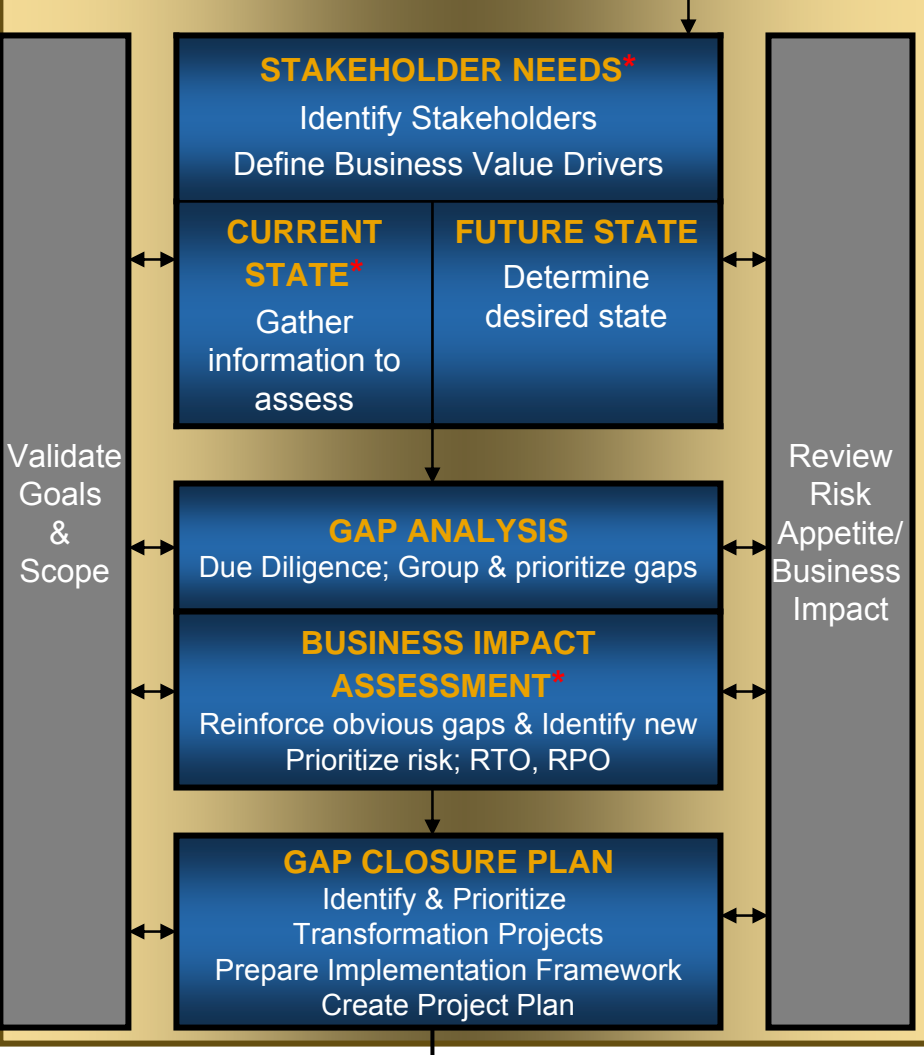


Security Incident Management Consulting

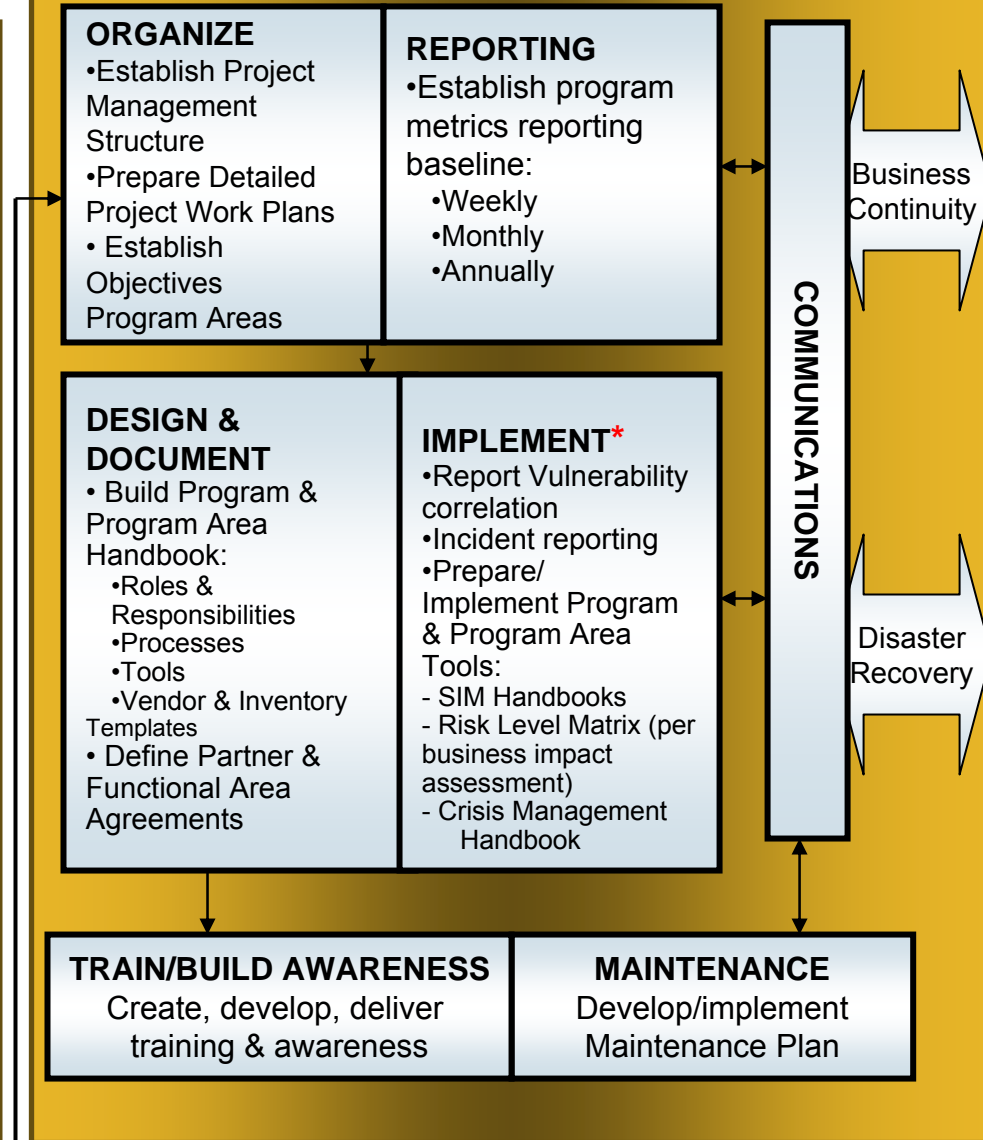
STATEMENT OF WORK

Create Goals & Scope; Gather information in Planning Meetings

PHASE 1 – ASSESS & PLAN



PHASE 2 – DESIGN & IMPLEMENT

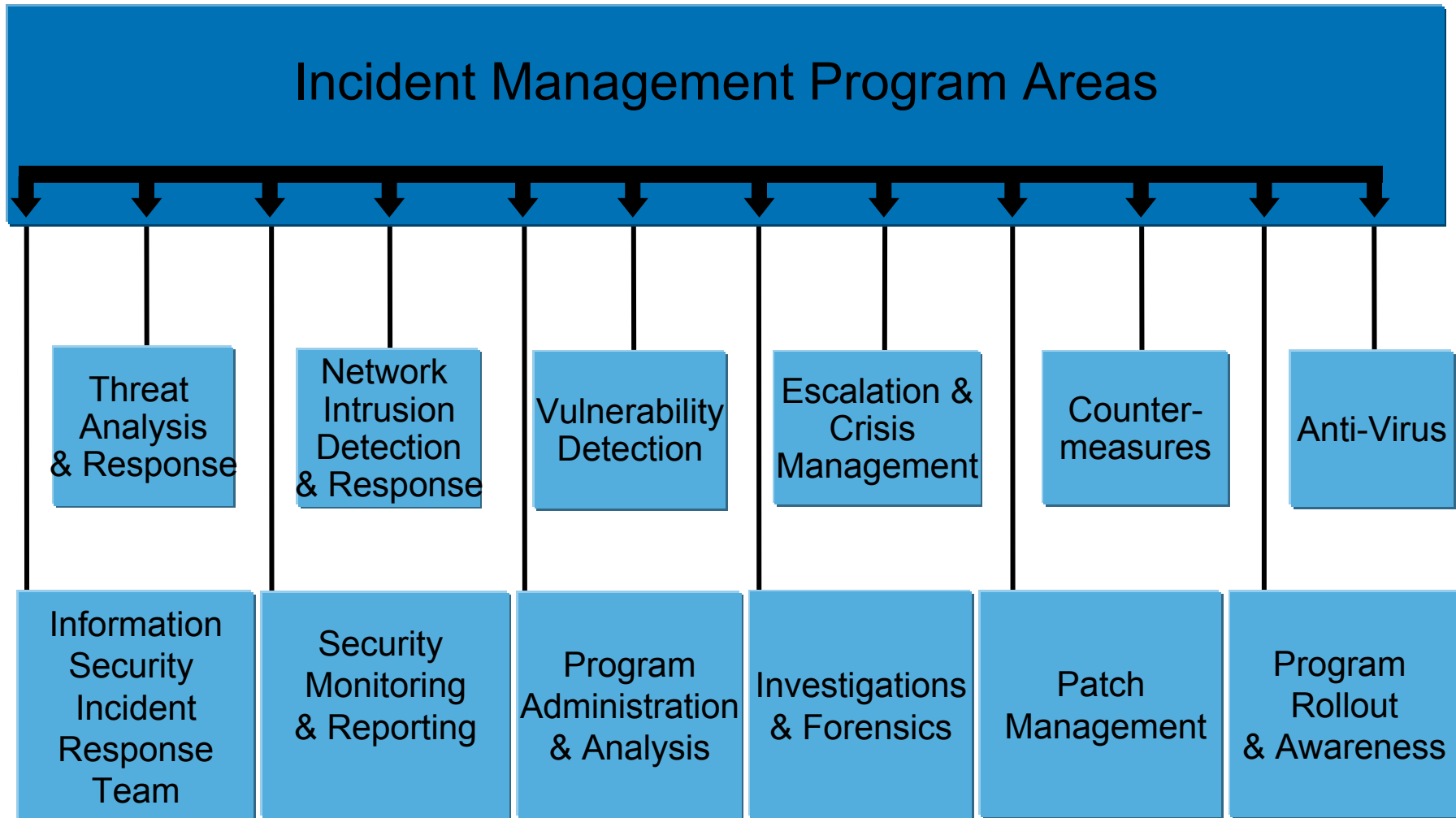


* Incident Cost Calculator may be used in pre-sales and as indicated.

ORANGE CAPS = Report/Deliverable

RTO: Recovery Time Objective **RPO**: Recovery Point Objective

Incident Management Program Components



Threat Analysis and Response

The Threat Analysis and Response Team:

- Proactively researches and monitors security-related information to identify information security threats that may impact your organization
- Threats are analyzed for their impact to your organization and assigned a risk classification
- Informational alerts and remediation requirements are developed and distributed to the appropriate parties throughout your company
- This process ensures threats are consistently addressed in a timely manner throughout the enterprise

Network Intrusion Detection and Response



The Network Intrusion Detection and Response Team:

The Network Intrusion Detection and Response Team:

- Proactively monitors the Internet-facing infrastructure for signs of network intrusions and other anomalous activities, traffic, etc. This involves ensuring that network intrusion detection sensor (IDS) alerts are properly addressed.
- Assists the Information Security Incident Response Team (ISIRT) in addressing detected attacks in real time
- Works in close cooperation with the Infrastructure Network Team related to the deployment and tuning of network-based intrusion detection sensors

Vulnerability Detection

The Vulnerability Detection Team:

- Conducts regular ongoing vulnerability scans/probes of the Internet-facing infrastructure to identify key high-risk vulnerabilities
- Provides vulnerability data to the Information Security Incident Response Team (ISIRT) so that the vulnerabilities are addressed
- Conducts “special request” scans of the infrastructure
- Rescans vulnerable systems to assess remediation status
- Assists in the management of exception requests related to vulnerability remediation

Escalation & Crisis Management

The Information Security Escalation & Crisis Management Team:

The Information Security Escalation & Crisis Management Team:

- Prepares for and addresses those unique information security-related incidents that are anticipated to cause significant impact or have caused enterprise-wide severe impact or interruption.



Countermeasures

The Information Security Countermeasures Team:

- Conducts regular and targeted scanning for specific critical information security vulnerabilities and/or compromised systems
- Delivers a customized payload to the impacted system which results in the mitigation of the vulnerability and/or the remote shut-down/disabling of the impacted system

Anti-Virus

The Information Security Anti-Virus Team:

The Information Security Anti-Virus Team:

- Plans and implements the company's AntiVirus strategy (e.g., choice of tools, tool deployment, etc.)
- Obtains and tests new versions of AntiVirus tools when they are made available
- Facilitates the communication of AntiVirus strategy, directions and tools available



Information Security Incident Response Team (ISIRT)



The Information Security Incident Response Team (ISIRT):

The Information Security Incident Response Team (ISIRT):

- Is a global team with corporate-wide responsibilities pertaining to receiving, assessing, responding to, addressing and managing information security incidents
- Depending on the severity of incidents, ISIRT will own, hand-off, address, or escalate security incidents, thus ensuring incidents are handled commensurate with their level of risk

Infosec Security Monitoring and Reporting



The Information Security Monitoring and Reporting Team:

The Information Security Monitoring and Reporting Team:

- Monitors patching compliance related to high-risk vulnerabilities for internal systems where these conditions can be remotely detected
- Works closely with regional and business security teams, IT delivery teams, and other teams within Information Security and the Information Security Incident Management Program.

Program Administration and Analysis



The Program Administration and Analysis Team:

- Collects, consolidates, analyzes and provides specific audience-based reports related to the functional programs within the Information Security Threat, Vulnerability and Incident Management Program
- This Team also conducts strategic planning and budgeting and leads the program/project management and maintenance activities within the Program.

Investigations and Forensics

The Information Security Investigations & Forensics Team:

The Information Security Investigations & Forensics Team:

- Addresses serious information security related incidents which involve civil, criminal, administrative, disciplinary, brand and/or financial implications
- Works closely with internal partners such as Legal, HR/ER, Media Relations and Security and external parties such as law enforcement and government authorities
- Has ability to recover, decrypt, and analyze IT-related data and report, present, and represent such data in civil, criminal, and administrative proceedings

Patch Management

The Information Security Patch Management Team:

- Works in conjunction with Threat Analysis and Response and Vulnerability Detection program areas
- Provides system owners with remediation information related to high-risk vulnerabilities affecting the company's infrastructure
- Creates weekly reports which track number of vulnerable systems detected and number of systems remediated

InfoSec Program Rollout and Awareness



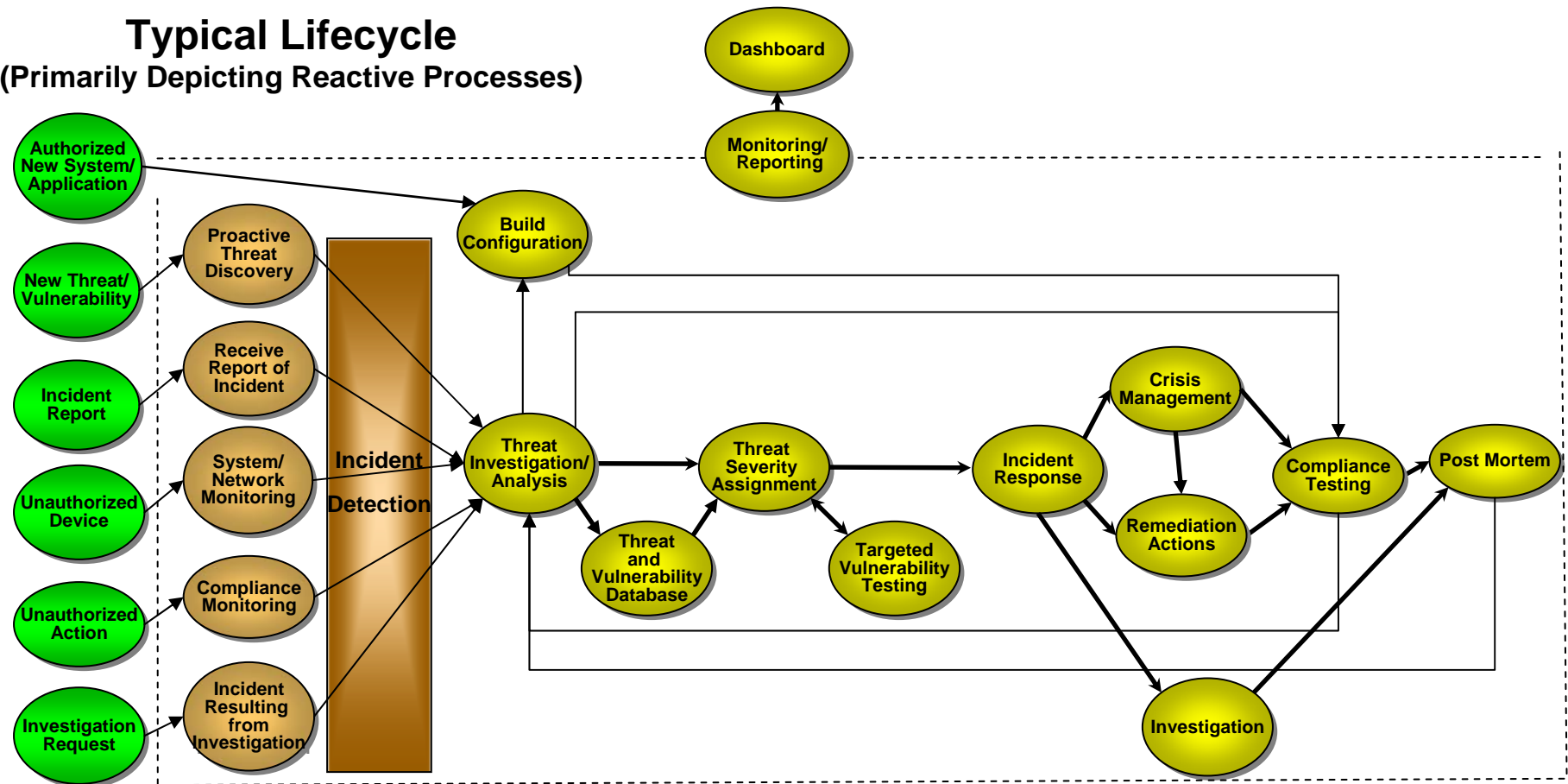
The Information Security Program Rollout and Awareness Team:

The Information Security Program Rollout and Awareness Team:

- Develops and delivers end-user and partner-focused communications and awareness activities to increase understanding, use of, and compliance related to the Information Security Threat, Vulnerability and Incident Management Program.

Typical Lifecycle

(Primarily Depicting Reactive Processes)



Triggers	Incident Initiation	Incident Management		
Intrusion Detection				
			Crisis Mgmnt	
Vulnerability Detection				
			Investigations & Forensics	
Threat Analysis				
Anti-Virus		Incident Response Team		
Countermeasures			Countermeasures	Countermeasures
Compliance Monitoring				
Monitoring and Reporting				
Program Administration & Analysis				
Program Rollout & Awareness				

Information Security Incident Management Program



Incident Management Tools

- An effective Incident Management Program requires specific tools be developed. Examples include:
 - Security Incident Cost Calculator
 - Risk Assessment Matrix
 - Crisis Management Manual
 - Incident Management Handbook
- Each tool must be customized for the specific business structure and IT infrastructure of a given company
- It is difficult for a company to develop these tools without outside help



Incident Management Tools

Security Incident Cost Calculator

Incident Management Program Per Incident Cost					
Instructions - Please fill in all fields highlighted in yellow.					
	Total	Totals by System Administrator			
		AP	Japan	EMEA	Latin America
Productivity Loss					
# of Servers Affected					
Average # of Hours of Server Downtime					
Average # of Users on Server During This Time					
# of Clients or PCs Affected					
Average # of Hours of Client or PC Downtime					
Average # of Users on Clients or PCs During This Time					
# of Employees Reading Messaging					
# of Hours Reading Messaging per Employee					
# of Employees Required to Perform Actions					
# of Hours Implementing Required Actions per Employee					
Hourly Rate per Employee					
Productivity Loss Subtotal	#VALUE!	#VALUE!	#VALUE!	#VALUE!	#VALUE!
Call Center Costs					
# of Support Calls	0				
Average Length of Call (in Hours)	0				
Cost per Call or Hour					

Considerations for calculating the cost of security incidents



Know your downtime cost: per hour, per day, per Business Unit...

Productivity

- Number employees impacted x hours out x burdened hours =

Revenue

- Direct loss
- Compensatory payment
- Lost future revenues
- Billing losses
- Investment losses

Financial performance

- Revenue recognition
- Cash flow
- Payment guarantees
- Credit rating
- Stock price

Damaged reputation

- Customers
- Suppliers
- Financial markets
- Banks
- Business partners



Other expenses

- Temporary employees
- Overtime & travel costs
- Equipment rental
- Extra shipping expenses

Incident Management Tools

Risk Assessment Matrix

- A Risk Assessment Matrix provides a quick and consistent way to evaluate the risk severity of an information security threat, vulnerability or incident. It standardizes escalation triggers, thresholds and actions across the Incident Management Program.
- The Risk Assessment Matrix serves as a strong guideline for the initiation of a crisis or escalation and contains a series of metrics to help users identify the level of escalation. Scores are assigned in the areas of:
 - The likelihood of an information security threat, vulnerability, or incident impacting the IT Infrastructure and
 - The potential impact if the threat, vulnerability, or incident begins to impact the IT Infrastructure (including, but not limited to brand, financials, employees, customers, data/information loss, etc.)

Incident Management Tools

Crisis Management Manual

- The Crisis Management Manual is a tool to assist on-call crisis managers in the event of an Information Security related crisis.
- The Manual creates a standard process for managing high-profile incidents to ensure an immediate, appropriate, and consistent response to a geographic or worldwide crisis situation. This enables the Crisis Manager to take control of the crisis environment and manage the flow of information to most effectively protect the organization
- In addition to aiding the Crisis Manager, the Manual contains tools, templates, flow charts, checklists and processes and outlines the responsibilities of other critical parties in the management of a crisis

Incident Management Tools

Incident Management Program Handbook

- The Handbook is a tool utilized by all members of the Incident Management Program. It contains all job descriptions, roles and responsibilities, processes and tools documentation for each of the Program components.
- The Handbook provides a standard, easily accessible repository for securing all important Program documentation which lends consistency and stability to the IM Program.
- The Handbook is primarily utilized in a virtual manner with all documents undergoing regular scheduled review and update