



# **CYBER INCIDENT MANAGEMENT**

## **A PROCESS-DRIVEN APPROACH WITH AN INTEGRATED “TRAIN-IN-PLACE” CYBER DRILL AND EXERCISE CAPABILITY**

Presented to the  
**7<sup>th</sup> Annual**  
**GFIRST National Conference**

by  
Brian Zaas, Avineon  
Chris Fogle, Delta Risk

August 10, 2011



**AVINEON**<sup>®</sup>

**DELTA RISK**<sup>®</sup>

- Over 19 years delivering comprehensive IT services & solutions
- 1,200+ employees worldwide
- CMMI Maturity Level 3 and ISO 9001:200 registered

- Supporting DoD, DHS & Federal Agencies, commercial clients world-wide
- Network of highly qualified consultants
- Focus on *People* and *Process* in the cybersecurity equation

**Brian Zaas**  
Enterprise Solutions

**Chris Fogle, CISSP**  
Partner

# Operational View

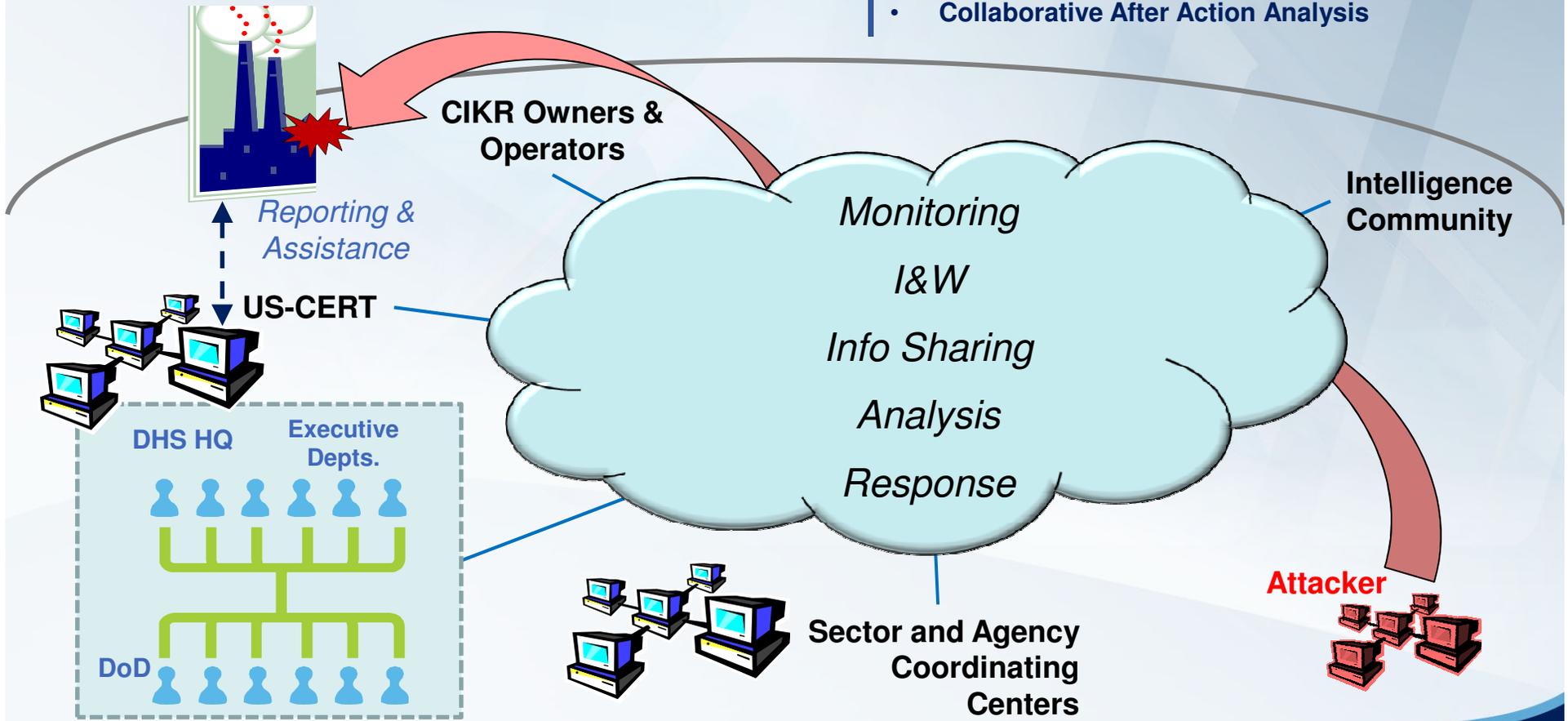
## Coordination and Response to Cyber Incidents



**The Cybersecurity Challenge:**  
*Coordination and Information Sharing among Agencies and Communities of Interest (COIs)*

### Information Sharing among Agencies (COI's)

- Simultaneous Operations
- Joint Analysis of Activities
- Command and Control of the Response
- Distributed Monitoring of the Situation
- Horizontal and Vertical reporting
- Collaborative After Action Analysis





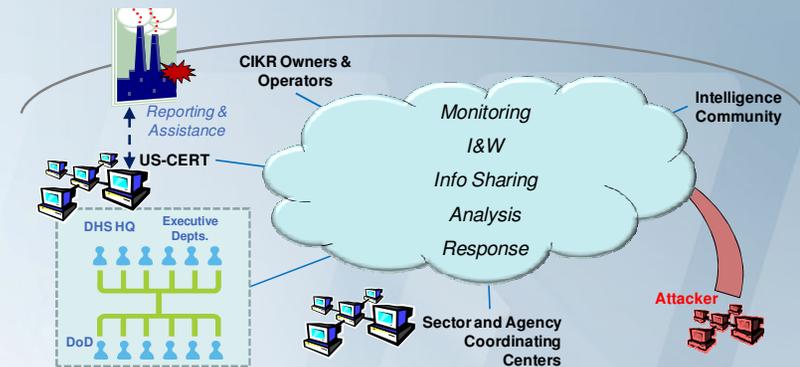
## COLLABORATION



- **“Severe” Threat Level**
  - Multi-stakeholders
    - Federal government agencies
    - State government agencies
    - Local government agencies
    - Private sector organizations
    - International partners
  - Widely distributed operations
  - Managing interdependencies
- **Plans and Processes**
  - Joint Incident Action Plans
  - Mitigation Actions



## What does “experience” suggest it takes to respond and manage effectively?



**Technology-aided** – speeds response and manages complexity

**Connectivity** – widely distributed and diverse operations

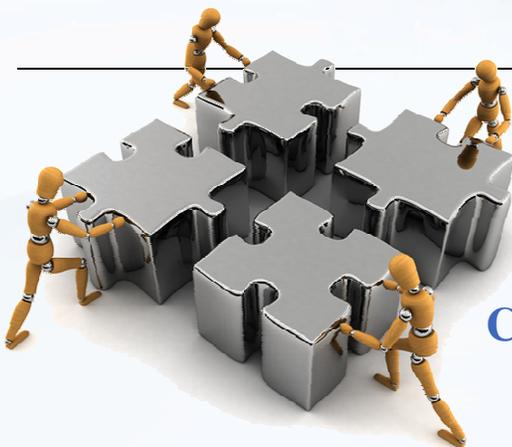
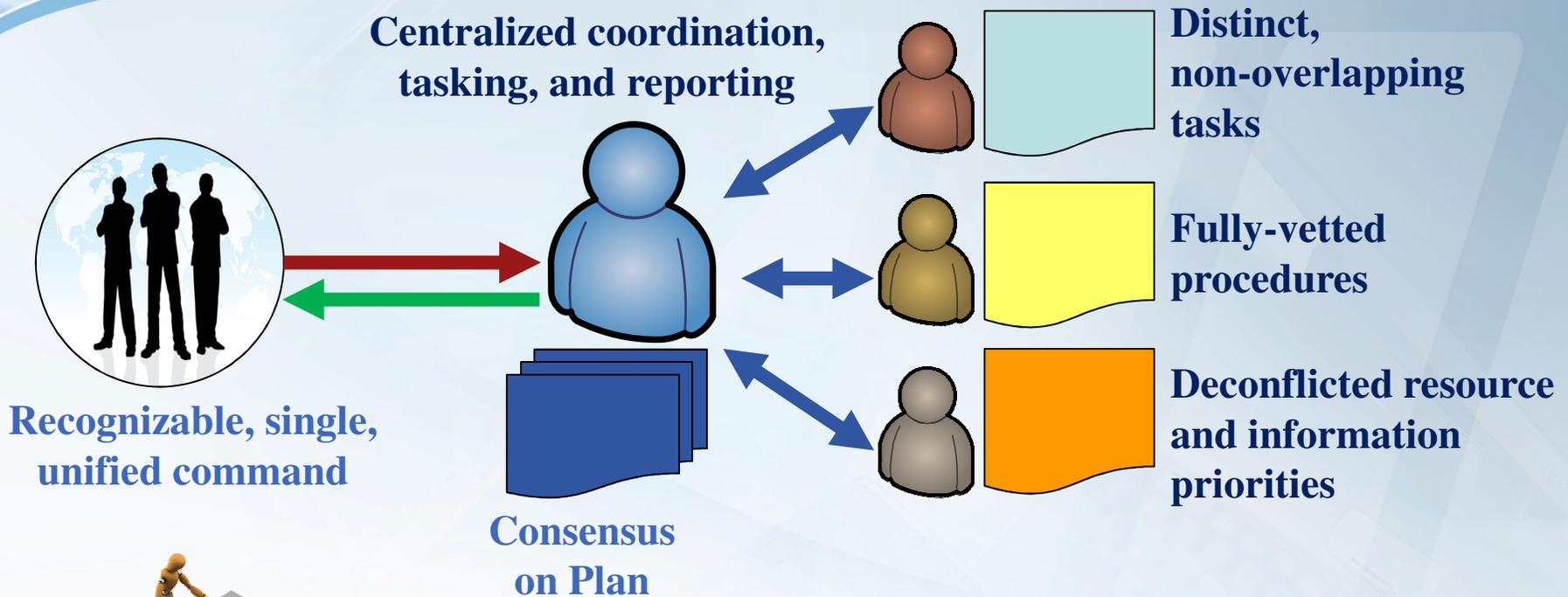
**Authorities** – clearly defined for decision making

**Visibility & situational awareness** – includes tracking and tracing of actions; access to plans and procedures

**Collaboration** – on planning, information sharing, and analysis

**Flexibility & extensibility** - easily handles “discovery” and dynamic changes to process, players, and activities

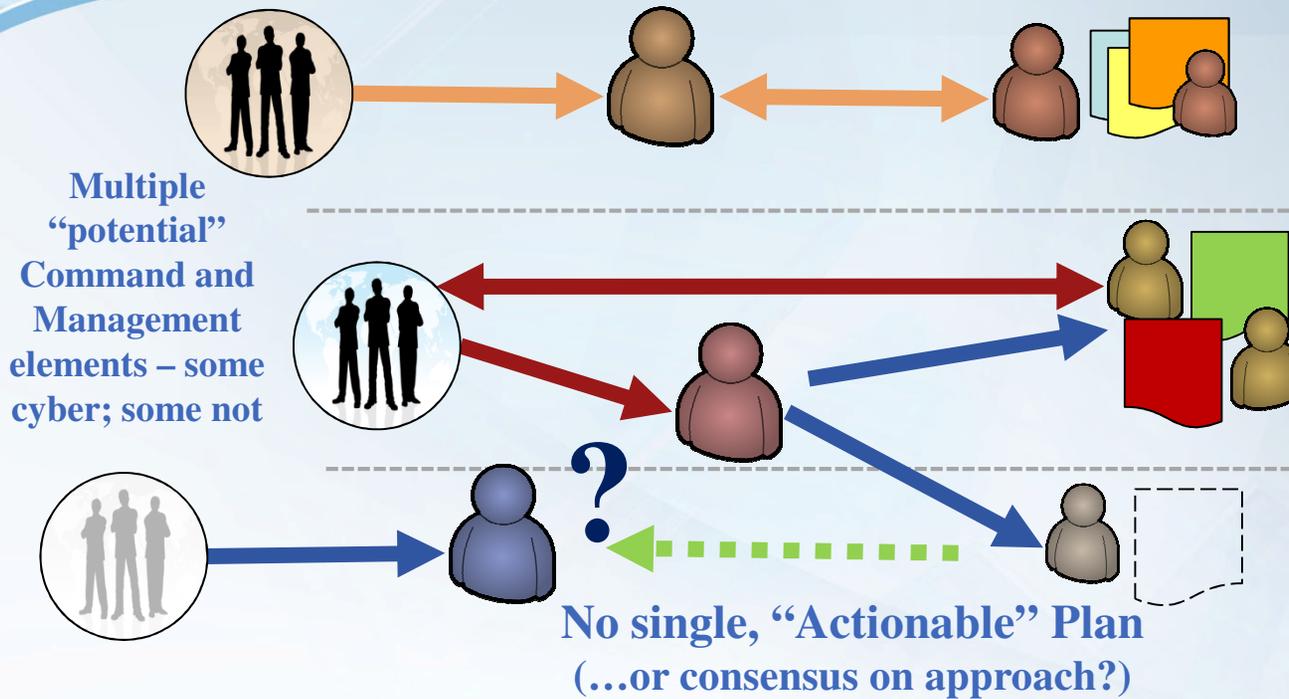
**“System Memory”** – resilient processes, campaign perspective, ability to leverage lessons learned



**Collaborative analysis**

**... and of course,**

- Assured attribution
- “Non-advanced and non-persistent” threat
- Interoperable tool suites & data sources
- Fully tracked metrics
- Immediate feedback & process improvement

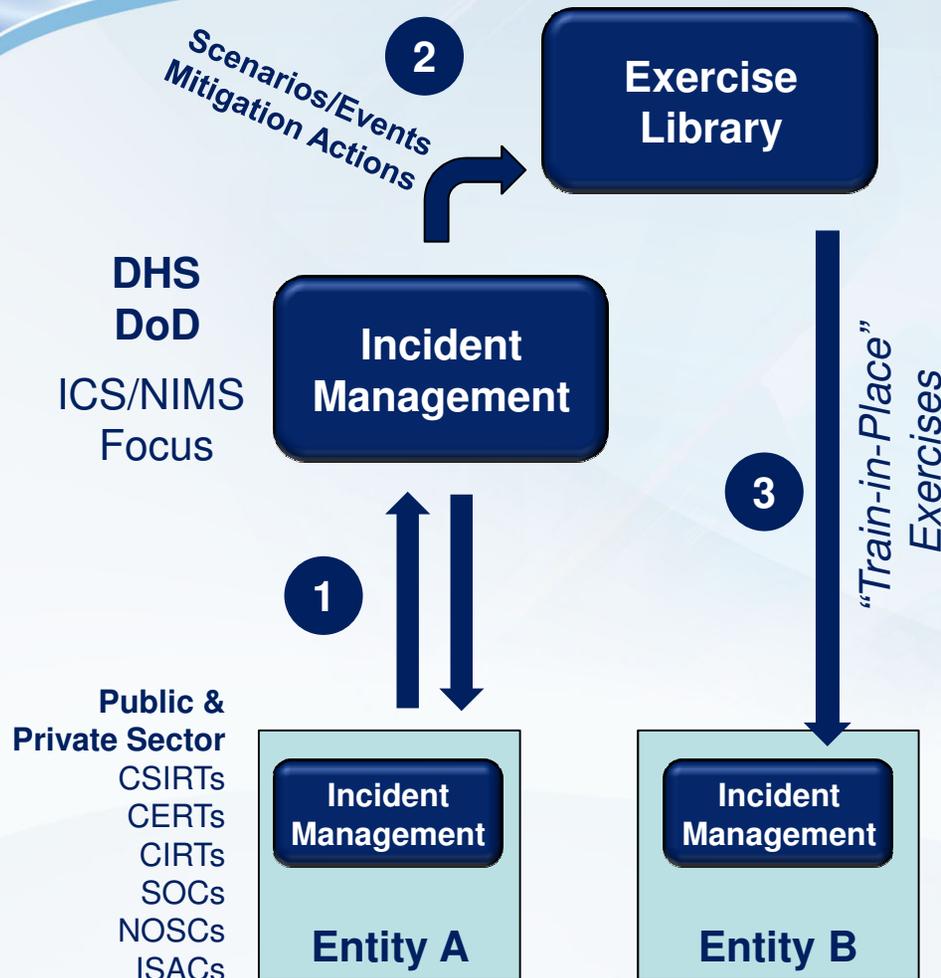


- Ambiguous tasking
- Conflicting and incomplete procedures
- Reliance on “walking corporate knowledge”
- High-maintenance planning and coordination “process”
- Disparate testing

## ... and of course,

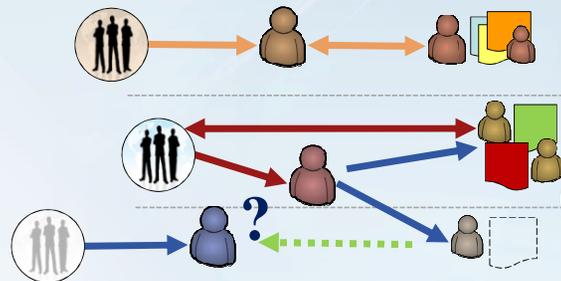
- Persistent “unknown” adversaries
- Various tools, protocols & classifications
- Ad-hoc performance indicators
- “Bit Bucket” approach to feedback and process improvement





## CONTINUOUS IMPROVEMENT

- **Processes**
  - What, When, Who
- **Process Automation**
  - ✓ Warnings
  - ⇒ Common Objectives
  - ⇒ Mitigation Actions
  - ⇒ Status Reporting
  - ⇒ After Action Reporting

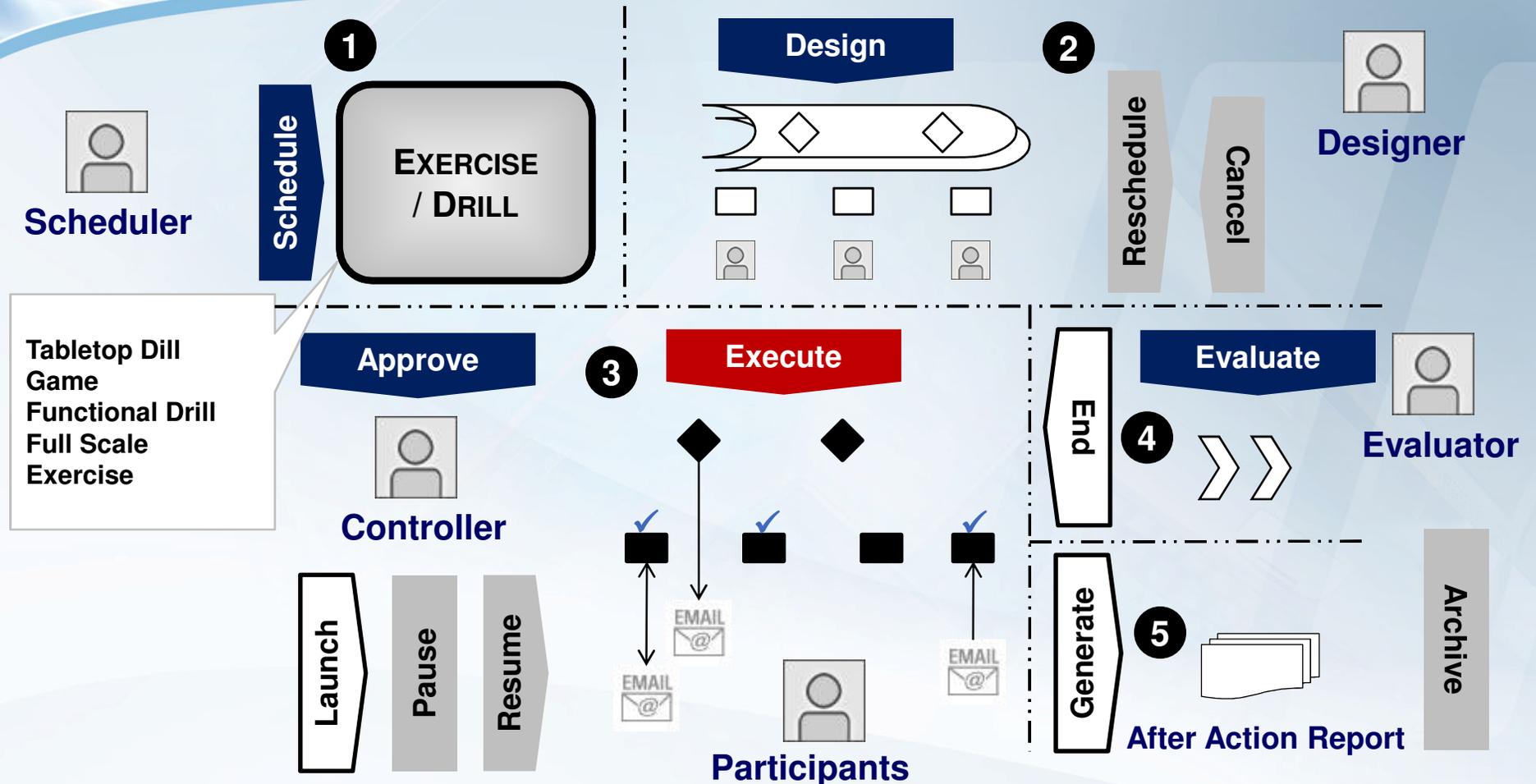


What does this mean for a cyber incident response organization (CSIRT, CERT, NOC, SOC, ... others)?

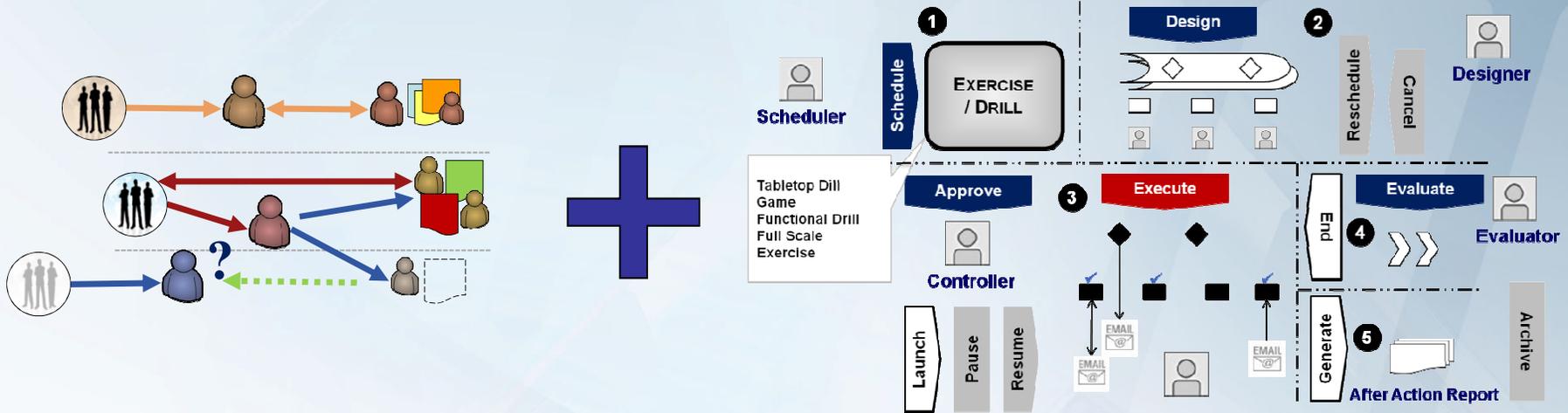
- ✦ Establish and maintain critical processes and communications
  - Define key response processes up front as part of a broader *planning* and *risk analysis* effort
  - Enforce their use during incident response using automated checklists and access to reference contingency plans
  - Facilitate use of metrics – in near-real time – including total exposure, readiness, and incident management ... “*dashboards*”
- ✦ Reinforcement with/through a program of regular, in-place cyber drills and exercises
  - *Same interfaces ... same processes*

# Exercises and Drills

## Concept of Implementation



<b>Scenario</b>	<b>Event/Injects</b>	<b>Tasks</b>	<b>User</b>	<b>Corrective Action</b>
Day 1 Day 2	Intrusion @ 8:14 AM Virus Attack @ 8:23 AM	Declare NCRAL Level Complete Mitigation Action	John Doe Sally Mae	Update Procedure Implement Intrusion Detection



## Core Capabilities

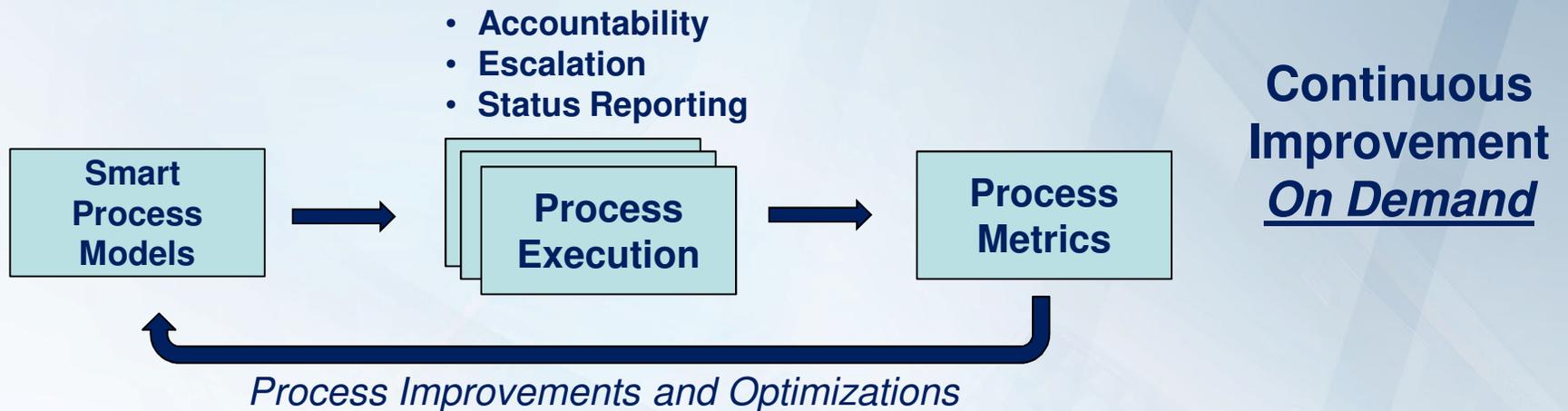
- Role assignments with backups
- Competency management
- Activity logs (Human Action Documentation)
- Access to underlying reference contingency plans
- “Exercise Mode”

## Process Areas

- Task / response management
- Communications management
- Resource management
- Planning & collaborative analysis



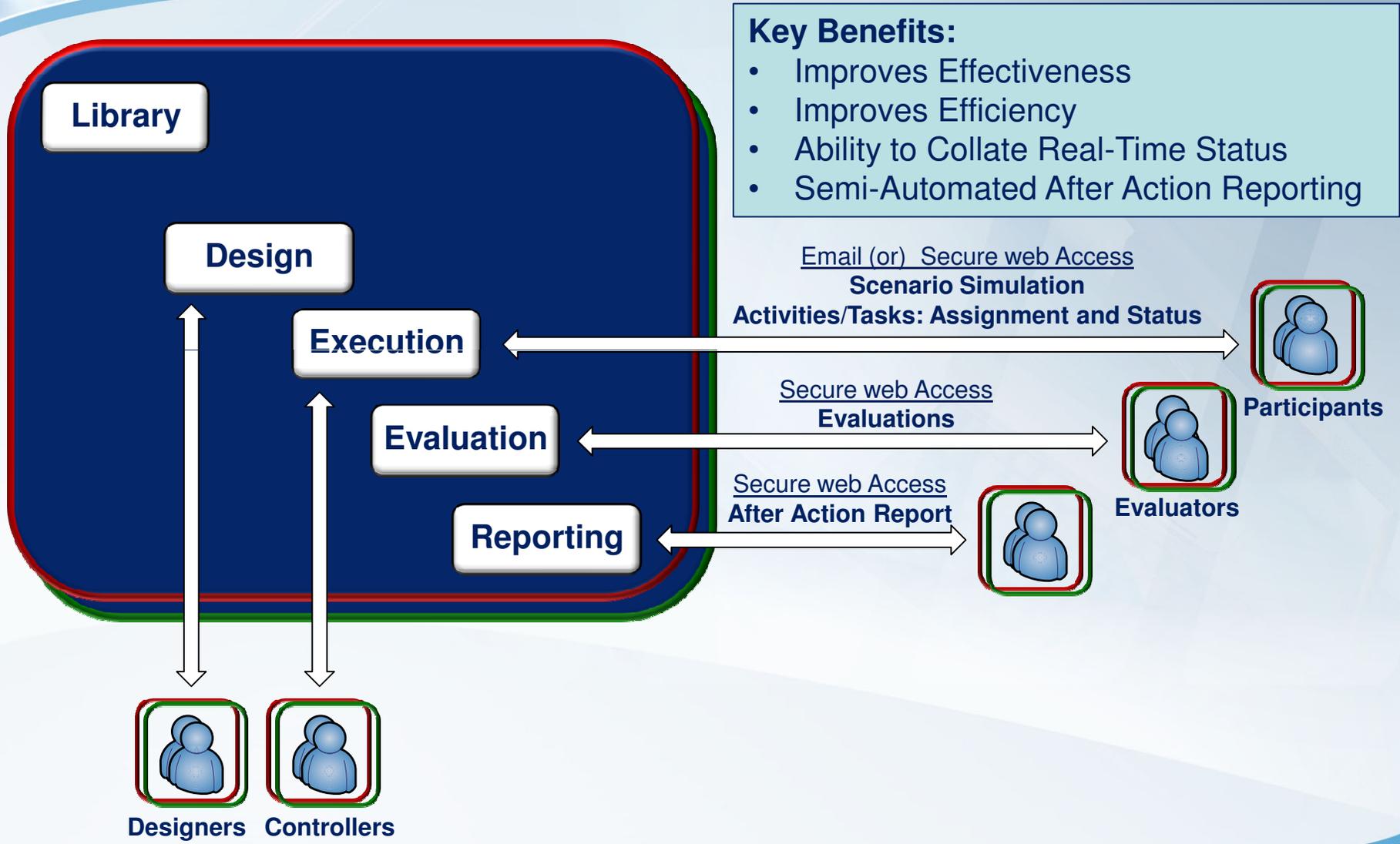
- **Process Driven Approach**



- **Traditional Approach**

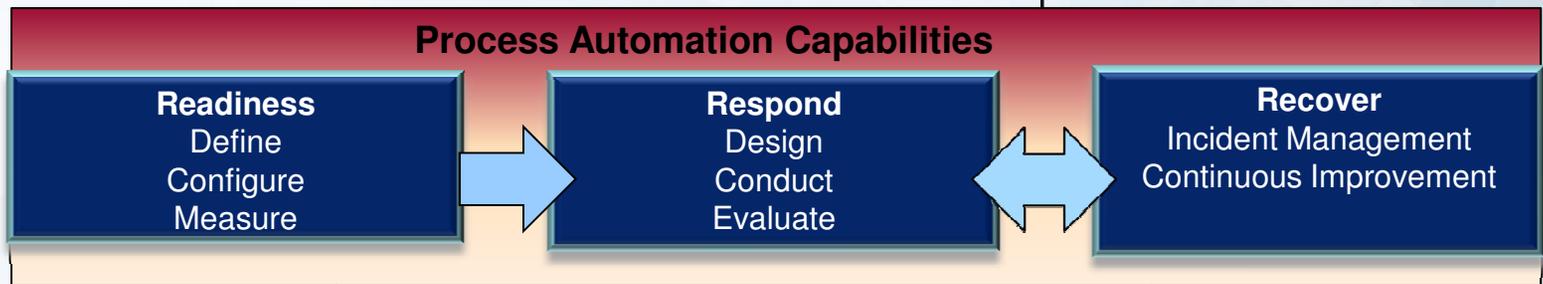
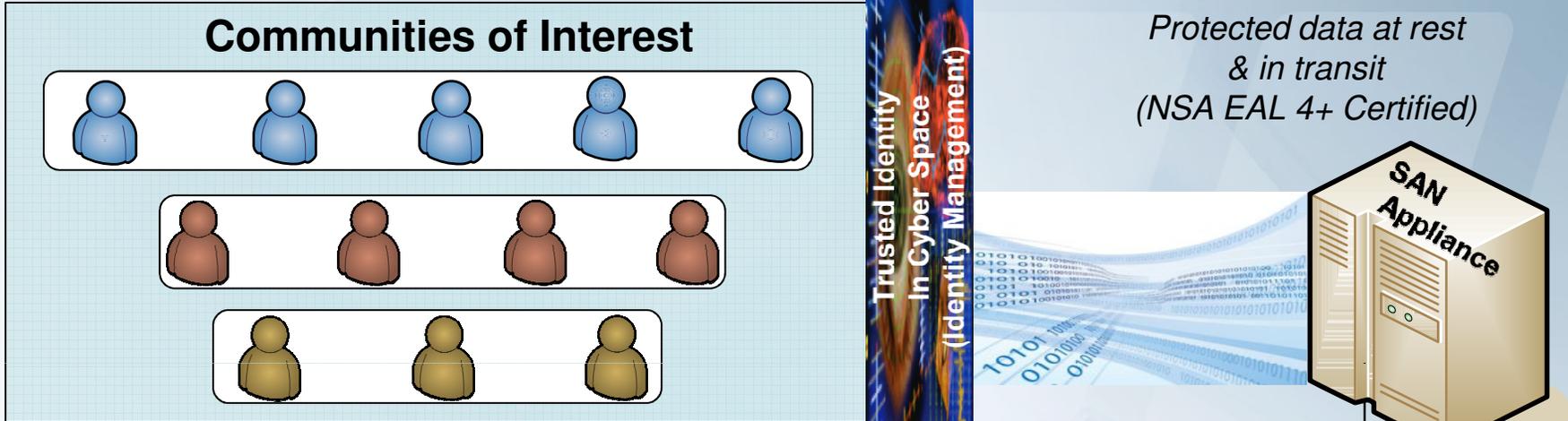
- Written plans, procedures, checklists
- Practice and test using exercises
- Improve based on lessons learned

Continuous Improvement  
Once a Year



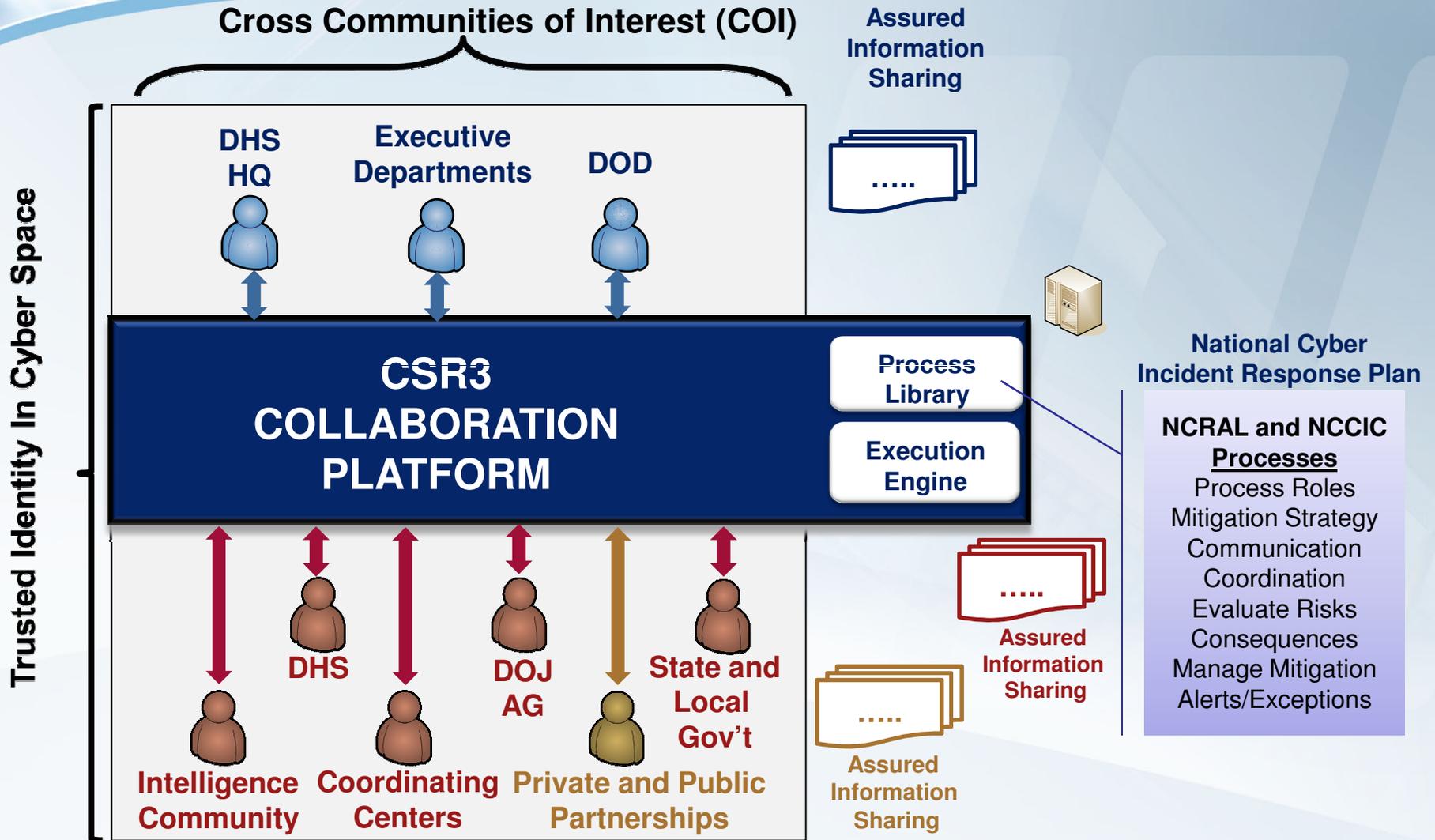


... as instantiated in the Avineonics CSR3 platform



**SIEM - Sensors – PSIM – Mst Tools**

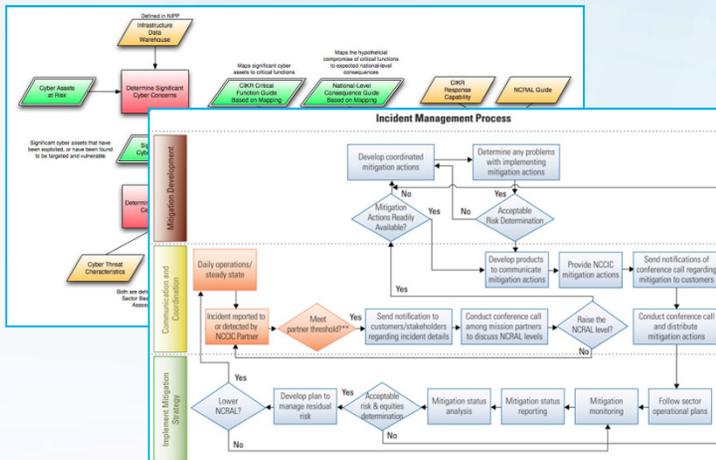
Cyber - IDS - Physical – Personnel – IT – Environmental – Video - Policy – Wireless – Operational – Terrorist



## NCRCG Collaboration

**NCRAL: Joint Decision Support**

**NCCIC: Incident Management Process, etc.**



## Process Areas

- Operations
- Watch & Warning
- Analysis
- Planning
- Assist & Assess
- Liaison

## Process Driven Approach

### • Process Adherence and Automation

- Who, What, When
- Collaborations
  - Process Initiation
  - Task Assignments
  - Information Sharing
  - Mitigation Actions and Status
  - Escalations and Exceptions
  - Status Consolidation
  - Status Reporting
- Situational Awareness

### • Process Metrics

- Task Durations
- Process Durations

### • Process Integration

- Boundaries and Triggers

*Across Public, Private and International Partners*



http://em.avineon.net/suite/process/startdesigner.none?idToOpen=5770

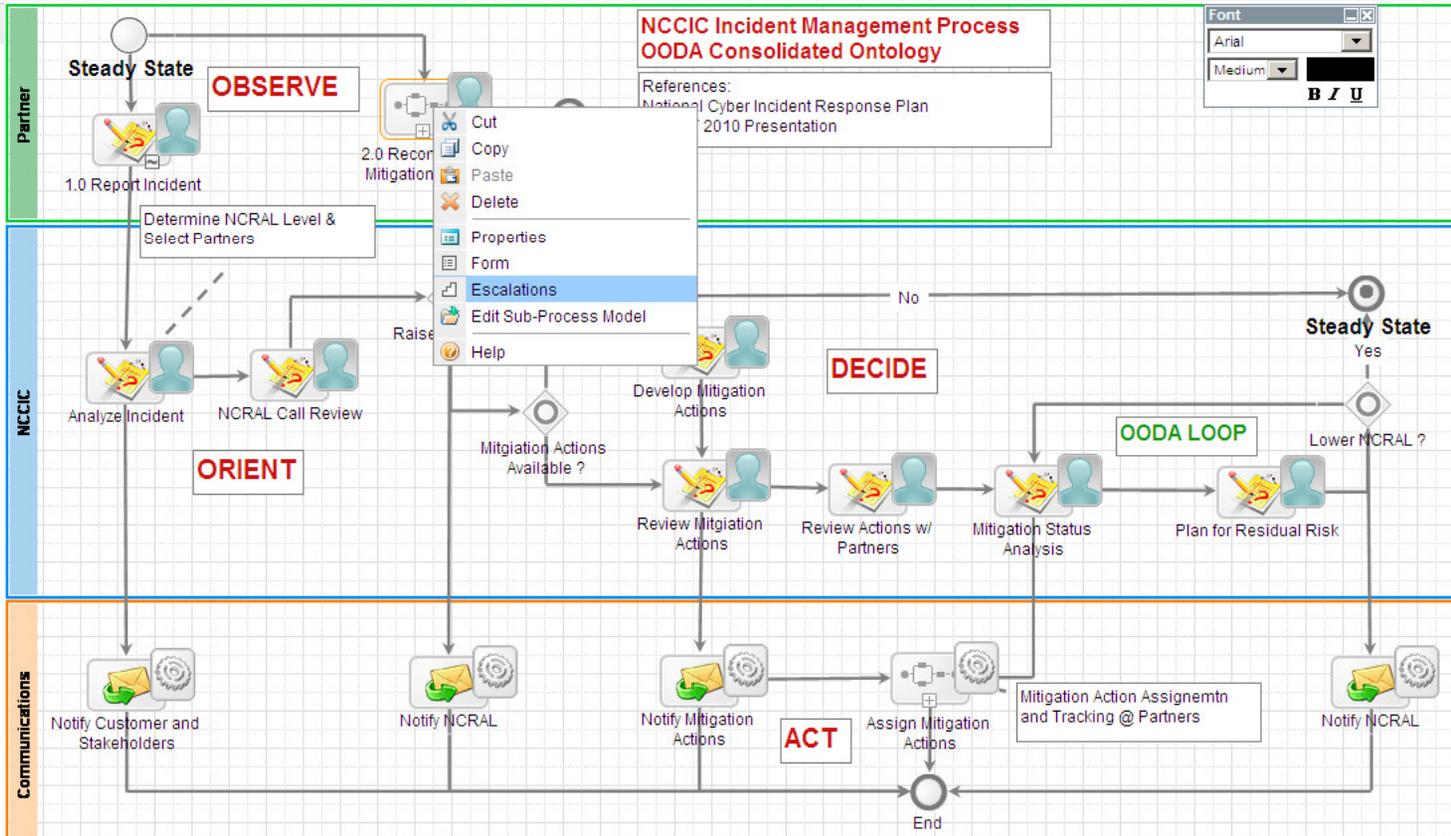
## Apian Process Modeler

File Edit View Tools Lanes Simulation Help

100%

Palette

- Standard Nodes
- Events
- Activities
- Gateways
- Apian Smart Services
  - Document Management
  - Forum Management
  - Portal Management
  - Identity Management
  - Process Management
  - Analytics
  - AE Administration
  - Communication
- Avineon Smart Services
  - ICS Forms
  - Action Reports
  - Incident Package
  - Action Plan
  - Validate Training
- Integration Services
  - Connectivity Services





**Configure User Input Task**

General | Data | Forms | **Scheduling** | Assignment | Escalations | Exceptions | Attachments | Notes | Other

**Scheduled Start**

Don't start this node until:

- Minute(s) after the last node completes
- The date and time specified by this expression:

**Repeat Node**

Repeat this node

Daily

Weekly

Monthly

Yearly

At an interval

Repeat this task

Every  day(s)

Every weekday

at:  =pp\timezone

**Repeat until:**

- Repeat indefinitely, or until cancelled
- instances have started
- The date and time specified by this expression:
- Expression is true:

©2003-2011 Appian Corporation

OK Cancel



Objectives

5. Incident Management

Incident: Cyber Attack 07-25-2011

1. Update | 2. Access | 3. Generate | 4. End | 5. Delete  
1. Event | 2. Strategy | 3. Objectives | 4. Operational Period

Significant Events

Response and Recovery Strategy

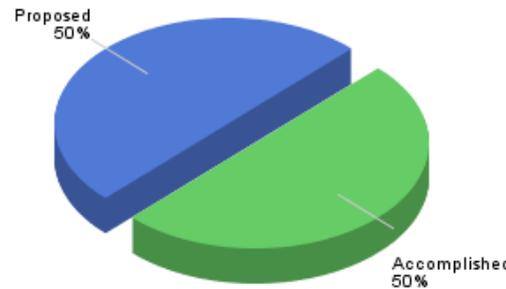
Objectives

Operational Periods

Activity Logs

Resource Requests

Demobilization Requests



- ICS 201 - Incident Briefing
- ICS 202 - Incident Objectives
- ICS 203 - Organizational Assignment
- ICS 214 - Unit Log
- ICS 215 - Operational Planning Worksheet
- ICS 215a - IAP Safety Analysis

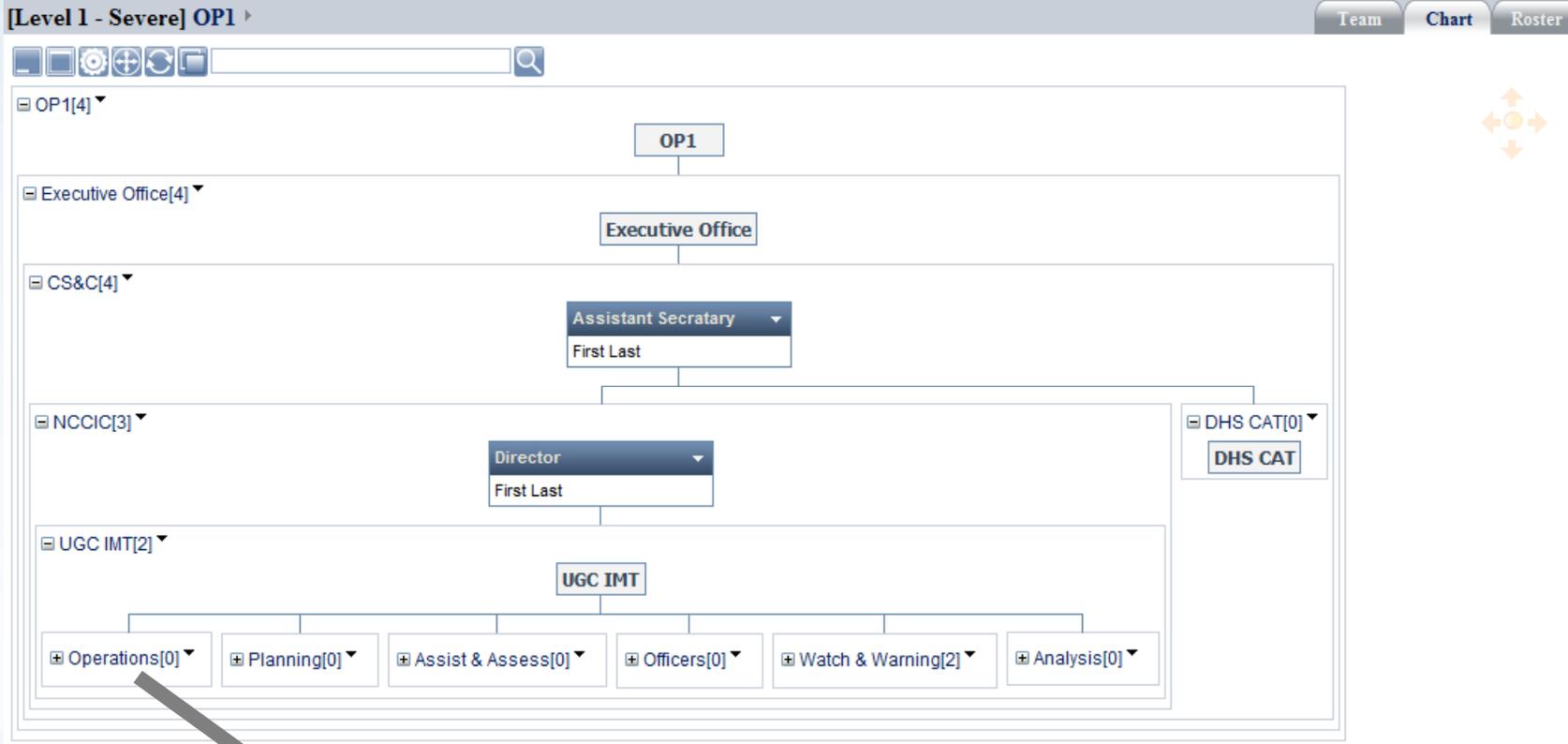
Operational Period: Cyber Attack 07-25-2011 > Cyber Attack 07-25-2011\_OP1

1. Update | 2. Delete  
3. Impact | 4. Divisions | 5. Locations | 6. Meetings | 7. Forecast | 8. Cost Estimate | Status  
10. Launch Checklists | 11. IAP | 9. Tasks

- Forecasted Impact
- Impact Summary
- Meetings Schedule
- Response and Recovery Sites and Locations
- Resource Requirements
- Task Assignments
- Checklist Assignments
- Response and Recovery Cost Estimates



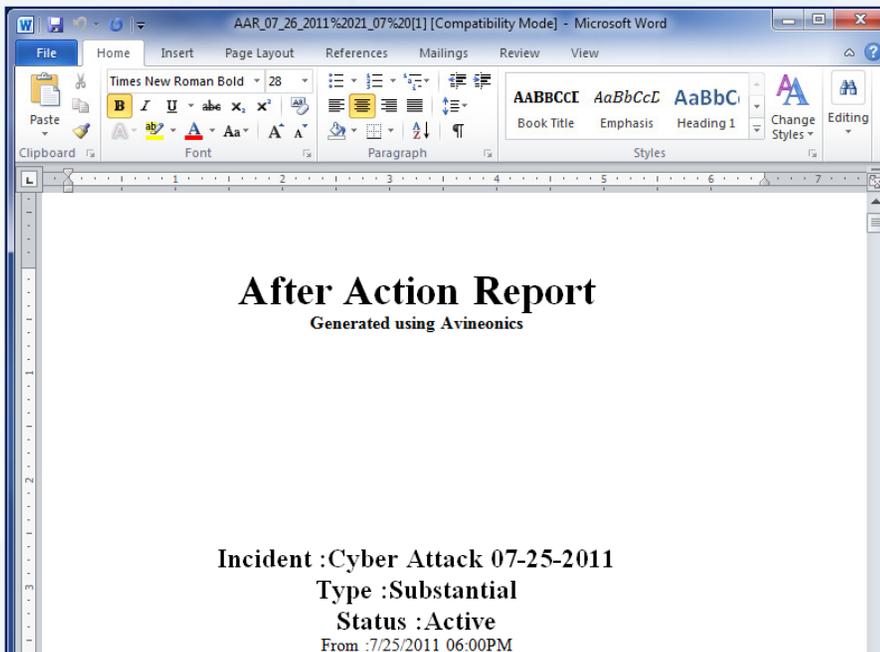
## ICS: Incident Command System



- |             |              |
|-------------|--------------|
| 1. Check In | 2. Check Out |
| 1. Transfer | 2. Log       |



## **Generate Automated Report** *Report Content by COI and Role* *Customizable Report Templates*

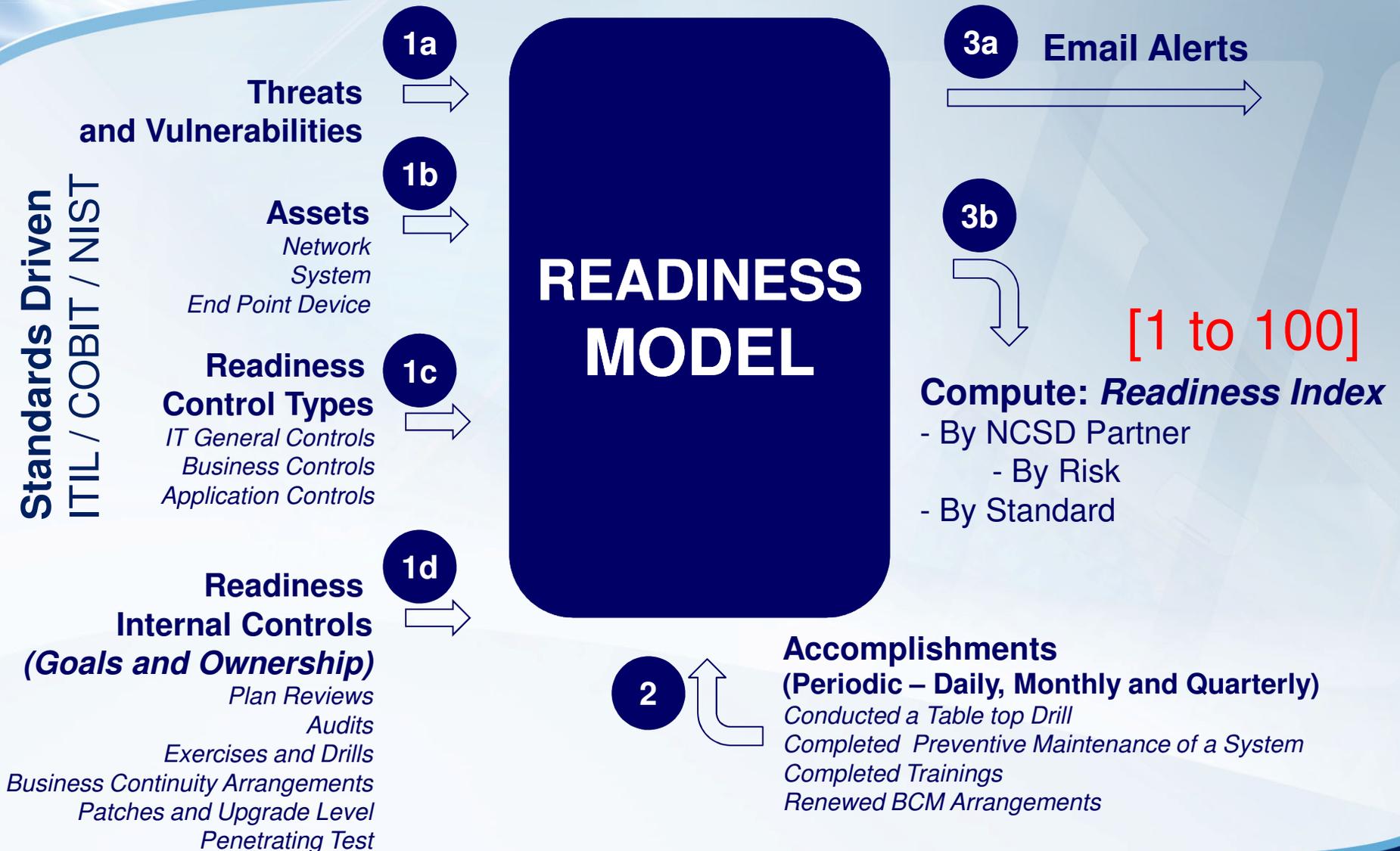


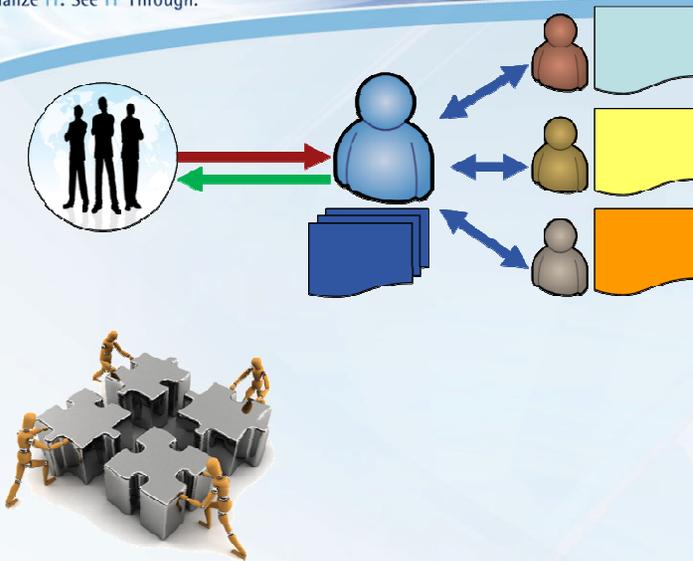
### **Table of Contents**

Section 1.0: Executive Summary  
Section 2.0: Incident Impact, Strategy and Events  
Section 3.0: Planning and Operations

Appendix A: Activity Logs

Appendix B: Personnel





Keys to maintaining a long-term, effective cyber incident management capability:

- Focus on process; not just procedures
- Use regular, frequent drills and exercises to ...
  - Instill process
  - Assess effectiveness
  - Provide confidence to staff and leadership about the capability



**Brian Zaas,**  
Enterprise Solutions  
Avineon, Inc.  
**BZaas@avineon.com**  
**<http://www.avineon.com>**



**Chris Fogle, CISSP**  
Partner, Delta Risk LLC  
**cfogle@delta-risk.net**  
**[http:// www.delta-risk.net](http://www.delta-risk.net)**