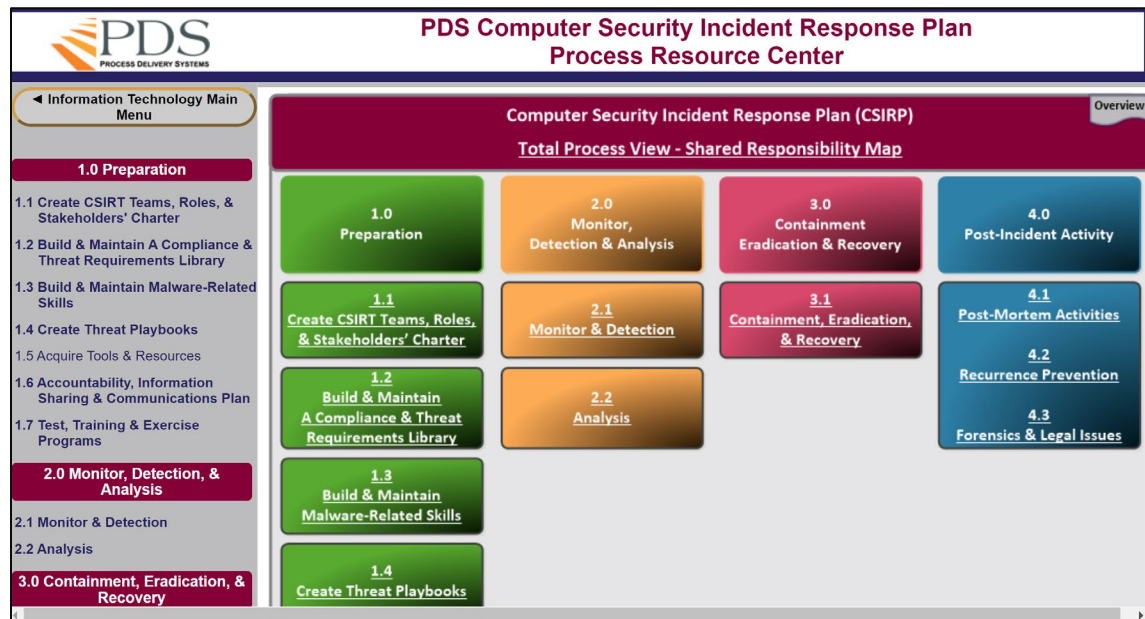


21st-Century Procedural Content Delivery



PDS Computer Security Incident Response Plan Process Resource Center

Information Technology Main Menu

1.0 Preparation

- 1.1 Create CSIRT Teams, Roles, & Stakeholders' Charter
- 1.2 Build & Maintain A Compliance & Threat Requirements Library
- 1.3 Build & Maintain Malware-Related Skills
- 1.4 Create Threat Playbooks
- 1.5 Acquire Tools & Resources
- 1.6 Accountability, Information Sharing & Communications Plan
- 1.7 Test, Training & Exercise Programs

2.0 Monitor, Detection, & Analysis

- 2.1 Monitor & Detection
- 2.2 Analysis

3.0 Containment, Eradication, & Recovery

4.0 Post-Incident Activity

4.1 Post-Mortem Activities

4.2 Recurrence Prevention

4.3 Forensics & Legal Issues

Computer Security Incident Response Plan (CSIRP)
Total Process View - Shared Responsibility Map

1.0 Preparation	2.0 Monitor, Detection & Analysis	3.0 Containment Eradication & Recovery	4.0 Post-Incident Activity
1.1 Create CSIRT Teams, Roles, & Stakeholders' Charter	2.1 Monitor & Detection	3.1 Containment, Eradication, & Recovery	4.1 Post-Mortem Activities
1.2 Build & Maintain A Compliance & Threat Requirements Library	2.2 Analysis		4.2 Recurrence Prevention
1.3 Build & Maintain Malware-Related Skills			4.3 Forensics & Legal Issues
1.4 Create Threat Playbooks			



Hyperlinked Table of Contents

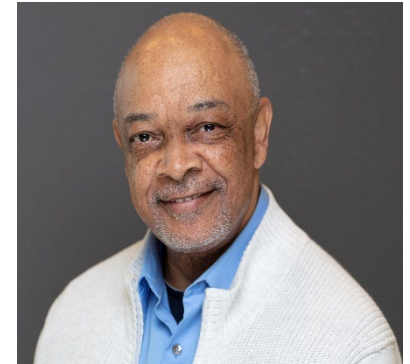
- ◆ [21st-Century Procedural Content Delivery](#)
- ◆ [About the Presenter](#)
- ◆ [Critical Importance of Checklist & Process](#)
- ◆ [Horizontal Fight](#)
- ◆ [Going Vertical](#)
- ◆ [This is Not a Sales Presentation](#)
- ◆ [Process Improvement Projects – What Has Worked](#)
- ◆ [Eliminate Confusion in Complex Processes](#)
- ◆ [Integrate Best Practices into Processes](#)
- ◆ [Cybersecurity Incident Response Process Resource Center](#)
- ◆ [E-Book Design for Fast Document Navigation](#)
- ◆ [Use Table of Contents and Bookmarks in Digital Documents](#)
- ◆ [Documentation Design for 21st-Century Workers](#)
- ◆ [Improved PowerPoint Document Navigation](#)
- ◆ [Step 2.1 Monitor and Detection](#)
- ◆ [Step 2.1 Monitor and Detection Information Panel](#)
- ◆ [Step 2.15 Work Instruction – E-Book Design](#)
- ◆ [Shared Responsibility Mapping](#)
- ◆ [Suppliers, Inputs, Processes, Outputs, Customers](#)
- ◆ [Responsible, Accountable, Consult, Inform](#)
- ◆ [Shared Responsibility Maps Combine SIPOC & RACI](#)
- ◆ [End-to-End Shared Responsibility Maps](#)
- ◆ [Tables for Shared Responsibility Map Development](#)
- ◆ [Diagramming Shared Responsibility Maps](#)
- ◆ [Shared Responsibilities in Process Resource Centers](#)
- ◆ [Information Center](#)
- ◆ [Resources \(page 1 of 2\)](#)
- ◆ [Resources \(page 2 of 2\)](#)
- ◆ [Contact](#)



About the Presenter

Henry Draughon

- Former U.S. Navy Radar Intercept Officer F4-Phantom & Air Traffic Control Officer
- IBM
- Self-Employed
- Importance of 21st- Century Quality Procedural Documentation
- Process Accountability – End-to-End Communication is a Critical Success Factor



Critical Importance of Checklist & Process



Horizontal Flight



Going Vertical



This is Not a Sales Presentation

- Our 12 Years of Process Improvement Projects
- What Hasn't Worked
 - Projects without executive sponsorship
 - No process mindset – ad hoc, reactive, shoot from the hip
 - Intimidated by accountability
 - No budget
 - Silver bullet – Not continuous improvement
 - Not effectively managing process-opposed team members
 - Problem not identified, No ROI in sight
 - Responding to ad-hoc, inconsistent changes



Process Improvement Projects – What Has Worked

- Executive-Sponsored Projects
 - Recognize critical process and communications are broken
 - Easily identified financial/operation deficiencies in current processes
 - Executive is process-oriented
 - Desires improved accountability
- Team Leaders that are Process Receptive
- Use of Industry-Recognized Best Practices and Frameworks
- Clearly and Accurately Defining the Organization's Operational Framework



Eliminate Confusion in Complex Processes

WALL O' TEXT

First of all, you have no idea what you're talking about. It is clearly the advantages of random text that make the internet so distinctive from other crappy text that I'm ad listing specifically for this nonsense paragraph. Second of all, pointing out my poor grammar is weak like Bush's approval ratings, even though history will clearly show that he was among the best presidents the US has ever had. A badger just humped my leg. Can you believe this crap? These buttons need to be shut front of a spending train. I studied for a bit there, but I will keep on writing a block of text so that it may appear as if I have a good point to make and you shall be overwhelmed by my return-key-ignoring skills. Resistance is futile! And then, when you attempt to reply to it, you will inevitably neglect some points that I may have made. I shall point this out to you in a lame-ass effort to appear more intellectual and, thus, right. You are lucky that I'm using commas, even though I firmly believe in capital punishment. Your feebly mind cannot begin to comprehend the massive skill and patience that it takes to add a big-ass wall of text that you see before you. I would be truly impressed if you have made it this far and, as you can see, you are not even half-way through! You poor soul. Avatar sunglasses is where it's at. Where what is it? And how can something be as impressive? Well does that mean? Unless we're talking about microbes, then nothing else would be fitting. You can't be "at" something of that size! Even those big-ass Paris Hilton sunglasses that can cause nuclear winter by blocking the sun. Really, NASA was planning on bringing a gun to shoot the space station. But then their toilet broke and they were like "oh fuck that." Speaking of fuck that, am I the only one who thinks that today's music sucks ass? I mean I saw some chick singing and I was about to pour motor oil in my ears. Where is today's good music like Boston, AC/DC, or Led Zepplin? What will be considered today's classic 20 years from now? Oh yes, the world ends in 2012 so it doesn't even matter. What's that? Ah yes the mayans were the shittiest astronomers. As far as astronomy goes, the mayans is where is at. yep! They knew that every 20,000 years, the Earth and the sun line up with the center of the Milky Way. How the hell do you figure that out? That's badass. Probably the aliens taught them. But what kind of stupid aliens would teach that? Seriously? Wouldnt they teach something USEFUL, like how to make a big black HEMP with a supercharger? That would've handed ass back there! But no, instead they taught them how to figure out when shit lines up in the sky. And so, tic-tac-toe was born. Line up the stars, bitchest! The return key feels extremely neglected by now. It misses the touch of my right pinky! Shadow of the Colossus for the PS2 is a bad-ass game. I recommend it. I'm listening to the soundtrack right now! Bushcock is also the shit, as well as Half Life 2. Anyone who disagrees with this is a vegetarian. And apparently there is something even further than that, people who eat fruit. I forgot the name but I'm astonished that they exist! More power to them and their leather belts. You're still reading? wow, you got some sort of prize. Like a granola bar or something. How about gum? You like gum? Substrains is where it's at... where the mint is at. Oh, snap! Alright this is the last few lines so let's make it sound serious. The democrats have undoubtedly put this country in the toilet in the short 2 years that they've been in power of Congress! Not to mention that things can indeed go down that fast and don't need years to build up, which is what a bubble or '08 shortcomings is typical of a liberal pinkie commie and you are destroying america with your tolerance for different people, ya hippie! If you don't like it, boy you can get out and go to go Canada to munch on some Canadian bacon, EH EH! This is our country and we will make whatever messes with us! USA NUMBER ONE! Congratulations Bro, yep!

I'M NOT READING IT

PRESCRIPTION: DOUBLE DOSE OF RETURN KEY



RCM Project Complete Consultant Gone



Beat down – procedures
won't get used

Disconnected technologies
and data drain productivity



Lost information
assets –
something the
company paid
for



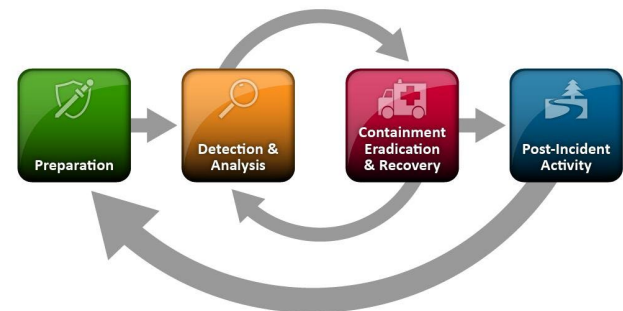
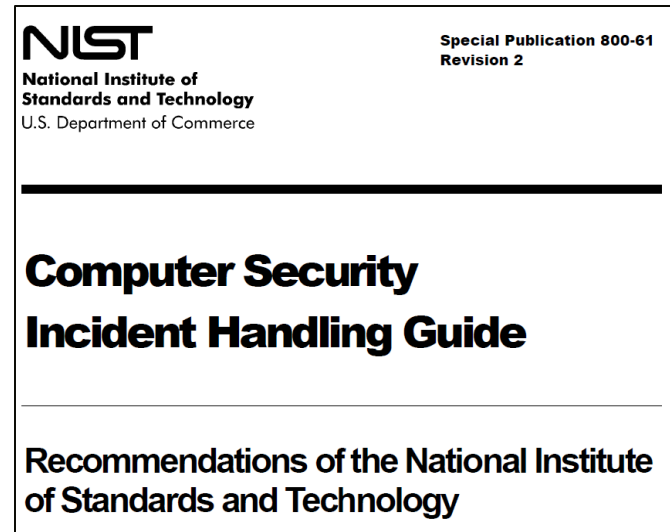
Integrate Best Practices into Processes

National Institute of Standards and Technology (NIST)

Part of the U.S. Department of Commerce


Special Publication 800-61 Revision 2
(NIST SP 800-61 R2)

Industry-Recognized and Widely Adopted
Best Practice for Cybersecurity Incident
Response



Cybersecurity Incident Response Process Resource Center





PDS Computer Security Incident Response Plan Process Resource Center

◀ Information Technology Main Menu

Overview

Computer Security Incident Response Plan (CSIRP)

Total Process View - Shared Responsibility Map

1.0 Preparation	2.0 Monitor, Detection & Analysis	3.0 Containment Eradication & Recovery	4.0 Post-Incident Activity
1.1 <u>Create CSIRT Teams, Roles, & Stakeholders' Charter</u>	2.1 <u>Monitor & Detection</u>	3.1 <u>Containment, Eradication, & Recovery</u>	4.1 <u>Post-Mortem Activities</u>
1.2 <u>Build & Maintain A Compliance & Threat Requirements Library</u>	2.2 <u>Analysis</u>		4.2 <u>Recurrence Prevention</u>
1.3 <u>Build & Maintain Malware-Related Skills</u>			4.3 <u>Forensics & Legal Issues</u>
1.4 <u>Create Threat Playbooks</u>			

1.0 Preparation

- 1.1 Create CSIRT Teams, Roles, & Stakeholders' Charter
- 1.2 Build & Maintain A Compliance & Threat Requirements Library
- 1.3 Build & Maintain Malware-Related Skills
- 1.4 Create Threat Playbooks
- 1.5 Acquire Tools & Resources
- 1.6 Accountability, Information Sharing & Communications Plan
- 1.7 Test, Training & Exercise Programs

2.0 Monitor, Detection, & Analysis

- 2.1 Monitor & Detection
- 2.2 Analysis

3.0 Containment, Eradication, & Recovery

[Return to Table of Contents](#)



E-Book Design for Fast Document Navigation

Computer Security Incident Response Team (CSIRT) Charter

Contact:

Henry Draughon

Process Delivery Systems

hdraughon@processdeliversystems.com

Tap Hyperlinks to Navigate

Hyperlinks

Table of Contents

Introduction	3
Purpose	4
Scope	4
Goals	5
Authority	6
Membership	7
CSIRT Diagram	8
Roles Responsibilities	8
Internal Roles Responsibilities	8
External Roles Responsibilities	11
Roster	14
Approved by	15

Computer Security Incident Response Team (CSIRT) Charter

Computer Security Incident Response Team (CSIRT)

Tap Hyperlinks to Navigate

Hyperlinks

Table of Contents

Introduction	3
Purpose	4
Scope	4
Goals	5
Authority	6
Membership	7
CSIRT Diagram	8
Roles Responsibilities	8
Internal Roles Responsibilities	8
External Roles Responsibilities	11
Roster	14
Approved by	15

Roles and Responsibilities

CSIRT Internal Members' Roles and Responsibilities

The CSIRT is led by the Chief Information Security Officer (CISO). The additional team component roles and responsibilities are as follows:

- Computer Security Incident Response Team Leader
 - One of the individuals listed as the Core Team Members will be assigned the role of Incident Response Lead. The Incident Response Lead is the

Removing Confusion from Process Complexity
Public
Page 8 of 14

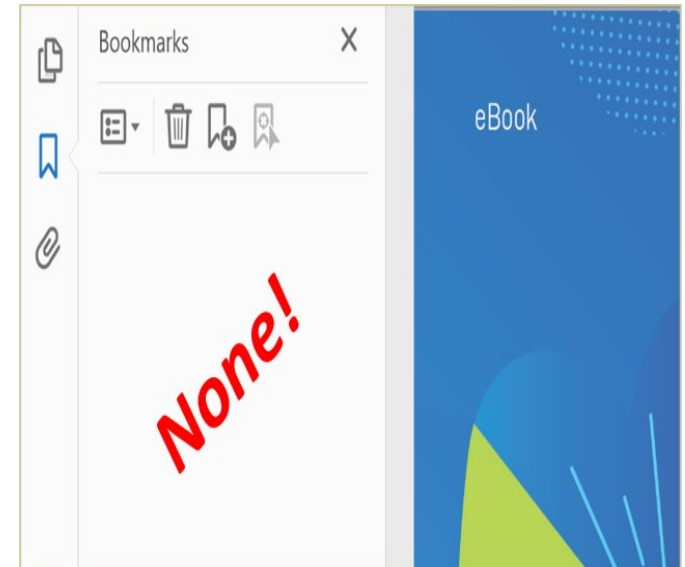


Use Table of Contents and Bookmarks in Digital Documents

Tens of thousands of documents.

Navigation issues include:

- No table of contents or bookmarks
- Table of contents with no hyperlinks
- Hyperlinked table of contents or bookmarks that tell you nothing about the content. For example:
 - Chapter 1
 - Chapter 2
- Table of contents on something other than page 1 or 2 (saw one with the table of contents on page 45)



- **White Paper: 8 Seconds is All You Get**

- <https://www.processdeliverysystems.com/white-paper-8-seconds-is-all-you-get.html>

White Paper – 5 Digital Documentation Features for 21st-Century Workers



8 seconds is all you get!

- ✓ 21st-century attention spans are shorter
- ✓ The efficient use of a worker's time is critical to their productivity
- ✓ 21st-century workers are mobile
- ✓ Many are working from home
- ✓ They're reading your digital documents on mobile devices



Writers and publishers are using these digital document features to optimize that 8 seconds.



Improved PowerPoint Document Navigation

- **This Presentation**

- Hyperlinked Table of Contents
- Return to Table of Contents Button Lower Left Corner
- Produced Using Microsoft PowerPoint Action Buttons and Links

Hyperlinked Table of Contents




- [21st-Century Procedural Content Delivery](#)
- [About the Presenter](#)
- [Critical Importance of Checklist & Process](#)
- [Horizontal Fight](#)
- [Going Vertical](#)
- [This is Not a Sales Presentation](#)
- [Process Improvement Projects – What Has Worked](#)
- [Eliminate Confusion in Complex Processes](#)
- [Integrate Best Practices into Processes](#)
- [Cybersecurity Incident Response Process Resource Center](#)
- [E-Book Design for Fast Document Navigation](#)
- [Use Table of Contents and Bookmarks in Digital Documents](#)
- [Documentation Design for 21st-Century Workers](#)
- [Improved PowerPoint Document Navigation](#)
- [Step 2.1 Monitor and Detection](#)

- [Step 2.1 Monitor and Detection Information Panel](#)
- [Step 2.15 Work Instruction – E-Book Design](#)
- [Shared Responsibility Mapping](#)
- [Suppliers, Inputs, Processes, Outputs, Customers](#)
- [Responsible, Accountable, Consult, Inform](#)
- [Shared Responsibility Maps Combine SIPOC & RACI](#)
- [End-to-End Shared Responsibility Maps](#)
- [Tables for Shared Responsibility Map Development](#)
- [Diagraming Shared Responsibility Maps](#)
- [Shared Responsibilities in Process Resource Centers](#)
- [Information Center](#)
- [Resources \(page 1 of 2\)](#)
- [Resources \(page 2 of 2\)](#)
- [Contact](#)


Return to Table of Contents 

Documentation Design for 21st-Century Workers




- **White Paper: 8 Seconds is All You Get**
 - <https://www.processdeliverysystems.com/white-paper-8-seconds-is-all-you-get.html>

White Paper – 5 Digital Documentation Features for 21st-Century Workers




8 seconds is all you get!

- ✓ 21st-century attention spans are shorter
- ✓ The efficient use of a worker's time is critical to their productivity
- ✓ 21st-century workers are mobile
- ✓ Many are working from home
- ✓ They're reading your digital documents on mobile devices

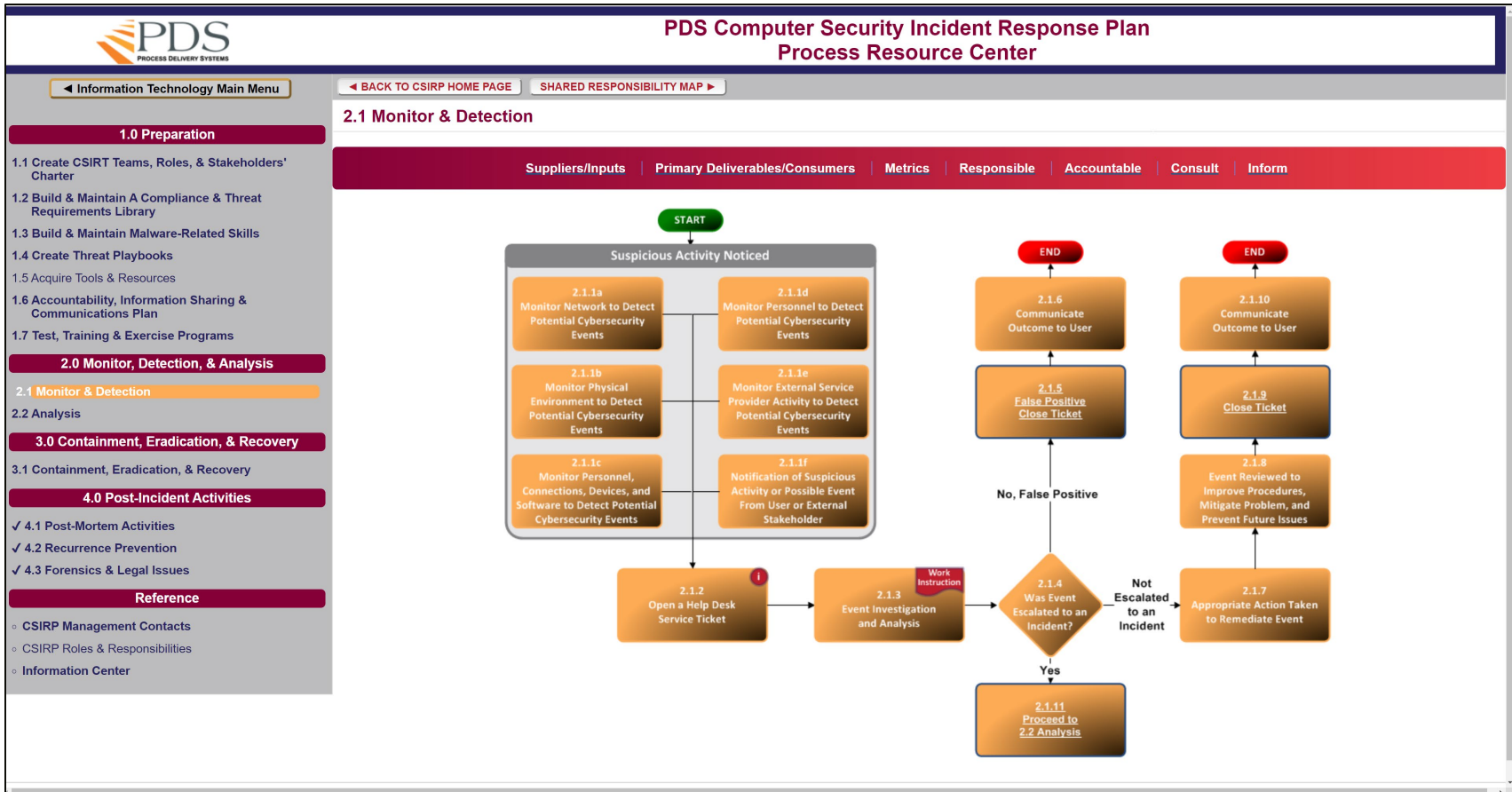


Writers and publishers are using these digital document features to optimize that 8 seconds.

Return to Table of Contents 



Step 2.1 Monitor and Detection



Step 2.1 Monitor and Detection Information Panel



PDS Computer Security Incident Response Plan

Process Resource Center

◀ Information Technology Main Menu

1.0 Preparation

1.1 Create CSIRT Teams, Roles, & Stakeholders' Charter

1.2 Build & Maintain A Compliance & Threat Requirements Library

1.3 Build & Maintain Malware-Related Skills

1.4 Create Threat Playbooks

1.5 Acquire Tools & Resources

1.6 Accountability, Information Sharing & Communications Plan

1.7 Test, Training & Exercise Programs

2.0 Monitor, Detection, & Analysis

2.1 Monitor & Detection

2.2 Analysis

3.0 Containment, Eradication, & Recovery

3.1 Containment, Eradication, & Recovery

4.0 Post-Incident Activities

✓ 4.1 Post-Mortem Activities

✓ 4.2 Recurrence Prevention

✓ 4.3 Forensics & Legal Issues

Reference

◦ CSIRP Management Contacts

◦ CSIRP Roles & Responsibilities

◦ Information Center

◀ BACK TO CSIRP HOME PAGE
SHARED RESPONSIBILITY MAP ▶

2.1 Monitor & Detection

Suppliers/Inputs | Primary Deliverables/Consumers | Metrics | Responsible | Accountable | Consult | Inform

2.1.2 Open a Help Desk Service Ticket:

- DO NOT TURN OFF YOUR COMPUTER!** You will be instructed on how to disconnect your computer from the network.
- User call Help Desk hotline number ☎ (972) 980-9041 and open a Priority 1 Ticket
- Technical Services NOC/SOC opens a Priority 1 Ticket

Noticed

Environment to Detect Potential Cybersecurity Events

2.1.1c Monitor Personnel, Connections, Devices, and Software to Detect Potential Cybersecurity Events

2.1.1d Monitor Personnel to Detect Potential Cybersecurity Events

2.1.1e Monitor External Service Provider Activity to Detect Potential Cybersecurity Events

2.1.1f Notification of Suspicious Activity or Possible Event From User or External Stakeholder

2.1.2 Open a Help Desk Service Ticket

2.1.3 Event Investigation and Analysis

2.1.4 Was Event Escalated to an Incident?

2.1.11 Proceed to 2.2 Analysis

2.1.5 False Positive Close Ticket

2.1.6 Communicate Outcome to User

END

2.1.7 Appropriate Action Taken to Remediate Event

2.1.8 Event Reviewed to Improve Procedures, Mitigate Problem, and Prevent Future Issues

2.1.9 Close Ticket

2.1.10 Communicate Outcome to User

END

Return to
Table of Contents

Step 2.15 Work Instruction – E-Book Design



**IT Security Plan – Computer Security Incident Response Plan (CSIRP)
Event Investigation and Analysis 2.1.5**



 Audience: _____
Implementation Date: _____
Last Reviewed/Updated: _____
Contact: _____

Table of Contents

- Quick Checklist**2
- Core Member Contacts**3
- Shared Responsibility Map**5
- Suspicious Activity Noticed**6
 - Event Logging and Tracking6
 - Sample Question Bank7
- Event Prioritization**8
 - Business8
 - Technical Impact8
 - Recoverability Effort9
- Investigation and Analysis Outcomes**10
- Next Steps**10
- Authorizations**10

 **Computer Security Incident Response Plan (CSIRP)
Event Investigation and Analysis 2.1.5**

Recoverability Effort

Category	Definition
Regular	Time to recovery is predictable with existing resources
Supplemented	Time to recovery is predictable with additional resources
Extended	Time to recovery is unpredictable; additional resources and outside help are needed
Non Recoverable	Recovery from the incident is not possible (e.g., sensitive data exfiltrated and posted publicly); launch investigation

Hyperlinks

- [Table of Contents](#)
- [Quick Checklist](#) P. 2
- [Core Member Contacts](#) P. 3
- [Shared Responsibility Map](#) P. 5
- [Suspicious Activity Noticed](#) P. 6
- [Event Logging and Tracking](#) P. 6
- [Sample Question Bank](#) P. 7
- [Event Prioritization](#) P. 8
- [Business](#) P. 8
- [Technical Impact](#) P. 8
- [Recoverability Effort](#) P. 9
- [Investigation & Analysis Outcomes](#) P. 10
- [Next Steps](#) P. 10
- [Authorizations](#) P. 10

Confidential -IT Security Plan - Page 9 of 10

Return to
Table of Contents



Shared Responsibility Mapping

- **Visually Illustrates and Measures Process Accountabilities**
- **All Processes Receive Inputs**
 - Someone or Something (Could be a Process, Department, or External Entity) Is Responsible for Providing the Inputs According to Predefined Specifications
- **All Processes Create Outputs**
 - Someone or Something (Could be a Process, Department, or External Entity) Expects to Receive the Outputs According to Predefined Specifications



Suppliers, Inputs, Processes, Outputs, Customers



- **Suppliers**

- Agree to the input specifications from the process team and provides the inputs to the process team according to those specifications

- **Inputs**

- The specified resources provided to the process team

- **Processes**

- The steps the process team will execute to create the outputs

- **Outputs**

- The deliverables created by the process team that will be delivered to the customer/consumer according to specifications

- **Customers**

- Expect to receive the outputs/deliverables developed according to predefined specifications by the process team



Responsible, Accountable, Consult, Inform

- **Responsible**

- (The Doers) Those who do the work to achieve the task. There is at least one role with a participation type of Responsible

- **Accountable**

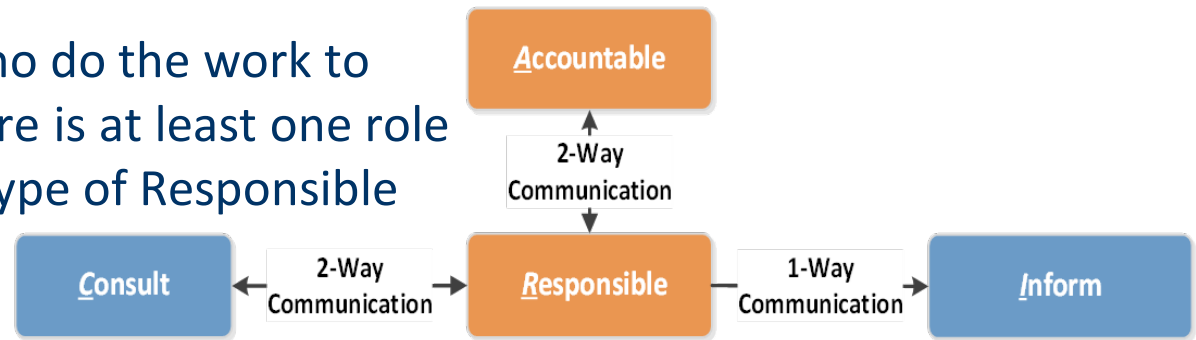
- (The Buck Stops Here) The executive ultimately answerable for the thoroughness of the completed task and owns the budget

- **Consult**

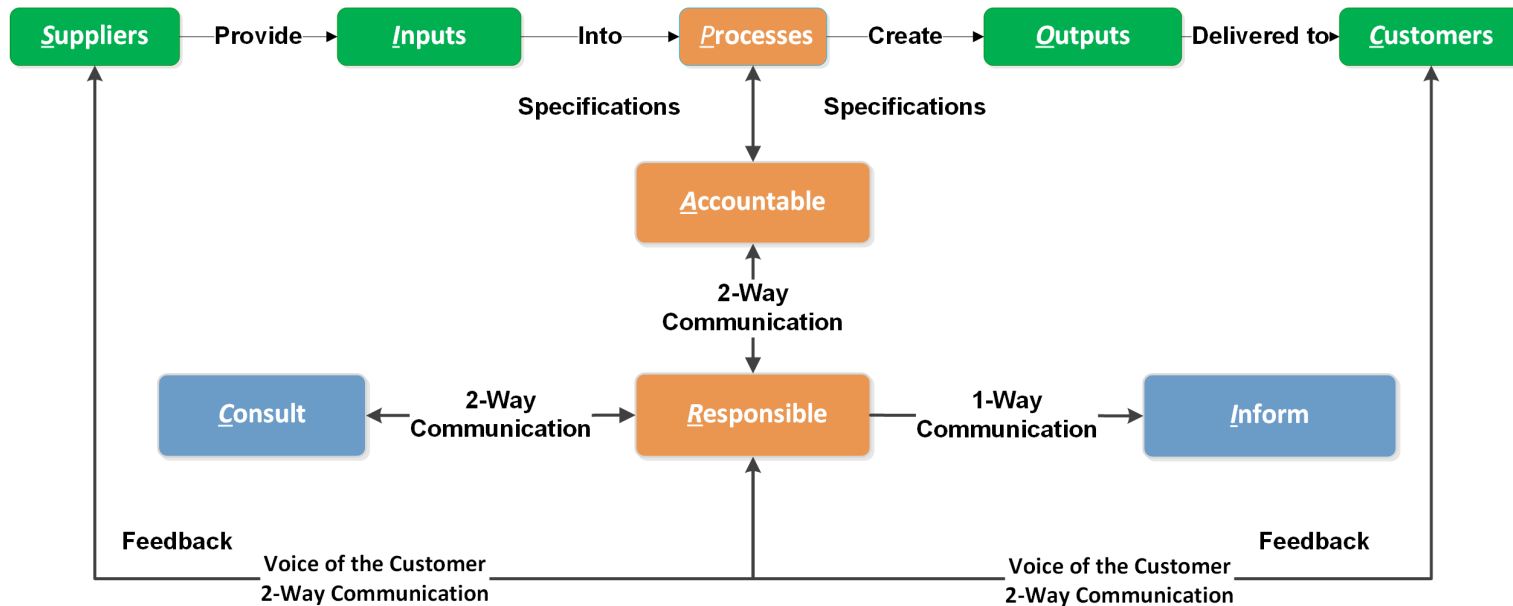
- Those whose opinions are sought, typically subject matter experts with whom there is two-way communication

- **Inform**

- Those kept up to date on progress with whom there is one-way communication



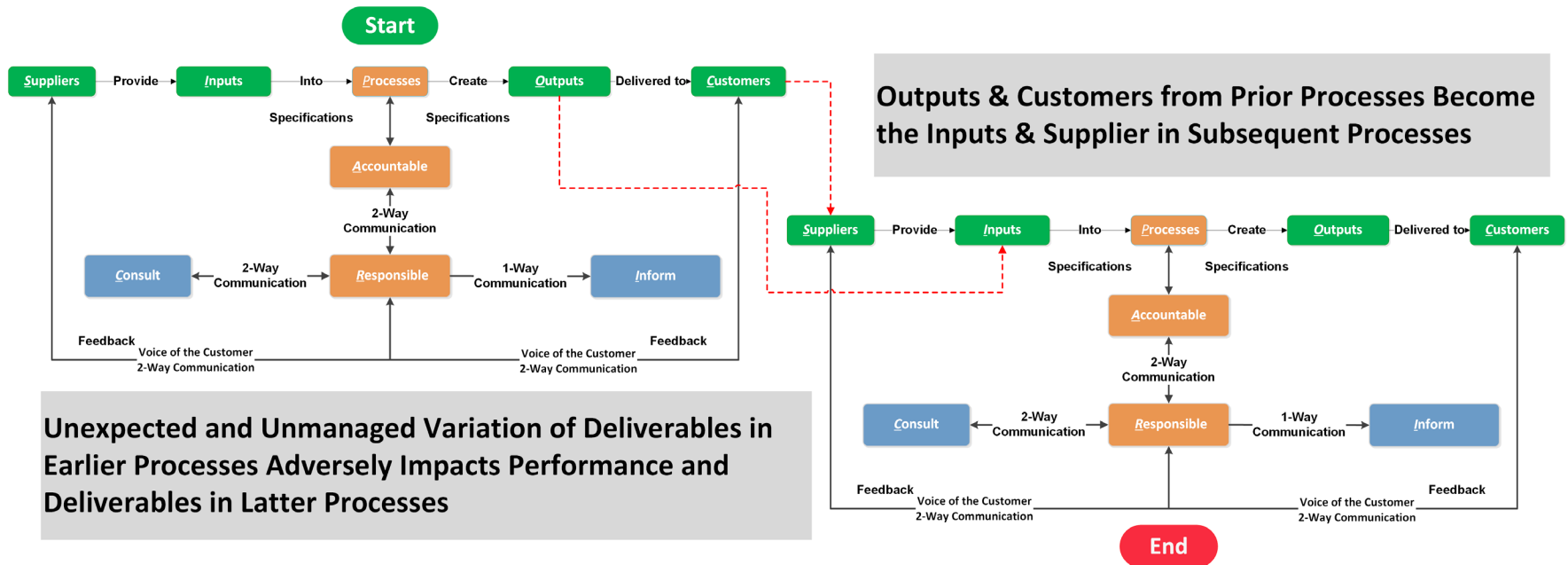
Shared Responsibility Maps Combine SIPOC & RACI



- Define Process External and Internal Roles, Responsibilities and Deliverables
- Visually Illustrate Who is Responsible for Providing Input into the Process
- Illustrate the Roles of Those Who Own Process Execution
- Visually Illustrate Who Receives Output From the Process
- **** Communication Including Feedback is Essential**
 - **Voice of the Customer is Critical**



End-to-End Shared Responsibility Maps



Unexpected and Unmanaged Variation of Deliverables in Earlier Processes Adversely Impacts Performance and Deliverables in Latter Processes



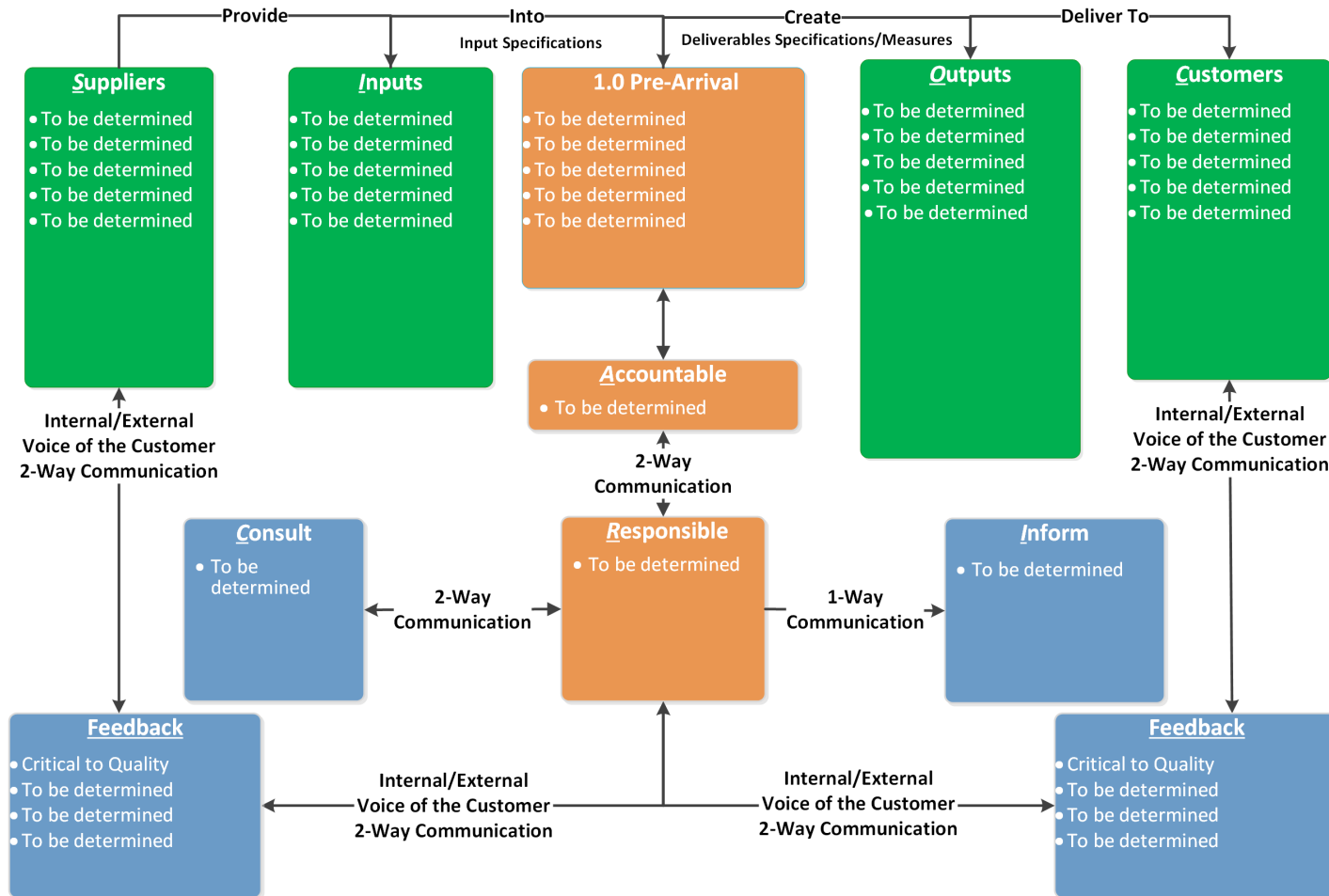
Tables for Shared Responsibility Map Development



2.0 Monitor, Detection & Analysis		
Process: 2.2 Analysis		
Supplier(s)/Inputs		
Supplier(s): Role-based	Inputs	Requirements
Individual, Department, Team	Inputs required for the process	Specification of inputs
Deliverables/Customers		
Deliverables	Customers	Requirements
Outputs from the process	Those receiving the outputs of the process	Specification of deliverables/outputs
Responsible	The person/team leader responsible for process execution	
Accountable	The executive that owns the process	
Consult	Those outside the team with relevant expertise that should be considered	
Inform	Those that may need to kept informed	
Metrics	Process performance	



Diagramming Shared Responsibility Maps



Shared Responsibilities in Process Resource Centers

PDS Computer Security Incident Response Plan Process Resource Center

[Information Technology Main Menu](#)

[BACK TO CSIRP HOME PAGE](#)

[SHARED RESPONSIBILITY MAP](#)

2.1 Monitor & Detection

1.0 Preparation

- 1.1 Create CSIRT Teams, Roles, & Stakeholders' Charter
- 1.2 Build & Maintain A Compliance & Threat Requirements Library
- 1.3 Build & Maintain Malware-Related Skills
- 1.4 Create Threat Playbooks
- 1.5 Acquire Tools & Resources
- 1.6 Accountability, Information Sharing & Communications Plan
- 1.7 Test, Training & Exercise Programs

2.0 Monitor, Detection, & Analysis


2.1 Monitor & Detection

2.2 Analysis

3.0 Containment, Eradication, & Recovery

Suppliers/Inputs	Primary Deliverables/Consumers	Metrics	Responsible	Accountable	Consult
<ul style="list-style-type: none"> Users Information Technology Staff NOC/SOC Security Monitoring Tools Event Logging Tool External Partners Victims 	<ul style="list-style-type: none"> Suspicious Network/Computer Activity Report or Complaint of Personal Information Compromised 	<ul style="list-style-type: none"> Continuous monitoring with timely response Users adequately trained to recognized and report suspicious network/system activities Automated tools with updates to recognize and report suspicious network/system activities Recognition of deviations from normal activities 			<div style="border: 1px solid gray; padding: 5px; margin-bottom: 10px;"> <div style="display: flex; justify-content: space-between;"> (C)onsult Close </div> <p style="font-size: small; margin: 0;"><i>Those whose opinions are sought, typically subject matter experts. Two-way communication.</i></p> <ul style="list-style-type: none"> CSIRT Information Technology Legal Physical Security Insurance Company </div> <div style="background-color: #FFD700; padding: 5px; text-align: center; margin-bottom: 10px;">2.1.8</div> <div style="background-color: #FFD700; padding: 5px; text-align: center;">Event Reviewed to Improve Procedures, Mitigate Problem, and Prevent Future Issues</div>
Monitor Personnel, Connections, Devices, and Software to Detect Potential Cybersecurity Events	Notification of Suspicious Activity or Possible Event From User or External Stakeholder		No, False Positive		





PDS Computer Security Incident Response Plan Process Resource Center

Reference CLOSE

- CSIRP Management Contacts
- CSIRP Roles & Responsibilities
- Information Center**

CSIRP Information Center

- Threat Playbook Catalog
- Cloud Service Providers**
 - Amazon Web Services Best Practices
 - Microsoft Shared responsibilities for Cloud Computing
 - PCI DSS Cloud Computing Guidelines
 - Protecting Data in Microsoft Azure
- CSIRP Governmental Organizations**
 - Department of Homeland Security (DHS):
[\(More on DHS...\)](#)
 - North American Electric Reliability Corporation (NERC):
[\(More on NERC...\)](#)
 - SANS Institute
 - The National Council of ISACS
 - The National Institute of Standards and Technology (NIST)
 - U.S. Department of Health and Human Services (HIPAA Requirements)
 - US-CERT | United States Computer Emergency Readiness Team
- CSIRP Industry Contacts**
 - Securities Industry and Financial Markets Association (SIFMA)
- Reference Publications**
 - Carnegie Mellon Software Engineering Institute CERT Resilience Management Model Version 1.2, Incident Management and Control
 - NIST PUBLICATIONS BY SECURITY CONTROL FAMILY - (SP 800-53):
 - National Institute of Standards and Technology Special Publication 800-61 Revision 2 (NIST SP 800-61 R2), Computer Security Incident Handling Guide:
- Malware Remediation Resources**
 - KnowBe4 Ransomware Knowledgebase:
 - KnowBe4 has assembled a Ransomware Knowledgebase that gives you the background, history and inner-workings of all widespread ransomware strains and families that have appeared over the last few years.
 - Alien Vault Open Threat Exchange (OTX):
 - The world's first truly open threat intelligence community that enables collaborative defense with actionable, community-powered threat data
 - Lenny Zeltzer - Free Online Tools for Looking up Potentially Malicious Websites:
 - Free Online Tools for Looking up Potentially Malicious



Resources (page 1 of 2)

- **NIST SP 800-61 R2**

- <https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final>

- **Microsoft Word Videos and Tutorials**

- <https://support.microsoft.com/en-us/office/word-2013-videos-and-tutorials-14807f76-d2b5-44d6-af11-9c880c44e551?ui=en-us&rs=en-us&ad=us>

- **MS Word – Introduction to Table of Contents**

- <https://support.microsoft.com/en-us/office/video-introduction-to-tables-of-contents-tocs-0af555b1-fa51-4790-be03-53f022cc086a?ui=en-us&rs=en-us&ad=us>

- **MS Word – Introduction to Table of Contents**

- <https://support.microsoft.com/en-us/office/video-introduction-to-tables-of-contents-tocs-0af555b1-fa51-4790-be03-53f022cc086a?ui=en-us&rs=en-us&ad=us>

- **Test Drive the Computer Security Incident Response Plan - Process Resource Center**

- Description of what to look for: <https://www.processdeliverysystems.com/test-drive---csirp-process-resource-center.html>
- Test Drive: https://www.pdsimplified.com/pds_CSIRPDemo/index.htm



- **White Paper – 5 Digital Documentation Features for 21st-Century Workers – 8 Seconds is All You Get**
 - https://www.processdeliverysystems.com/uploads/1/3/2/9/132974232/8_seconds_5_features.pdf
- **LinkedIn Article - Mapping Revenue Cycle Management Cross-Department Roles & Responsibilities**
 - <https://www.linkedin.com/pulse/mapping-revenue-cycle-management-cross-department-henry-draughon-/>
- **White Paper – Mobile Business E-Document Design**
 - https://www.processdeliverysystems.com/uploads/1/3/2/9/132974232/pds_bus_e-docs_short_attention_span.pdf



Henry Draughon
Process Delivery Systems
(972) 980-9041
hdraughon@processdeliverysystems.com

Reducing Process Confusion and Complexity

