RESOLUTE GUARD

Central San Joaquin Valley Risk Management Authority
CSJVRMA

ResoluteGuard™
SMART- Cyber Action Plan™
(SMART-CAP™)

You must have a plan with a strategy of
continuously improving your cyber-security profile
to meet todays ever-evolving cyber security challenges

RESOLUTE
GUARD

User-Friendly SMART-Cyber Action Plan

Smart Workflow Management Solution Aligns:

- Member Initiatives with Insurance and Regulatory Objectives and
- Executive Governance with Administrative and Technical Activities To

Guard Against A Cyber Disruption Of Service

RESOLUTE GUARD

User-Friendly SMART-Cyber Action Plans™ Address Insurance 2022-2023 "Best Practices"

Prioritized Action Items Listed in "Easy-to-Use" Smart-Cyber Action Plan

Manage Workflow With "Easy to Understand" Best Practice Guidelines

Documented Procedures & Electronic Verification Support

Network Scans Document Current Software and Hardware Environment

Progress and Change Report Updates to Support Continuous Improvement

Cyber Insurance Coverage
Public Entity Minimum System Security Standards/Best Practices

Patching- Updated within 30 days; 1-7 days for Critical & High Severity patching

Guidelines/Policies- Incident Response; Disaster Recovery; Business Continuity

Backups- Separate from Primary Network; Regular Backups; Testing; Encryption; Restore within 72 Hours, Anti-Virus

Multi-factor Authentication (MFA)- 100% for Remote Access and Privileged User Accounts; Email Access

Endpoint Protection, Detection & Response (EDR)- EDR Solution in place across Enterprise

Remote Desktop Protocol- MFA Enabled VPN Remote access; Network-level Authentication enabled

Employee Training- Simulated Phishing Email Training; Regular Cyber Security Training; Fraudulent Accounting Transactions

End of Life Software- Plan/Guidelines and Adequate Measures to Protect EOL Software

RESOLUTE GUARD

How SMART-Cyber Action Plan's™ Align Executive Governance With Administrative and Technical Activities To Address Insurance Requirements

Translates Technical Language into Easy-to-Understand Reports and Best Practices Policies

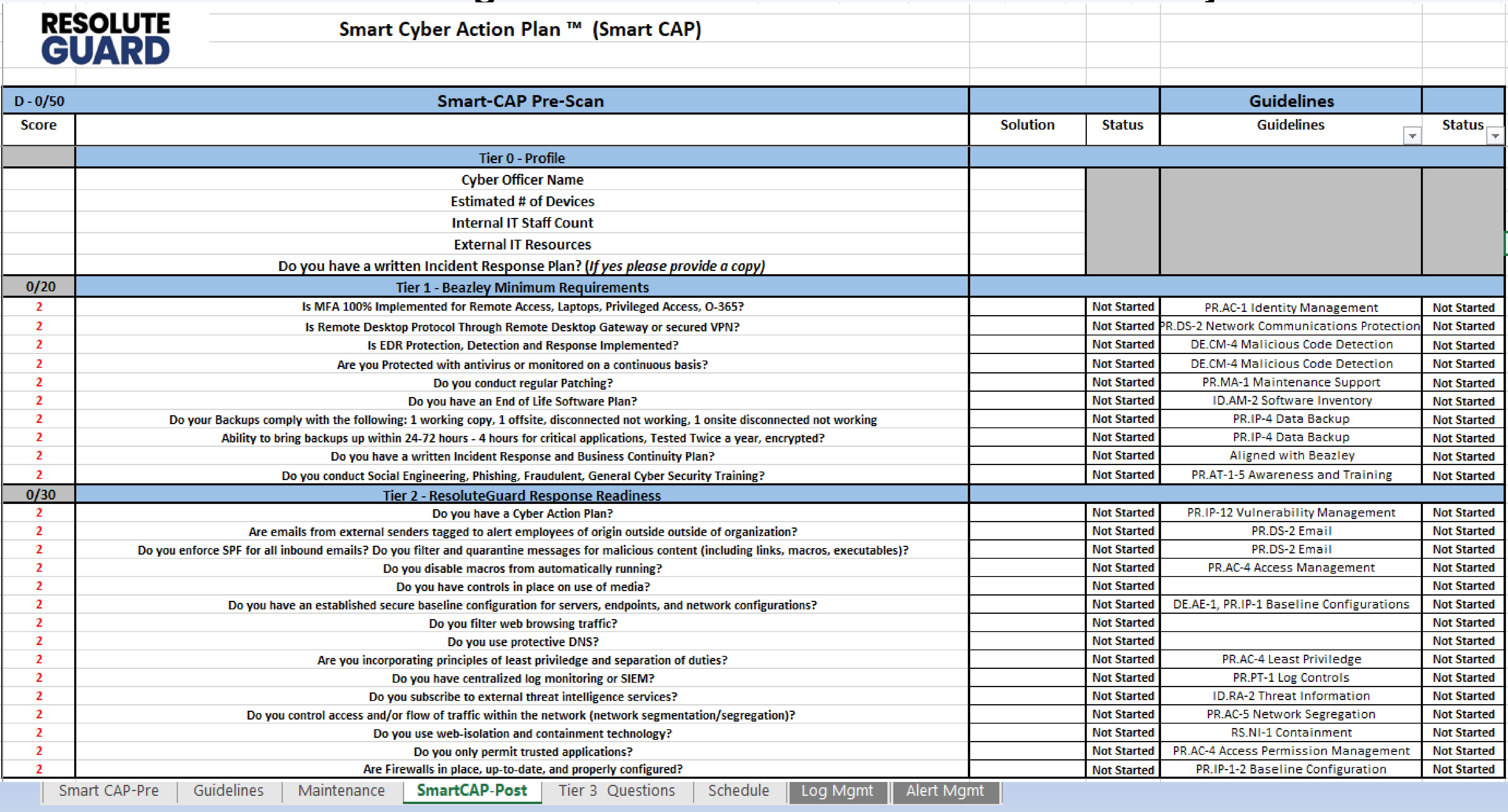
Program Identifies Current Networks Internal & External "Strengths and Weaknesses"

Prioritizes Activities Into "Easy to Use" SMART- Cyber Action Plans™ (SMART-CAP)

Customized To Specific Insurance Company Recommendations

Smart Workflow Management Supports Insureds to
"Do The Best You Can As Fast As You Can"
To Guard Against A Cyber Disruption of Service

SMART-CAP's Align Insured Workflow With Insurance Objectives



RESOLUTE GUARD

Smart Cyber Action Plan ™ (Smart CAP)

D - 0/50	Smart-CAP Pre-Scan			Guidelines	
Score		Solution	Status	Guidelines	Status
	Tier 0 - Profile				
	Cyber Officer Name				
	Estimated # of Devices				
	Internal IT Staff Count				
	External IT Resources				
	Do you have a written Incident Response Plan? *(If yes please provide a copy)*				
0/20	Tier 1 - Beazley Minimum Requirements				
2	Is MFA 100% Implemented for Remote Access, Laptops, Privileged Access, O-365?		Not Started	PR.AC-1 Identity Management	Not Started
2	Is Remote Desktop Protocol Through Remote Desktop Gateway or secured VPN?		Not Started	PR.DS-2 Network Communications Protection	Not Started
2	Is EDR Protection, Detection and Response Implemented?		Not Started	DE.CM-4 Malicious Code Detection	Not Started
2	Are you Protected with antivirus or monitored on a continuous basis?		Not Started	DE.CM-4 Malicious Code Detection	Not Started
2	Do you conduct regular Patching?		Not Started	PR.MA-1 Maintenance Support	Not Started
2	Do you have an End of Life Software Plan?		Not Started	ID.AM-2 Software Inventory	Not Started
2	Do your Backups comply with the following: 1 working copy, 1 offsite, disconnected not working, 1 onsite disconnected not working		Not Started	PR.IP-4 Data Backup	Not Started
2	Ability to bring backups up within 24-72 hours - 4 hours for critical applications, Tested Twice a year, encrypted?		Not Started	PR.IP-4 Data Backup	Not Started
2	Do you have a written Incident Response and Business Continuity Plan?		Not Started	Aligned with Beazley	Not Started
2	Do you conduct Social Engineering, Phishing, Fraudulent, General Cyber Security Training?		Not Started	PR.AT-1-5 Awareness and Training	Not Started
0/30	Tier 2 - ResoluteGuard Response Readiness				
2	Do you have a Cyber Action Plan?		Not Started	PR.IP-12 Vulnerability Management	Not Started
2	Are emails from external senders tagged to alert employees of origin outside outside of organization?		Not Started	PR.DS-2 Email	Not Started
2	Do you enforce SPF for all inbound emails? Do you filter and quarantine messages for malicious content (including links, macros, executables)?		Not Started	PR.DS-2 Email	Not Started
2	Do you disable macros from automatically running?		Not Started	PR.AC-4 Access Management	Not Started
2	Do you have controls in place on use of media?		Not Started		Not Started
2	Do you have an established secure baseline configuration for servers, endpoints, and network configurations?		Not Started	DE.AE-1, PR.IP-1 Baseline Configurations	Not Started
2	Do you filter web browsing traffic?		Not Started		Not Started
2	Do you use protective DNS?		Not Started		Not Started
2	Are you incorporating principles of least priviledge and separation of duties?		Not Started	PR.AC-4 Least Priviledge	Not Started
2	Do you have centralized log monitoring or SIEM?		Not Started	PR.PT-1 Log Controls	Not Started
2	Do you subscribe to external threat intelligence services?		Not Started	ID.RA-2 Threat Information	Not Started
2	Do you control access and/or flow of traffic within the network (network segmentation/segregation)?		Not Started	PR.AC-5 Network Segregation	Not Started
2	Do you use web-isolation and containment technology?		Not Started	RS.NI-1 Containment	Not Started
2	Do you only permit trusted applications?		Not Started	PR.AC-4 Access Permission Management	Not Started
2	Are Firewalls in place, up-to-date, and properly configured?		Not Started	PR.IP-1-2 Baseline Configuration	Not Started

RESOLUTE GUARD

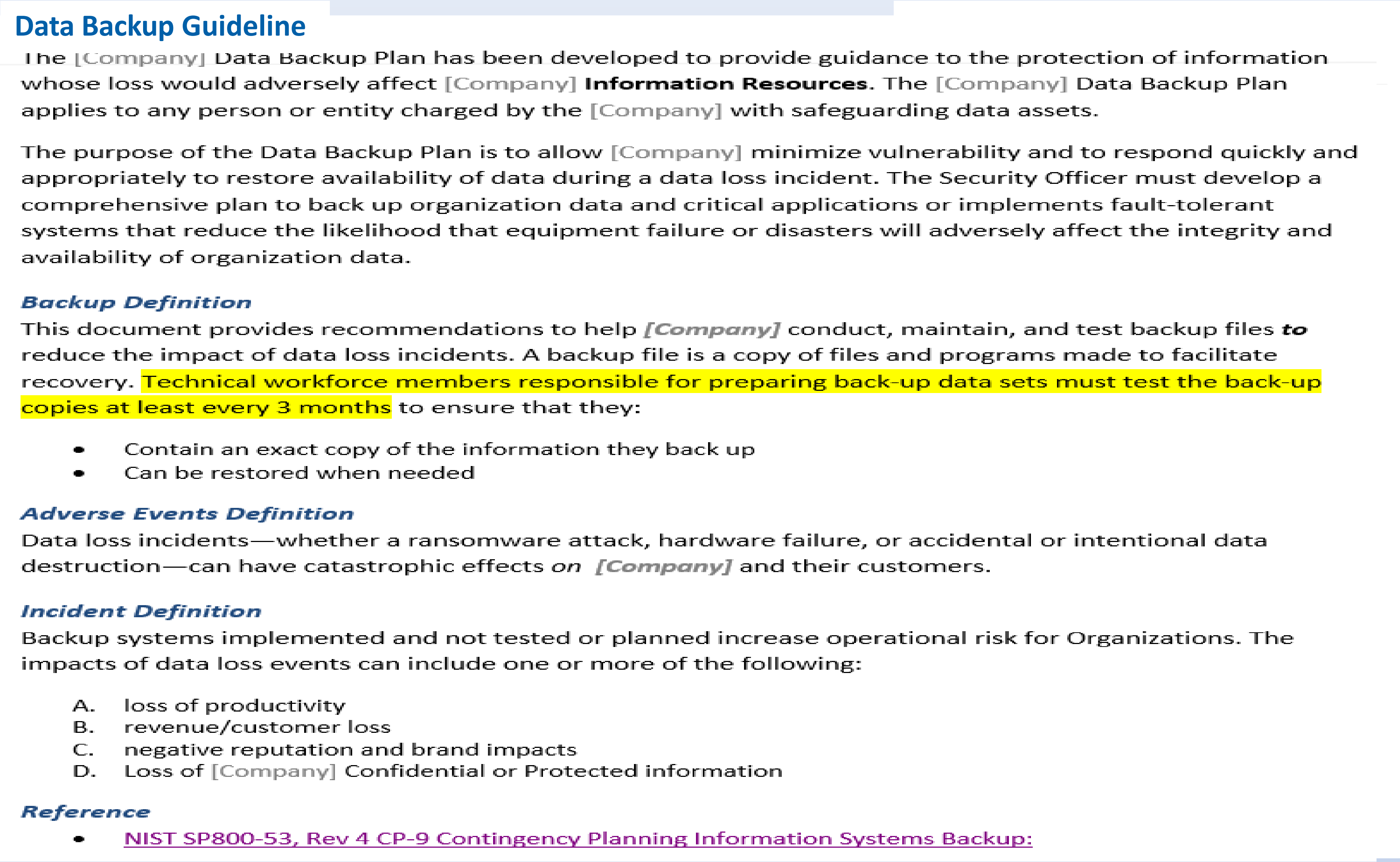
Importance of Documenting NIST-CSF Guidelines To Manage Maintenance Activities and Continuous Improvement are also Discussed on First Call

Documented Guidelines and Procedures

Multi-Factor Authentication
Security Awareness & Training
End-Point Detection & Response
Firewalls and Anti-Virus
Data Backup Guideline
Regular Network Scans

ResoluteGuard Best Practices

Cyber Action Plan
Incident Response Plan
Business Continuity & Disaster Recovery Plan



Data Backup Guideline

The [Company] Data Backup Plan has been developed to provide guidance to the protection of information whose loss would adversely affect [Company] **Information Resources**. The [Company] Data Backup Plan applies to any person or entity charged by the [Company] with safeguarding data assets.

The purpose of the Data Backup Plan is to allow [Company] minimize vulnerability and to respond quickly and appropriately to restore availability of data during a data loss incident. The Security Officer must develop a comprehensive plan to back up organization data and critical applications or implements fault-tolerant systems that reduce the likelihood that equipment failure or disasters will adversely affect the integrity and availability of organization data.

Backup Definition

This document provides recommendations to help *[Company]* conduct, maintain, and test backup files ***to*** reduce the impact of data loss incidents. A backup file is a copy of files and programs made to facilitate recovery. Technical workforce members responsible for preparing back-up data sets must test the back-up copies at least every 3 months to ensure that they:

- Contain an exact copy of the information they back up
- Can be restored when needed

Adverse Events Definition

Data loss incidents—whether a ransomware attack, hardware failure, or accidental or intentional data destruction—can have catastrophic effects *on* ***[Company]*** and their customers.

Incident Definition

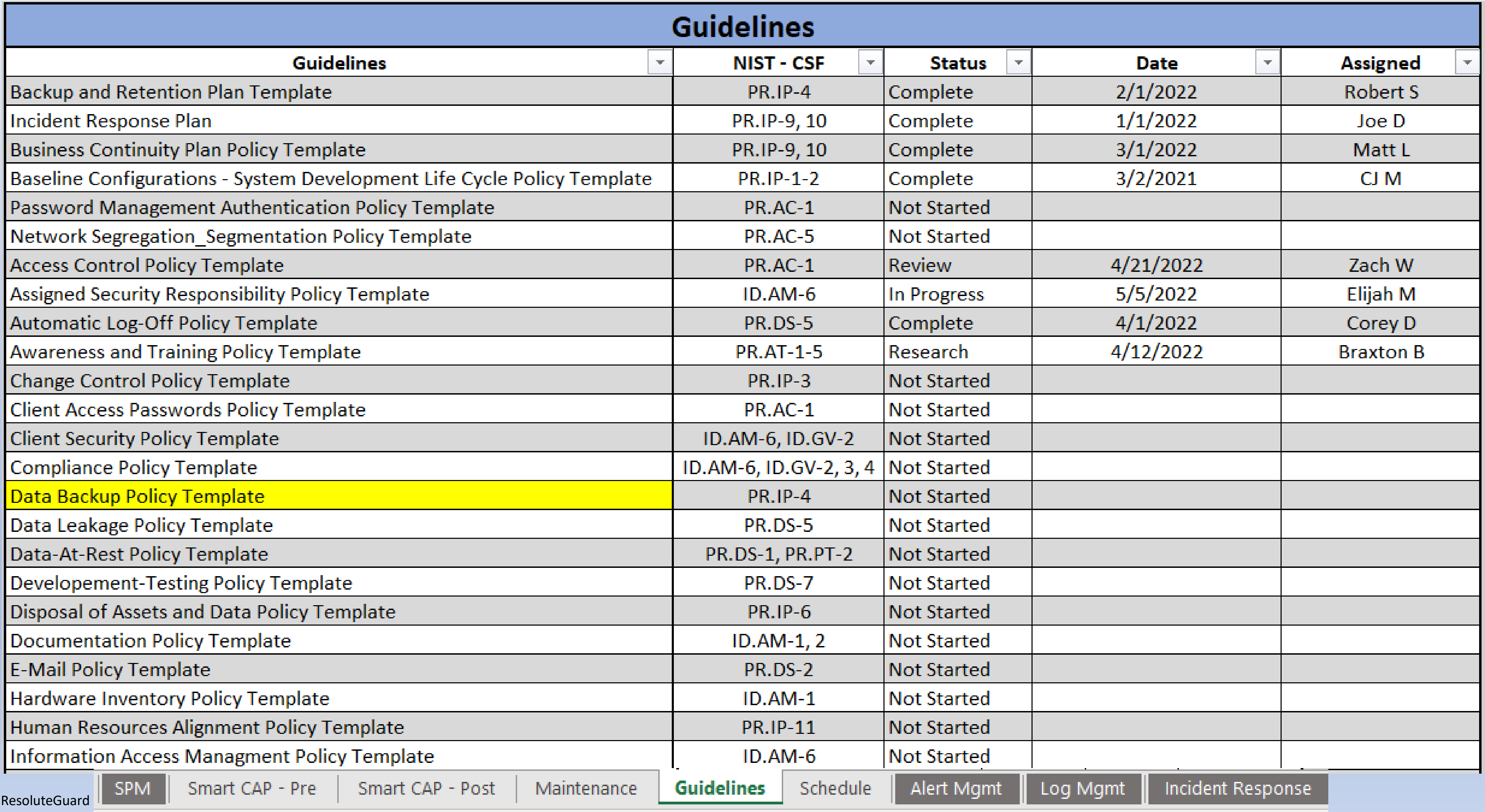
Backup systems implemented and not tested or planned increase operational risk for Organizations. The impacts of data loss events can include one or more of the following:

A. loss of productivity
B. revenue/customer loss
C. negative reputation and brand impacts
D. Loss of [Company] Confidential or Protected information

Reference

- NIST SP800-53, Rev 4 CP-9 Contingency Planning Information Systems Backup:

Worksheet Contains Links to Written Policy Templates- Important to Complete As Solutions Are Put In Place



Guidelines

Guidelines	NIST - CSF	Status	Date	Assigned
Backup and Retention Plan Template	PR.IP-4	Complete	2/1/2022	Robert S
Incident Response Plan	PR.IP-9, 10	Complete	1/1/2022	Joe D
Business Continuity Plan Policy Template	PR.IP-9, 10	Complete	3/1/2022	Matt L
Baseline Configurations - System Development Life Cycle Policy Template	PR.IP-1-2	Complete	3/2/2021	CJ M
Password Management Authentication Policy Template	PR.AC-1	Not Started		
Network Segregation_Segmentation Policy Template	PR.AC-5	Not Started		
Access Control Policy Template	PR.AC-1	Review	4/21/2022	Zach W
Assigned Security Responsibility Policy Template	ID.AM-6	In Progress	5/5/2022	Elijah M
Automatic Log-Off Policy Template	PR.DS-5	Complete	4/1/2022	Corey D
Awareness and Training Policy Template	PR.AT-1-5	Research	4/12/2022	Braxton B
Change Control Policy Template	PR.IP-3	Not Started		
Client Access Passwords Policy Template	PR.AC-1	Not Started		
Client Security Policy Template	ID.AM-6, ID.GV-2	Not Started		
Compliance Policy Template	ID.AM-6, ID.GV-2, 3, 4	Not Started		
Data Backup Policy Template	PR.IP-4	Not Started		
Data Leakage Policy Template	PR.DS-5	Not Started		
Data-At-Rest Policy Template	PR.DS-1, PR.PT-2	Not Started		
Developement-Testing Policy Template	PR.DS-7	Not Started		
Disposal of Assets and Data Policy Template	PR.IP-6	Not Started		
Documentation Policy Template	ID.AM-1, 2	Not Started		
E-Mail Policy Template	PR.DS-2	Not Started		
Hardware Inventory Policy Template	ID.AM-1	Not Started		
Human Resources Alignment Policy Template	PR.IP-11	Not Started		
Information Access Managment Policy Template	ID.AM-6	Not Started		

“It Is Not IF, But WHEN”

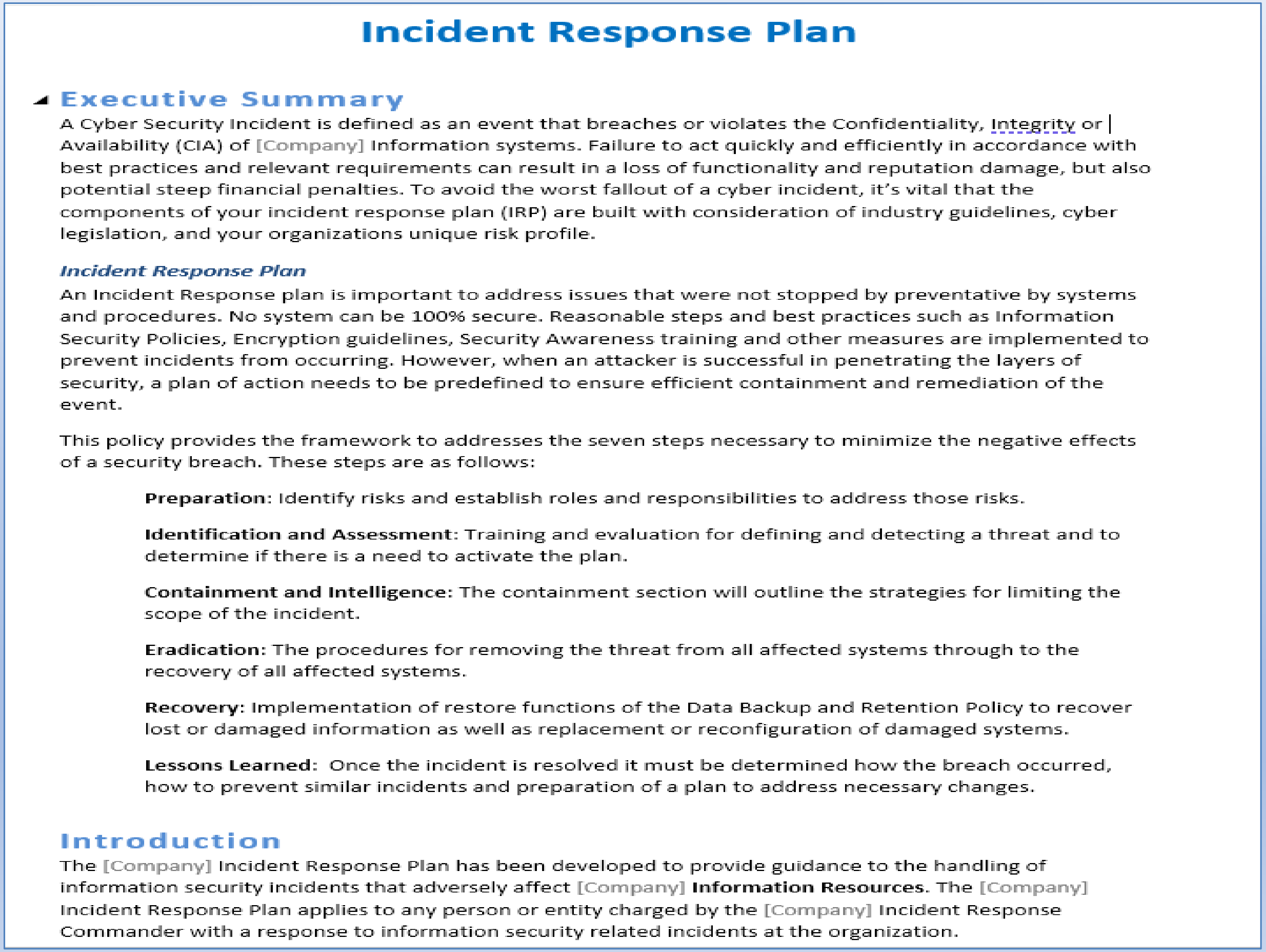
Prioritize Incident Response Readiness

1. Build a Comprehensive Incident Response Plan
2. Implement Solutions to Build “WHEN Attacked Resilience”
3. Manage the Activities That Fortify Your Readiness
    - Support Maintenance Listed in IRP Guidelines
    - Schedule Incident Response Practice Sessions

Protect Incidents From Becoming Disasters to Manage Potential Loss And Avoid A Disruption of Critical Community Services

RESOLUTE GUARD

"It Is Not IF, But WHEN"
Build Your Response Readiness to Prevent an Incident from Becoming a Disaster



Incident Response Plan

Executive Summary

A Cyber Security Incident is defined as an event that breaches or violates the Confidentiality, Integrity or Availability (CIA) of [Company] Information systems. Failure to act quickly and efficiently in accordance with best practices and relevant requirements can result in a loss of functionality and reputation damage, but also potential steep financial penalties. To avoid the worst fallout of a cyber incident, it's vital that the components of your incident response plan (IRP) are built with consideration of industry guidelines, cyber legislation, and your organizations unique risk profile.

Incident Response Plan

An Incident Response plan is important to address issues that were not stopped by preventative by systems and procedures. No system can be 100% secure. Reasonable steps and best practices such as Information Security Policies, Encryption guidelines, Security Awareness training and other measures are implemented to prevent incidents from occurring. However, when an attacker is successful in penetrating the layers of security, a plan of action needs to be predefined to ensure efficient containment and remediation of the event.

This policy provides the framework to addresses the seven steps necessary to minimize the negative effects of a security breach. These steps are as follows:

Preparation: Identify risks and establish roles and responsibilities to address those risks.

Identification and Assessment: Training and evaluation for defining and detecting a threat and to determine if there is a need to activate the plan.

Containment and Intelligence: The containment section will outline the strategies for limiting the scope of the incident.

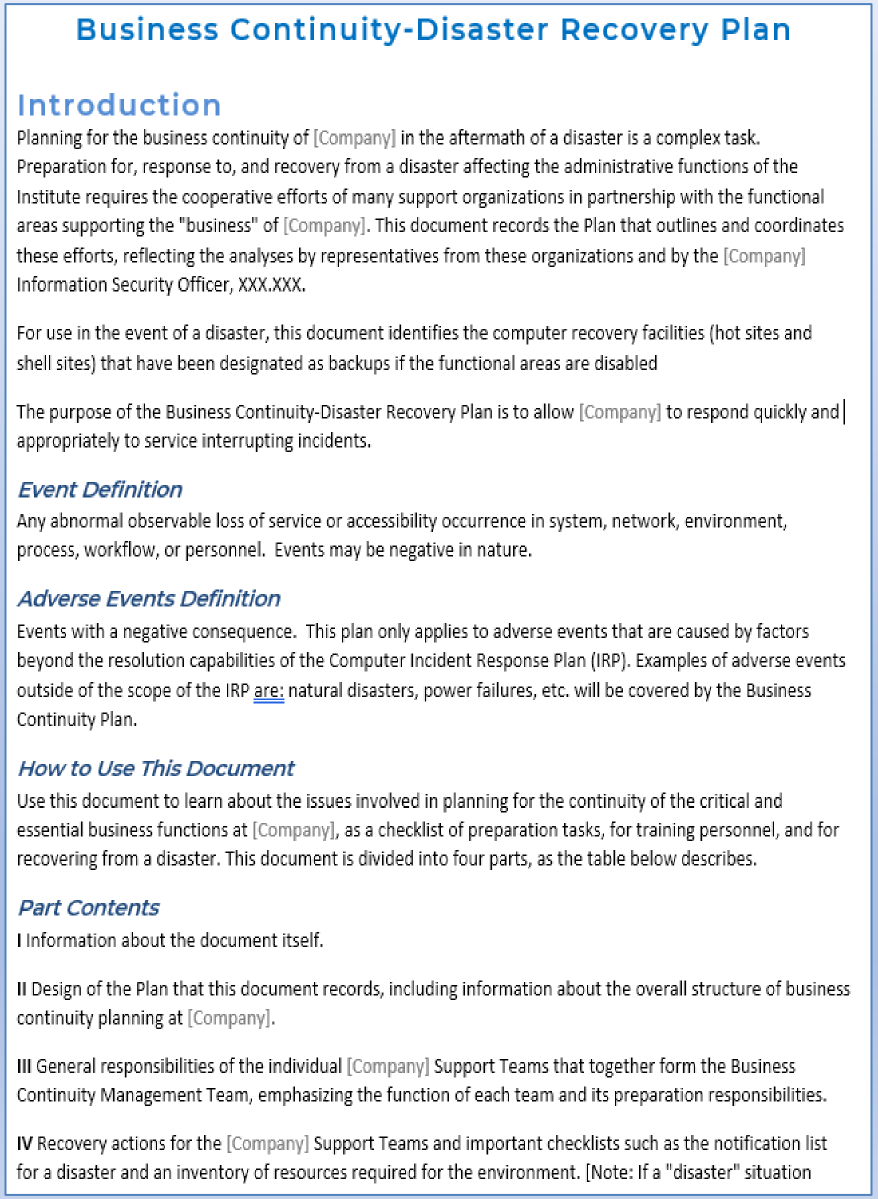
Eradication: The procedures for removing the threat from all affected systems through to the recovery of all affected systems.

Recovery: Implementation of restore functions of the Data Backup and Retention Policy to recover lost or damaged information as well as replacement or reconfiguration of damaged systems.

Lessons Learned: Once the incident is resolved it must be determined how the breach occurred, how to prevent similar incidents and preparation of a plan to address necessary changes.

Introduction

The [Company] Incident Response Plan has been developed to provide guidance to the handling of information security incidents that adversely affect [Company] **Information Resources**. The [Company] Incident Response Plan applies to any person or entity charged by the [Company] Incident Response Commander with a response to information security related incidents at the organization.



Business Continuity-Disaster Recovery Plan

Introduction

Planning for the business continuity of [Company] in the aftermath of a disaster is a complex task. Preparation for, response to, and recovery from a disaster affecting the administrative functions of the Institute requires the cooperative efforts of many support organizations in partnership with the functional areas supporting the "business" of [Company]. This document records the Plan that outlines and coordinates these efforts, reflecting the analyses by representatives from these organizations and by the [Company] Information Security Officer, XXX.XXX.

For use in the event of a disaster, this document identifies the computer recovery facilities (hot sites and shell sites) that have been designated as backups if the functional areas are disabled

The purpose of the Business Continuity-Disaster Recovery Plan is to allow [Company] to respond quickly and appropriately to service interrupting incidents.

Event Definition

Any abnormal observable loss of service or accessibility occurrence in system, network, environment, process, workflow, or personnel. Events may be negative in nature.

Adverse Events Definition

Events with a negative consequence. This plan only applies to adverse events that are caused by factors beyond the resolution capabilities of the Computer Incident Response Plan (IRP). Examples of adverse events outside of the scope of the IRP are: natural disasters, power failures, etc. will be covered by the Business Continuity Plan.

How to Use This Document

Use this document to learn about the issues involved in planning for the continuity of the critical and essential business functions at [Company], as a checklist of preparation tasks, for training personnel, and for recovering from a disaster. This document is divided into four parts, as the table below describes.

Part Contents

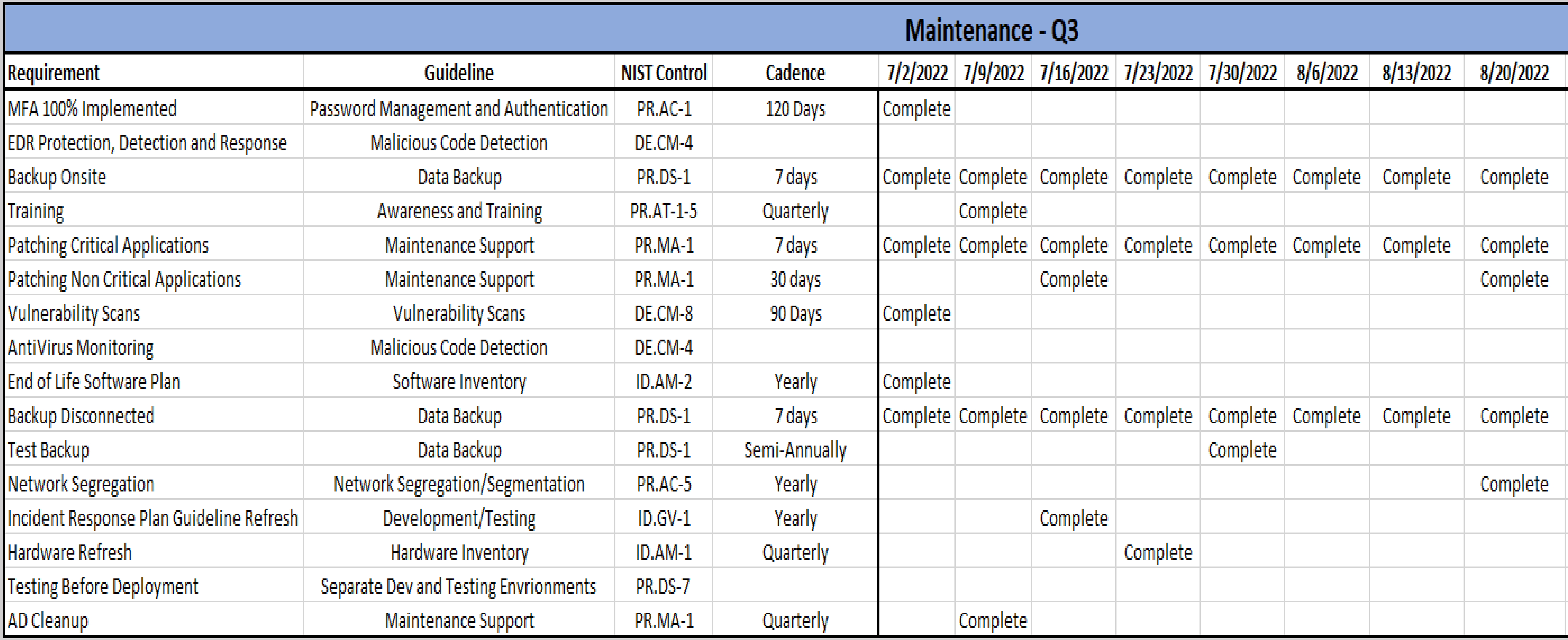
I Information about the document itself.

II Design of the Plan that this document records, including information about the overall structure of business continuity planning at [Company].

III General responsibilities of the individual [Company] Support Teams that together form the Business Continuity Management Team, emphasizing the function of each team and its preparation responsibilities.

IV Recovery actions for the [Company] Support Teams and important checklists such as the notification list for a disaster and an inventory of resources required for the environment. [Note: If a "disaster" situation

Manage the Maintenance Activities that Fortify Solutions in Place

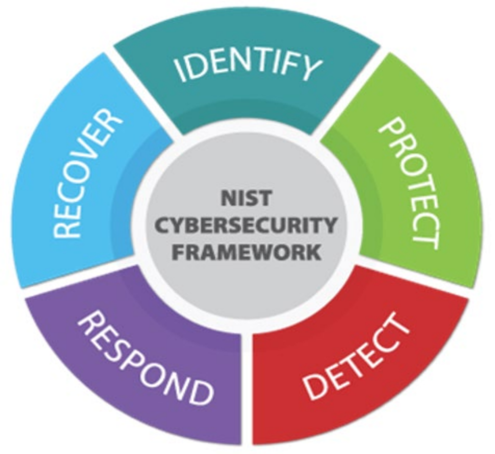


				Maintenance - Q3							
Requirement	Guideline	NIST Control	Cadence	7/2/2022	7/9/2022	7/16/2022	7/23/2022	7/30/2022	8/6/2022	8/13/2022	8/20/2022
MFA 100% Implemented	Password Management and Authentication	PR.AC-1	120 Days	Complete							
EDR Protection, Detection and Response	Malicious Code Detection	DE.CM-4									
Backup Onsite	Data Backup	PR.DS-1	7 days	Complete	Complete	Complete	Complete	Complete	Complete	Complete	Complete
Training	Awareness and Training	PR.AT-1-5	Quarterly		Complete						
Patching Critical Applications	Maintenance Support	PR.MA-1	7 days	Complete	Complete	Complete	Complete	Complete	Complete	Complete	Complete
Patching Non Critical Applications	Maintenance Support	PR.MA-1	30 days			Complete					Complete
Vulnerability Scans	Vulnerability Scans	DE.CM-8	90 Days	Complete							
AntiVirus Monitoring	Malicious Code Detection	DE.CM-4									
End of Life Software Plan	Software Inventory	ID.AM-2	Yearly	Complete							
Backup Disconnected	Data Backup	PR.DS-1	7 days	Complete	Complete	Complete	Complete	Complete	Complete	Complete	Complete
Test Backup	Data Backup	PR.DS-1	Semi-Annually					Complete			
Network Segregation	Network Segregation/Segmentation	PR.AC-5	Yearly								Complete
Incident Response Plan Guideline Refresh	Development/Testing	ID.GV-1	Yearly			Complete					
Hardware Refresh	Hardware Inventory	ID.AM-1	Quarterly				Complete				
Testing Before Deployment	Separate Dev and Testing Envrionments	PR.DS-7									
AD Cleanup	Maintenance Support	PR.MA-1	Quarterly		Complete						

RESOLUTE GUARD

Industry Best Internal / External Scanning Tools

Identify Strengths and Weaknesses in Alignment with Regulatory Objectives



in Accordance with the United States

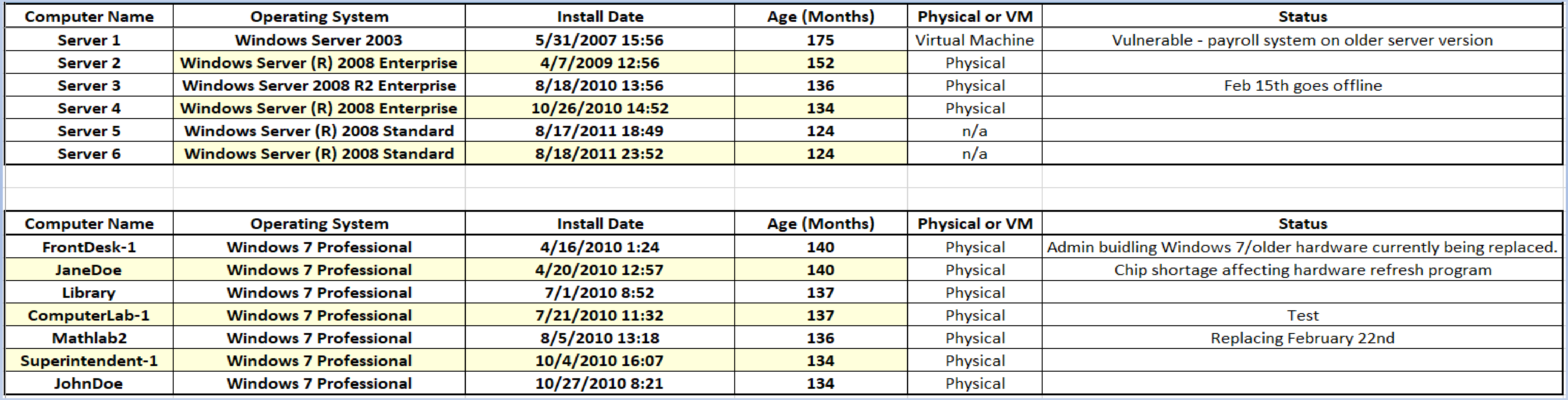
National Institute of Standards & Technology Cyber Security Framework (NIST-CSF)

Universal "Gold Standard" Framework Mandated / Recommended as a Basis For All Government Programs

Continuously Updated With Newly Identified Cyber Risk

Network Scans are Conducted to Document Your Current NIST-CSF based Internal and External Software and Hardware Strengths and Weaknesses

Anti-Virus, Anti-Spyware, Patching, Firewalls, Data Backup, MFA, Password and Access Management, Email filtering, Employee Training, Inactive Computers and Users, External Listening Port Vulnerabilities, Operating Systems and Software No Longer Supported, etc.

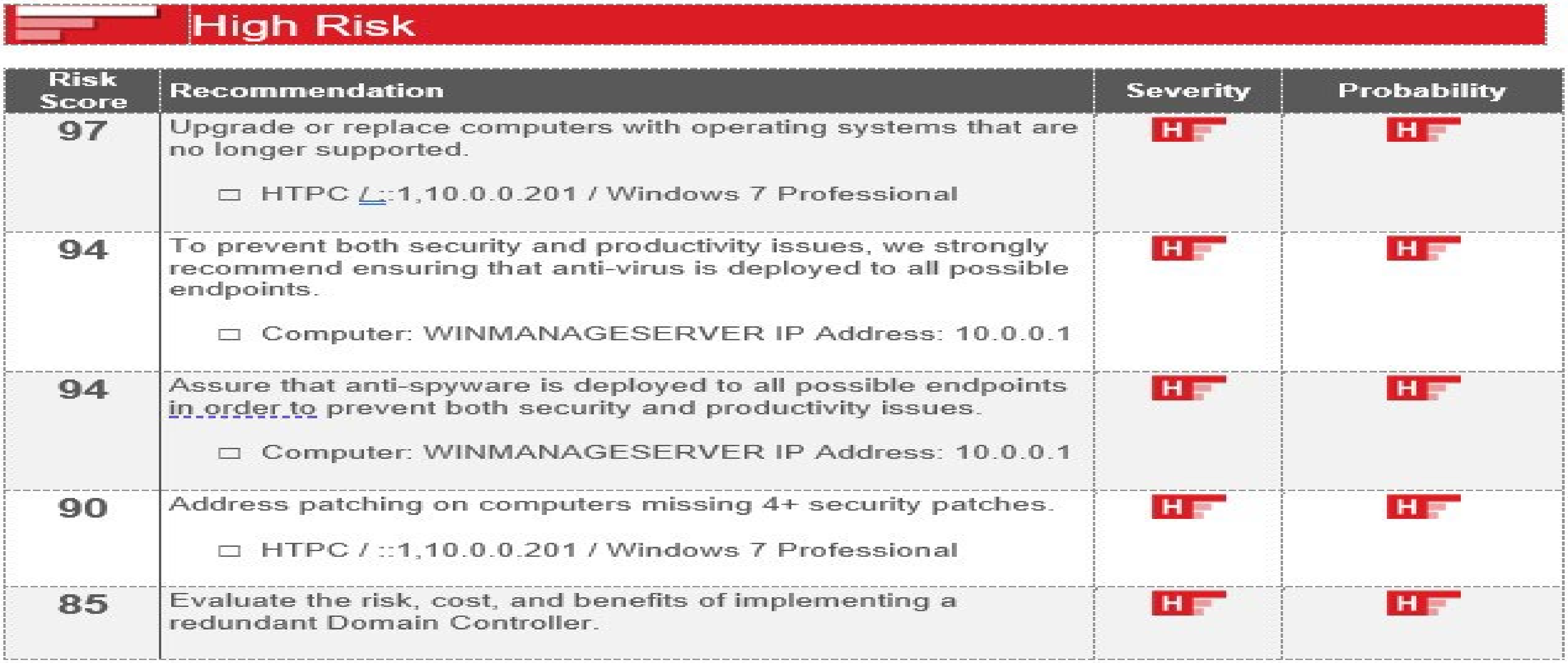


Computer Name	Operating System	Install Date	Age (Months)	Physical or VM	Status
Server 1	Windows Server 2003	5/31/2007 15:56	175	Virtual Machine	Vulnerable - payroll system on older server version
Server 2	Windows Server (R) 2008 Enterprise	4/7/2009 12:56	152	Physical	
Server 3	Windows Server 2008 R2 Enterprise	8/18/2010 13:56	136	Physical	Feb 15th goes offline
Server 4	Windows Server (R) 2008 Enterprise	10/26/2010 14:52	134	Physical	
Server 5	Windows Server (R) 2008 Standard	8/17/2011 18:49	124	n/a	
Server 6	Windows Server (R) 2008 Standard	8/18/2011 23:52	124	n/a	

Computer Name	Operating System	Install Date	Age (Months)	Physical or VM	Status
FrontDesk-1	Windows 7 Professional	4/16/2010 1:24	140	Physical	Admin buidling Windows 7/older hardware currently being replaced.
JaneDoe	Windows 7 Professional	4/20/2010 12:57	140	Physical	Chip shortage affecting hardware refresh program
Library	Windows 7 Professional	7/1/2010 8:52	137	Physical	
ComputerLab-1	Windows 7 Professional	7/21/2010 11:32	137	Physical	Test
Mathlab2	Windows 7 Professional	8/5/2010 13:18	136	Physical	Replacing February 22nd
Superintendent-1	Windows 7 Professional	10/4/2010 16:07	134	Physical	
JohnDoe	Windows 7 Professional	10/27/2010 8:21	134	Physical	

Prioritized Technical Action Scan Result Reports Are Reviewed For Members To Address Their Current Vulnerabilities

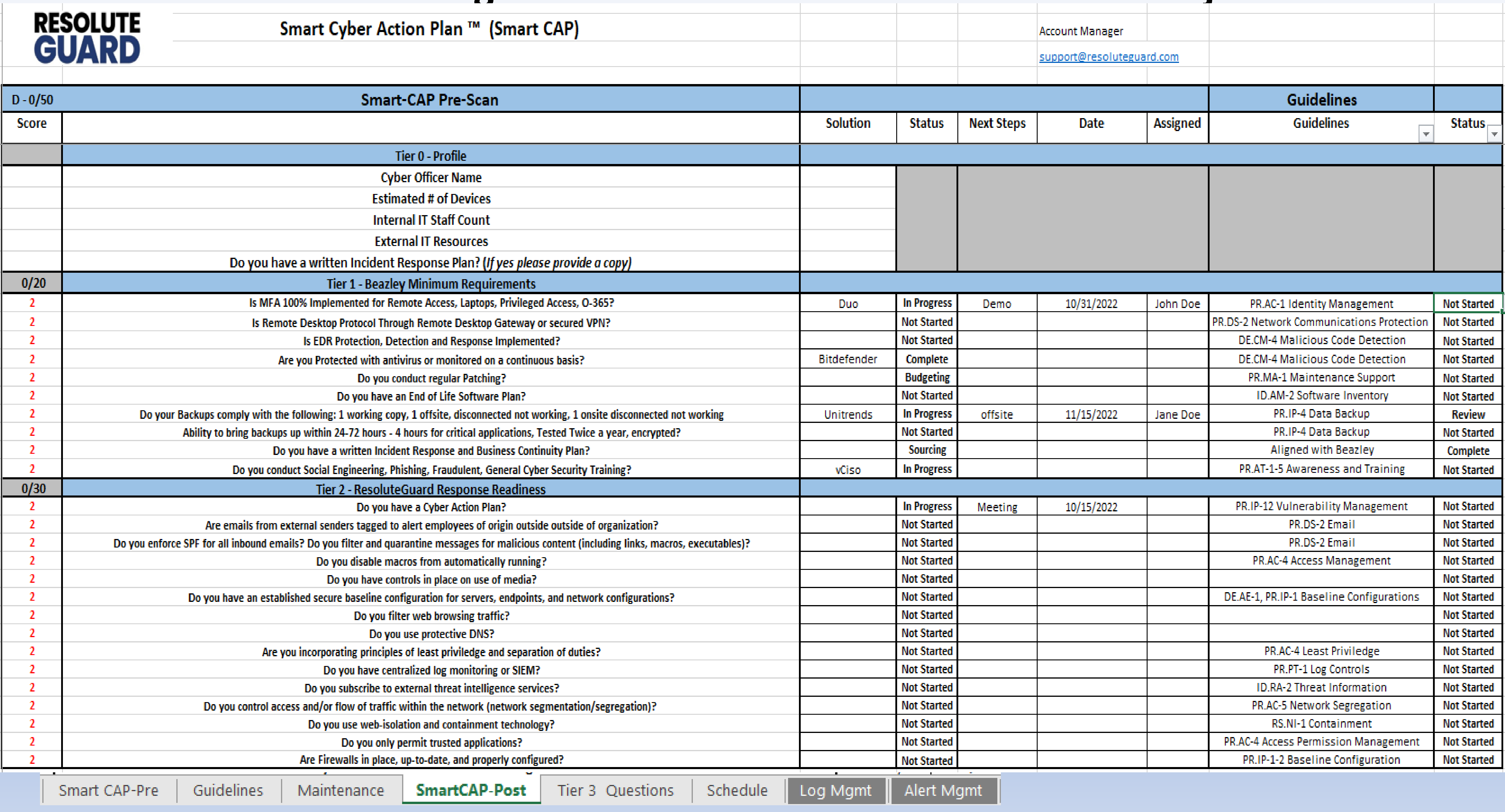
Immediate Action List



High Risk

Risk Score	Recommendation	Severity	Probability
97	Upgrade or replace computers with operating systems that are no longer supported. □ HTPC / ::1,10.0.0.201 / Windows 7 Professional	H	H
94	To prevent both security and productivity issues, we strongly recommend ensuring that anti-virus is deployed to all possible endpoints. □ Computer: WINMANAGESERVER IP Address: 10.0.0.1	H	H
94	Assure that anti-spyware is deployed to all possible endpoints in order to prevent both security and productivity issues. □ Computer: WINMANAGESERVER IP Address: 10.0.0.1	H	H
90	Address patching on computers missing 4+ security patches. □ HTPC / ::1,10.0.0.201 / Windows 7 Professional	H	H
85	Evaluate the risk, cost, and benefits of implementing a redundant Domain Controller.	H	H

SMART-CAP's Align Insured Workflow With Insurance Objectives



RESOLUTE GUARD

Smart Cyber Action Plan ™ (Smart CAP)

Account Manager

support@resoluteguard.com

D - 0/50	Smart-CAP Pre-Scan						Guidelines	
Score		Solution	Status	Next Steps	Date	Assigned	Guidelines	Status
	Tier 0 - Profile							
	Cyber Officer Name							
	Estimated # of Devices							
	Internal IT Staff Count							
	External IT Resources							
	Do you have a written Incident Response Plan? (*If yes please provide a copy*)							
0/20	Tier 1 - Beazley Minimum Requirements							
2	Is MFA 100% Implemented for Remote Access, Laptops, Privileged Access, O-365?	Duo	In Progress	Demo	10/31/2022	John Doe	PR.AC-1 Identity Management	Not Started
2	Is Remote Desktop Protocol Through Remote Desktop Gateway or secured VPN?		Not Started				PR.DS-2 Network Communications Protection	Not Started
2	Is EDR Protection, Detection and Response Implemented?		Not Started				DE.CM-4 Malicious Code Detection	Not Started
2	Are you Protected with antivirus or monitored on a continuous basis?	Bitdefender	Complete				DE.CM-4 Malicious Code Detection	Not Started
2	Do you conduct regular Patching?		Budgeting				PR.MA-1 Maintenance Support	Not Started
2	Do you have an End of Life Software Plan?		Not Started				ID.AM-2 Software Inventory	Not Started
2	Do your Backups comply with the following: 1 working copy, 1 offsite, disconnected not working, 1 onsite disconnected not working	Unitrends	In Progress	offsite	11/15/2022	Jane Doe	PR.IP-4 Data Backup	Review
2	Ability to bring backups up within 24-72 hours - 4 hours for critical applications, Tested Twice a year, encrypted?		Not Started				PR.IP-4 Data Backup	Not Started
2	Do you have a written Incident Response and Business Continuity Plan?		Sourcing				Aligned with Beazley	Complete
2	Do you conduct Social Engineering, Phishing, Fraudulent, General Cyber Security Training?	vCiso	In Progress				PR.AT-1-5 Awareness and Training	Not Started
0/30	Tier 2 - ResoluteGuard Response Readiness							
2	Do you have a Cyber Action Plan?		In Progress	Meeting	10/15/2022		PR.IP-12 Vulnerability Management	Not Started
2	Are emails from external senders tagged to alert employees of origin outside outside of organization?		Not Started				PR.DS-2 Email	Not Started
2	Do you enforce SPF for all inbound emails? Do you filter and quarantine messages for malicious content (including links, macros, executables)?		Not Started				PR.DS-2 Email	Not Started
2	Do you disable macros from automatically running?		Not Started				PR.AC-4 Access Management	Not Started
2	Do you have controls in place on use of media?		Not Started					Not Started
2	Do you have an established secure baseline configuration for servers, endpoints, and network configurations?		Not Started				DE.AE-1, PR.IP-1 Baseline Configurations	Not Started
2	Do you filter web browsing traffic?		Not Started					Not Started
2	Do you use protective DNS?		Not Started					Not Started
2	Are you incorporating principles of least priviledge and separation of duties?		Not Started				PR.AC-4 Least Priviledge	Not Started
2	Do you have centralized log monitoring or SIEM?		Not Started				PR.PT-1 Log Controls	Not Started
2	Do you subscribe to external threat intelligence services?		Not Started				ID.RA-2 Threat Information	Not Started
2	Do you control access and/or flow of traffic within the network (network segmentation/segregation)?		Not Started				PR.AC-5 Network Segregation	Not Started
2	Do you use web-isolation and containment technology?		Not Started				RS.NI-1 Containment	Not Started
2	Do you only permit trusted applications?		Not Started				PR.AC-4 Access Permission Management	Not Started
2	Are Firewalls in place, up-to-date, and properly configured?		Not Started				PR.IP-1-2 Baseline Configuration	Not Started

Progress & Change is Reviewed Every 90 Days

Internal / External Scan Updates Your “**Strengths and Weaknesses**”

Incorporates Progress Made and Any Newly Identified NIST-CSF Risks

Updates & Re-Prioritizes Cyber Action Plan (SMART-CAP) Activities by Risk of Loss

Smart Workflow Management Supports Continuous Improvement

RESOLUTE
GUARD

In Summary ”Easy To Use” SMART- Cyber Action Plans

Translate Technical Language into Easy-to-Understand Reports and Guidelines

Are Customized To Validate Compliance with Specific 2022-2023 Insurance Company Requirements

Prioritize Protecting A Cyber-Incident from Becoming a “Disruption of Critical Service Disaster”

Conduct Scans to Identify and Document Your Internal & External “Strengths and Weaknesses”

Align Continuous Improvement Objectives with Evolving NIST-CSF Based Control Requirements

RESOLUTE GUARD

Questions?

Next Steps

1. Click here to Sign the Pre-approved “Services Agreement”
2. ResoluteGuard Schedules Program Overview Call
3. ResoluteGuard Scan & Schedule Report Review

RESOLUTE
GUARD

NEXT STEPS

1. Click here to Sign the Pre-approved “Services Agreement”
2. ResoluteGuard Schedules Program Overview Call
3. ResoluteGuard Scan & Schedule Report Review

support@resoluteguard.com

888-728-6030

RESOLUTE GUARD

“Easy to Understand” Data Collector Process

1- INTERNALLY scan to identify status of:

Azure and Microsoft Office 365 Cloud Services
Local servers and computers versions
Software applications and user-access

2- Individually scans:

LINUX and MAC OS (non-Windows) devices on your network.
SQL Databases for unencrypted Personal Identifiable Information (PII)
EXTERNAL ports for open, unsecure, outdated services and listening agents

3- Provides “current status” reports and diagrams, prioritized by risk, to create Cyber Action Plan:

Back-up, firewall, incident response, and business continuity plans
OS, inactive computers, application and endpoint Patches, endpoint Security
Inactive Users, user access permissions and shares, PII management

RESOLUTE GUARD

“Easy to Use” Data Collector

“Easy to use” data collector software is locally installed and requires no hardware.

Safe and non-disruptive, causes no conflict with other applications or firewalls, and requires zero maintenance.

A 30-minute remote call is set with your assigned resource to activate the tool and collect all your hardware, software and network “strengths and weaknesses” data.

This provides a comprehensive documented view of your current environment.

Knowing “where you are” empowers you to identify the best steps to
“Do the Best You Can as Fast As You Can”