[logo]

Governance, Risk, and Compliance (GRC) Program Plan

Contents

[Mission and Vision 3](#_Toc139205062)

[Purpose 3](#_Toc139205063)

[Scope 3](#_Toc139205064)

[Governance Structure 3](#_Toc139205065)

[Plan Deficiencies 3](#_Toc139205066)

[Review 4](#_Toc139205067)

[Documentation 4](#_Toc139205068)

[Effectiveness of Controls 4](#_Toc139205069)

[Risks 5](#_Toc139205070)

[Internal Assessments 6](#_Toc139205071)

[External Assessments 6](#_Toc139205072)

[Appendix A – Control Review Schedule and Evidence Example Chart 7](#_Toc139205073)

# Mission and Vision

At **[ORGANIZATION NAME]**, we are dedicated to upholding the security and resilience of our information systems and data, which are integral to our organizational values. Our executive leadership is fully committed to ensuring that the organization adheres to prescribed requirements, enabling us to maintain a robust cybersecurity posture.

# Purpose

This document provides comprehensive guidance for the ongoing maintenance of our Governance, Risk, and Compliance program ("program"). It serves as a valuable resource, offering direction to GRC stakeholders on the necessary requirements for fostering and ensuring the confidentiality, integrity, and availability of our systems and data.

# Scope

The program encompasses all information systems, data, and GRC stakeholders within our organization. It is designed to address the needs and responsibilities related to the program's successful implementation.

# Governance Structure

The program's success and sustainability rest on the collective efforts of our GRC stakeholders. The following chart outlines the specific roles and responsibilities assigned to each stakeholder, highlighting their vital contributions to the program's effectiveness and longevity.

|  |  |  |
| --- | --- | --- |
| **Title** | **Role** | **Responsibilities** |
|  | Executive Leadership | Approval and support |
|  | Chief Technology Officer / Director | Adoption and enforcement |
|  | Security Analyst/Internal Assessor | Adherence and confirmation |
|  | IT Staff | Technical support |
|  | Data Owner | Data management |
|  | Operations Managers | Operational support |
|  | Human Resources | Acceptance and disciplinary |
|  | Legal | Alignment with rules and regulations |

# Plan Deficiencies

Deficiencies identified within the program shall be effectively managed through a comprehensive Plan of Action and Milestones (POAAM). Each deficiency within the POAAM should include the following components:

* Milestones – These represent significant steps involved in remediating the identified deficiency.
* Responsibility – Key individuals responsible for the remediation process should be clearly identified.
* Estimated dates of completion – Approximate dates should be provided to indicate when the deficiency is expected to be fully addressed.

The acting Technology Officer holds the responsibility for ensuring that all deficiencies in the plan are promptly and appropriately addressed. Other members of the GRC team are responsible for reporting deficiencies and ensuring adequate communication with the acting Technology Officer.

Additionally, the Technology Officer is accountable for consulting and informing Executive Leadership about any issues that may hinder the effective application of the program. Executive Leadership, in turn, assumes responsibility for addressing these matters consistent with the organization's Mission, Vision, and Values.

# Review

The Technology Officer will be responsible for coordinating activities related to reviewing key aspects of the program. Activities shall be documented with updates noted in relevant supporting documentation. Records should be created and maintained in accordance with the organization’s defined records retention requirements.

## Documentation

This comprehensive review will entail an examination of all supporting program documentation. The chart below shows the activities to be undertaken and their respective frequencies for review and update.

|  |  |
| --- | --- |
| **Documents** | **Frequency (minimum)** |
| POAAM | Quarterly |
| Policies | Annually |
| Plans | Annually |
| Standards | Annually |

Updates to documentation will contain the date and a summary of changes within the document register.

## Effectiveness of Controls

To ensure the ongoing effectiveness of controls, a systematic review process will be implemented. Ongoing review of deployed controls (administrative and technical) will be analyzed against new and emerging threats, as well as any potential residual risk which may be inherent within the organization. Aspects such as cost, impact, end-of-life/end-of-support, and manageability shall be considered as aspects of the overall review.

While this analysis can be performed at any time, the following chart outlines the minimal review

|  |  |  |  |
| --- | --- | --- | --- |
| **Controls** | **Mission** | **Frequency** | **Period** |
| Plan Documentation | GRC | Annually | 1st quarter |
| Incident Response (IR) Plan Review | IR Plan Update | Annually | 1st quarter |
| IR Practice | IR Team Training | Annually | 1st quarter |
| Risk Management (RM) Plan and Worksheet Review | RM Plan Update | Annually | 1st quarter |
| Vendor Risk Management Worksheet1 | RM Plan Update | Annually | 1st quarter |
| Vulnerability Management (VM) Plan Review | VM Plan Update | Annually | 2nd quarter |
| VM Events Review | VM Plan Update | Monthly | All quarters |
| VM Data Flows and Baseline Alerts Review | VM Plan Update | Annually | 2nd quarter |
| Access Control (AC) Plan Review | AC Plan Update | Annually | 3rd quarter |
| Active Directory Account Management Review for Privileged Users and Critical Staff | AC Plan | Monthly | All quarters |
| Active Directory Account Management Review for Non-Privileged Users and Non-Critical Staff | AC Plan | Biannually | 2 defined months |
| Critical Staff Plan Review | Critical Staff Plan | Annually | 3rd quarter |
| Sample Audit of Shared Folders | Critical Staff Plan | Annually | 3rd quarter |
| Vendor Roles and Responsibilities Review | Vendor Mgmt Update | Annually | 3rd quarter |
| Vendor Priorities and Assessments | Vendor Mgmt Update | Annually | 3rd quarter |
| Vendor Contract Review | Vendor Mgmt Update | Annually | 3rd quarter |
| Vendor Assessments, Audits and Evaluations | Vendor Mgmt Update | Annually | 3rd quarter |
| Vendor IR Response Review | Vendor Mgmt Update | Annually | 3rd quarter |
| Staff and Teacher Cybersecurity Awareness Review | Board Policy | Annually | 3rd quarter |
| Student Cybersecurity Awareness Review | Board Policy | Annually | 3rd quarter |
| Information Technology System Maintenance Plan Review | Information Technology System Maintenance Plan | Annually | 4th quarter |
| Firewall Perimeter Protection Rules | Information Technology System Maintenance Plan | Annually | 4th quarter |
| Email Filtering Protection Rules | Information Technology System Maintenance Plan | Annually | 4th quarter |
| Switch Protection Configuration | Information Technology System Maintenance Plan | Annually | 4th quarter |
| Endpoint Antivirus Protection Rules | Information Technology System Maintenance Plan | Annually | 4th quarter |
| VM Detection Protection Rules | Information Technology System Maintenance Plan | Annually | 4th quarter |

## Risks

Effective identification, assessing, mitigating, and monitoring constitute the activities required within Risk Management. These activities provide assurance that organizational risk is minimized and effectively managed throughout the asset’s life cycle.

Ongoing activities, such as vulnerability scans, assessments, scenarios, compliance and regulatory reviews, surveys, lessons learned, near-miss analysis, and risk registry review are methods which may identify risks. The following table outlines activities that are required for regular review.

|  |  |  |  |
| --- | --- | --- | --- |
| **Risk Type** | **Details** | **Frequency** | **Period** |
| Root Cause Analysis | Overall review of lessons learned and near-miss incidents | Immediately | All quarters |
| Vulnerability Management | New, existing, and remediated vulnerabilities | Monthly | All quarters |
| Asset Supportability and Patching | Analysis of assets end-of-life/end-of-support | Annually | 1st quarter |
| Partner Risk Management | Service Level Agreement, Shared Responsibility Matrix, and support contract review | Annually | 1st quarter |
| Risk Register | Evaluate of risks that cannot be fully remediated | Annually | 1st quarter |
| Supply Chain Risk Management | Review Service Level Agreements and support contract review | Annually | 1st quarter |

# Internal Assessments

An internal assessment (sometimes called an internal audit) is an independent evaluation of an organization's internal controls and processes. It assesses the effectiveness of risk management, governance, and compliance efforts. Through testing and analysis, internal assessors identify control deficiencies, provide recommendations for improvement, and enhance transparency and accountability within the organization.

Actions performed shall include some or all of the following including departmental interviews, observations via walk throughs or spot checks, and evidence gathering through sampling methods. Audits shall be conducted in an unbiased and ethical fashion as a proactive method of assurance.

The chart in **Appendix A** outlines the expected evidence required to satisfy the control, along with the Periods for which each should be tested. Outcomes from the tests shall be reported and made available to all relevant stakeholders.

# External Assessments

An external assessment (sometimes called an external audit) is an independent examination of an organization's controls and processes by an independent firm. Its primary purpose is to provide an objective assessment of the accuracy, reliability, and compliance requirements. External assessors conduct testing, analysis, and verification to ensure that the security and compliance practices present a true and fair view of the organization's position, giving confidence to stakeholders and enhancing trust in the GRC program.

The Ohio Cyber Reserve is an organization that is able to conduct the external assessment.

|  |  |  |  |
| --- | --- | --- | --- |
| **Assessment Type** | **Details** | **Frequency** | **Period** |
| Regulation/Compliance | Regular governance and compliance attestation/certification | Annually |  |
| Data Security Assessment | General review of cybersecurity | Annually |  |
| Penetration Test | Testing of technical controls | Annually |  |

# Appendix A – Control Review Schedule and Evidence Example Chart

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Function** | **Category** | **Sub ID** | **Subcategory** | **Evidence Example** | **Period** |
| **IDENTIFY (ID)** | **Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization’s risk strategy. | ID.AM-1 | Physical devices and systems within the organization are inventoried | Complete list of physical devices and systems within the organization. |  |
| ID.AM-2 | Software platforms and applications within the organization are inventoried | Complete list of software platforms and applications within the organization |  |
| ID.AM-3 | Organizational communication and data flows are mapped | Organizational and departmental data flows reviewed. |  |
| ID.AM-4 | External information systems are catalogued | Complete list of external information systems. |  |
| ID.AM-5 | Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value | Staff with Critical Data Security Procedure. Staff with Critical Data Annual Validation and Verifications. |  |
| ID.AM-6 | Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established | Complete list of key players by roles and responsibilities for the organization and third party as shown in the IR plan. |  |
| **Business Environment (ID.BE):** The organization’s mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions. | ID.BE-1 | The organization’s role in the supply chain is identified and communicated | Organization’s role in the supply chain is identified and communicated in school documentation, handbook, or website. |  |
| ID.BE-2 | The organization’s place in critical infrastructure and its industry sector is identified and communicated | Organization’s role in the critical infrastructure is identified and communicated in school documentation, handbook, or website. |  |
| ID.BE-3 | Priorities for organizational mission, objectives, and activities are established and communicated | Priorities for organizational mission, objectives, and activities are established and communicated in school documentation, handbook, or website. |  |
| ID.BE-4 | Dependencies and critical functions for delivery of critical services are established | School District Staff with Critical Data Plan and Checklist. Data Flows showing critical business functions. |  |
| ID.BE-5 | Resilience requirements to support delivery of critical services are established for all operating states (e.g., under duress/attack, during recovery, normal operations) | School District Staff with Critical Data Plan and Checklist Data flows. Risk Management Worksheet mitigation. Secondary systems. |  |
| **Governance (ID.GV):** The policies, procedures, and processes to manage and monitor the organization’s regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk. | ID.GV-1 | Organizational cybersecurity policy is established and communicated | School Board policies that define data security. |  |
| ID.GV-2 | Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners | IR plan has roles and responsibility. |  |
| ID.GV-3 | Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed | Legal and regulatory requirements regarding cybersecurity memo |  |
| ID.GV-4 | Governance and risk management processes address cybersecurity risks | Risk Assessment Plan and Worksheet.  Vendor Risk Assessment Worksheet. |  |
| **Risk Assessment (ID.RA):** The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals. | ID.RA-1 | Asset vulnerabilities are identified and documented | Risk Assessment Plan and Worksheet.  Vendor Risk Assessment Worksheet.  Vulnerability Management Plan and Review. |  |
| ID.RA-2 | Cyber threat intelligence is received from information sharing forums and sources | MS-ISAC reports Risk Assessment Plan and Worksheet.  Vendor Risk Assessment Worksheet. |  |
| ID.RA-3 | Threats, both internal and external, are identified and documented | Risk Assessment Plan and Worksheet Threat ID column. Vendor Risk Assessment Worksheet Threat ID column. |  |
| ID.RA-4 | Potential business impacts and likelihoods are identified | Risk Assessment Plan and Worksheet Likelihood and Impact column. Vendor Risk Assessment Worksheet Likelihood and Impact column. |  |
| ID.RA-5 | Threats, vulnerabilities, likelihoods, and impacts are used to determine risk | Risk Assessment Plan and Worksheet risk score. Vendor Risk Assessment Worksheet risk score. |  |
| ID.RA-6 | Risk responses are identified and prioritized | Risk Assessment Plan and Worksheet POAAM with highest risk on the top. Vendor Risk Assessment Worksheet POAAM with highest risk on the top. |  |
| **Risk Management Strategy (ID.RM):** The organization’s priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions. | ID.RM-1 | Risk management processes are established, managed, and agreed to by organizational stakeholders | Risk Assessment Plan and Worksheet signed off by identified executive (risk officer). Vendor Risk Assessment Worksheet signed off by identified executive (risk officer). |  |
| ID.RM-2 | Organizational risk tolerance is determined and clearly expressed | Risk Assessment Plan and Worksheet is completed with the risk officer’s responses. Vendor Risk Assessment Worksheet is completed with the risk officer’s responses. |  |
| ID.RM-3 | The organization’s determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis | Risk Assessment Plan and Worksheet. Vendor Risk Assessment Worksheet. Risk officer acceptance and report. |  |
| **Supply Chain Risk Management (ID.SC):** The organization’s priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks. | ID.SC-1 | Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders | Vendor Risk Assessment Plan and Worksheet. |  |
| ID.SC-2 | Suppliers and third-party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process | Vendor Risk Assessment Plan and Worksheet is sorted with high risks at the top. |  |
| ID.SC-3 | Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization’s cybersecurity program and Cyber Supply Chain Risk Management Plan. | Third party vendor contracts that show the vendor adheres to the organization's data security framework. |  |
| ID.SC-4 | Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations. | Third party vendor assessments, audits, and evaluations to the NIST CSF. |  |
| ID.SC-5 | Response and recovery planning and testing are conducted with suppliers and third-party providers | Third Party Vendors plans and test for response and recovery. |  |
| **PROTECT (PR)** | **Identity Management, Authentication and Access Control (PR.AC):** Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions. | PR.AC-1 | Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes | Access Control plan. Active Directory review. Active Directory privileged account review. Onboarding and off boarding procedures. Review of user account sampling |  |
| PR.AC-2 | Physical access to assets is managed and protected | Physical security inspection.  Background checks review. Vendor background checks review. |  |
| PR.AC-3 | Remote access is managed | Access Control plan. VPN review. Privileged access using remote connections. |  |
| PR.AC-4 | Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties | Access Control plan. School District Staff with Critical Data. |  |
| PR.AC-5 | Network integrity is protected (e.g., network segregation, network segmentation) | Access Control plan.  School District Staff with Critical Data. Staff with Critical Data Annual Validation and Verifications. |  |
| PR.AC-6 | Identities are proofed and bound to credentials and asserted in interactions | Check IDs. Access Control plan.  School District Staff with Critical Data. |  |
| PR.AC-7 | Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals’ security and privacy risks and other organizational risks) | System MFA. Password plan. Access Control plan.  School District Staff with Critical Data Plan. |  |
| **Awareness and Training (PR.AT):** The organization’s personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements. | PR.AT-1 | All users are informed and trained | Staff and Teachers Security Awareness Training Student Security Awareness Training |  |
| PR.AT-2 | Privileged users understand their roles and responsibilities | Access Control plan.  School District Staff with Critical Data. Staff with Critical Data Annual Validation and Verifications. |  |
| PR.AT-3 | Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities | IR Plan Vendor plan and review. |  |
| PR.AT-4 | Senior executives understand their roles and responsibilities | Senior Staff roles on IR plan (NIST) IR Plan |  |
| PR.AT-5 | Physical and cybersecurity personnel understand their roles and responsibilities | Senior Staff roles on IR plan (NIST) IR Plan |  |
| **Data Security (PR.DS):** Information and records (data) are managed consistent with the organization’s risk strategy to protect the confidentiality, integrity, and availability of information. | PR.DS-1 | Data-at-rest is protected | Data at Rest encryption - endpoints Data at Rest encryption - storage server Data at Rest encryption - backups |  |
| PR.DS-2 | Data-in-transit is protected | Email encryption Data at Rest encryption - endpoints Portal encryption for banking, ODE and other large transactions. |  |
| PR.DS-3 | Assets are formally managed throughout removal, transfers, and disposition | System Maintenance plan and review. Data Sanitization plan and review. |  |
| PR.DS-4 | Adequate capacity to ensure availability is maintained | Inspection of System capacity (%) |  |
| PR.DS-5 | Protections against data leaks are implemented | Data Leak Protection plan and review. |  |
| PR.DS-6 | Integrity checking mechanisms are used to verify software, firmware, and information integrity | Patching plan and review. System Maintenance Plan. |  |
| PR.DS-7 | The development and testing environment(s) are separate from the production environment | Look at any development from the last year and how it is tested before deployment. |  |
| PR.DS-8 | Integrity checking mechanisms are used to verify hardware integrity | System Maintenance Plan. Firmware review. |  |
| **Information Protection Processes and Procedures (PR.IP):** Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets. | PR.IP-1 | A baseline configuration of information technology / industrial control systems is created and maintained incorporating security principles (e.g., concept of least functionality) | Vulnerability Management Plan.  System baseline and alerts review. |  |
| PR.IP-2 | A System Development Life Cycle to manage systems is implemented | SDLC plan with Treasurer and TECHNOLOGY OFFICER. Refresh Cycle plan and review. |  |
| PR.IP-3 | Configuration change control processes are in place | System Maintenance Plan. Server Log Configuration Settings |  |
| PR.IP-4 | Backups of information are conducted, maintained, and tested | System Maintenance Plan. Backup recovery. Backup tests. |  |
| PR.IP-5 | Policy and regulations regarding the physical operating environment for organizational assets are met | See physical operating policies for the organization. Did they meet their requirements? |  |
| PR.IP-6 | Data is destroyed according to policy | Data Sanitization Plan. Certificates of Destruction review. Reconciliation reports for data bearing devices. |  |
| PR.IP-7 | Protection processes are improved | Policy and plans updates. Process with updates. |  |
| PR.IP-8 | Effectiveness of protection technologies is shared | Evidence of communication between individuals protecting data are improvements. |  |
| PR.IP-9 | Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed | Response and recovery plans are tested with the tabletop or other exercises. |  |
| PR.IP-10 | Response and recovery plans are tested | Response and recovery plans are tested with the tabletop or other exercises. Last IR test report. |  |
| PR.IP-11 | Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening) | Background checks for teachers and staff.  Admin background checks. |  |
| PR.IP-12 | A vulnerability management plan is developed and implemented | Vulnerability Management Plan Vulnerability Management Flow Diagram. ITC Vulnerability Management Flow Diagram. |  |
| **Maintenance (PR.MA):** Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures. | PR.MA-1 | Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools | Maintenance is logged in the ticketing system Information Technology System Maintenance Plan |  |
| PR.MA-2 | Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access | Maintenance is logged in the ticketing system Information Technology System Maintenance Plan |  |
| **Protective Technology (PR.PT):** Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements. | PR.PT-1 | Audit/log records are determined, documented, implemented, and reviewed in accordance with policy | Audit/log records are determined, documented, implemented, and reviewed |  |
| PR.PT-2 | Removable media is protected, and its use restricted according to policy | Removable media is protected. Use restricted according to policy. |  |
| PR.PT-3 | The principle of least functionality is incorporated by configuring systems to provide only essential capabilities | Principle of least functionality is incorporated. System configuring provides only essential capabilities. |  |
| PR.PT-4 | Communications and control networks are protected | Examine communications and control networks. |  |
| PR.PT-5 | Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations | Evaluate the organization's techniques and mechanism to achieve resilience. Check action plans from the risk assessment mitigations. |  |
| **DETECT (DE)** | **Anomalies and Events (DE.AE):** Anomalous activity is detected and the potential impact of events is understood. | DE.AE-1 | A baseline of network operations and expected data flows for users and systems is established and managed | Data flows show baseline network operations. |  |
| DE.AE-2 | Detected events are analyzed to understand attack targets and methods | Vulnerability Management Plan and review See sample of detected events analyzed to understand attack targets and methods and responded to CISA Albert, ITC and organizational reports |  |
| DE.AE-3 | Event data are collected and correlated from multiple sources and sensors | Vulnerability Management Plan and review. See sources and sensors plan. CISA Albert, ITC and organizational reports. |  |
| DE.AE-4 | Impact of events is determined | See impact of events as determined per VM plan. Inspect events in the ticketing log |  |
| DE.AE-5 | Incident alert thresholds are established | See incident alert thresholds are established for each platform by the ITC and the district. Vulnerability Management Plan |  |
| **Security Continuous Monitoring (DE.CM):** The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures. | DE.CM-1 | The network is monitored to detect potential cybersecurity events | Network monitoring plan and review CISA Cyber Hygiene program using Nessus and NMAP. Vulnerability Management Plan |  |
| DE.CM-2 | The physical environment is monitored to detect potential cybersecurity events | Physical security plan.  Critical data staff need physical security training. |  |
| DE.CM-3 | Personnel activity is monitored to detect potential cybersecurity events | Personnel activity is monitored to detect potential cybersecurity events using cameras and individual ID badges. Vulnerability Management Plan |  |
| DE.CM-4 | Malicious code is detected | See malicious code is detected with the antivirus software. Vulnerability Management Plan  Antivirus software on endpoints. |  |
| DE.CM-5 | Unauthorized mobile code is detected | See if unauthorized mobile code is sought out and detected. Vulnerability Management Plan  Antivirus software on endpoints.  CISA Cyber Hygiene program. |  |
| DE.CM-6 | External service provider activity is monitored to detect potential cybersecurity events | External service provider activity is monitored to detect potential cybersecurity events.  CISA Cyber Hygiene program. |  |
| DE.CM-7 | Monitoring for unauthorized personnel, connections, devices, and software is performed | Monitoring for unauthorized personnel, connections, devices, and software is performed. |  |
| DE.CM-8 | Vulnerability scans are performed | Vulnerability scans are performed. Vulnerability Management Plan Antivirus software on endpoints.  CISA Cyber Hygiene program. |  |
| **Detection Processes (DE.DP):** Detection processes and procedures are maintained and tested to ensure awareness of anomalous events. | DE.DP-1 | Roles and responsibilities for detection are well defined to ensure accountability | Roles and responsibilities for detection are well defined to ensure accountability in job functions IR plan. ITC VM plan. |  |
| DE.DP-2 | Detection activities comply with all applicable requirements | See detection activities comply with all applicable requirements for all activities. Vulnerability Management Plan. Antivirus software on endpoints.  CISA Cyber Hygiene program. |  |
| DE.DP-3 | Detection processes are tested | Detection processes are tested. Vulnerability Management Plan. Antivirus software on endpoints.  CISA Cyber Hygiene program. |  |
| DE.DP-4 | Event detection information is communicated | Event detection information is communicated. Ticketing logs comply with Vulnerability Management Plan Antivirus software on endpoints.  CISA Cyber Hygiene program. |  |
| DE.DP-5 | Detection processes are continuously improved | See all detection processes are reviewed and continuously approved Vulnerability Management Plan. Antivirus software on endpoints.  CISA Cyber Hygiene program. |  |
| **RESPOND (RS)** | **Analysis (RS.AN):** Analysis is conducted to ensure effective response and support recovery activities. | RS.AN-1 | Notifications from detection systems are investigated | Notifications from detection systems are investigated. Ticketing system contains the events. Vulnerability Management Plan. Antivirus software on endpoints.  CISA Cyber Hygiene program. |  |
| RS.AN-2 | The impact of the incident is understood | See the impact of the incident is understood by the organization. Vulnerability Management Plan. Antivirus software on endpoints.  CISA Cyber Hygiene program. |  |
| RS.AN-3 | Forensics are performed | Forensic specialist identified in the IR plan. |  |
| RS.AN-4 | Incidents are categorized consistent with response plans | See Incident categorization is achieved in the IR plan. See IR plan and Tabletop exercise. |  |
| RS.AN-5 | Processes are established to receive, analyze, and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g., internal testing, security bulletins, or security researchers) | Vulnerability Management Plan See security bulletins. |  |
| **Communications (RS.CO):** Response activities are coordinated with internal and external stakeholders (e.g., external support from law enforcement agencies). | RS.CO-1 | Personnel know their roles and order of operations when a response is needed | Personnel know their roles and order of operations when a response is needed as shown in the IR plan. |  |
| RS.CO-2 | Incidents are reported consistent with established criteria | See how incidents are reported, verified, and monitored consistent with established criteria as described in the IR plan. |  |
| RS.CO-3 | Information is shared consistent with response plans | See information sharing in the IR plan and Tabletop exercise. See IR plan report. |  |
| RS.CO-4 | Coordination with stakeholders occurs consistent with response plans | Implement an incident handling capability for incidents that is consistent with the incident response plan and includes preparation, training, execution, detection and analysis, containment, eradication, and recovery as shown in the IR plan. |  |
| RS.CO-5 | Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness | See information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness in the last exercise or event. |  |
| **Improvements (RS.MI):** Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities. | RS.IM-1 | Response plans incorporate lessons learned | See response plans incorporate lessons learned. |  |
| RS.IM-2 | Response strategies are updated | IR plan is updated yearly. |  |
| RS.MI-1 | Incidents are contained | Incidents containment is achieved as described in the IR plan. See IR plan and event tracking. |  |
| RS.MI-2 | Incidents are mitigated | See last IR exercise report that shows mitigation of the vulnerability and hardening. |  |
| RS.MI-3 | Newly identified vulnerabilities are mitigated or documented as accepted risks | See last IR exercise report that shows mitigation of the vulnerability and hardening. |  |
| **Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents. | RS.RP-1 | Response plan is executed during or after an incident | See last IR exercise report. |  |
| **RECOVER (RC)** | **Communications (RC.CO):** Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors). | RC.CO-1 | Public relations are managed | See IR public relations are plan. |  |
| RC.CO-2 | Reputation is repaired after an incident | See public relations repair plan. |  |
| RC.CO-3 | Recovery activities are communicated to internal and external stakeholders as well as executive and management teams | Recovery activities are communicated to internal and external stakeholders as well as executive and management teams. See written plan or report. |  |
| **Improvements (RC.IM):** Recovery planning and processes are improved by incorporating lessons learned into future activities. | RC.IM-1 | Recovery plans incorporate lessons learned | Recovery plans incorporate lessons learned. See written plan or report. |  |
| RC.IM-2 | Recovery strategies are updated | Recovery strategies are updated in the IR plan. See written plan or report. |  |
| RC.RP-1 | Recovery plan is executed during or after a cybersecurity incident | Recovery plan is executed during or after a cybersecurity incident. See written plan or report. |  |