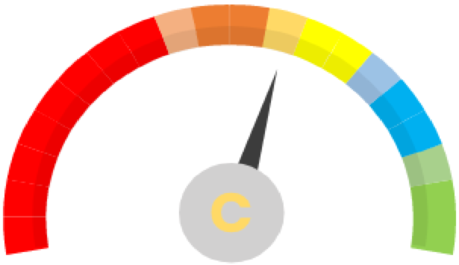
Company

Compliance Result

ACME BANK1

Report Generated: 15/08/2023



The results ranged between 55-61% of the assessment

Questionnaire - NIST CSF

User Email - bjgrosvenor72@hotmail.com

Audit Date - 15/08/2023

Tier -

Due Date - 15/08/2023

Compliance Control	Response	Compliance Reference
ID.AM-1	Mostly	ID.AM-1: Physical devices and systems within the domain's are inventoried Control Rationale: Asset inventory will help you identify the necessary steps and priorities on your estate from a cyber event.
ID.AM-2:	Partially	ID.AM-2: Software platforms and applications within the domain's are inventoried Control Rationale: Asset inventory will help you identify the necessary steps and priorities on your estate from a cyber event.
ID.AM-3:	Mostly	ID.AM-3: Domain communication and data flows are mapped Control Rationale: The transfer of data between systems can represent the transfer of security risk and therefore needs to be mapped and analysed for security weak points.
ID.AM-4:	Partially	ID.AM-4: External information systems are cataloged Control Rationale: External systems that are part of the domain solution, but are outside the control of the domain's direct supervision and authority, need to be security reviewed for any potential exposure.

ID.AM-5:	Partially	ID.AM-5: Resources (e.g., hardware, devices, data, time, and software) are prioritized based on their classification, criticality, and business value Control Rationale: To provide a centralized view of the domain's asset criticality, classification and associated protection requirements. This will also help prioritize respond and recover steps for the domain.
ID.AM-6:	Partially	ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established Control Rationale: A management framework with roles and responsibilities provides control of the implementation and operation of cybersecurity and the necessary checks and balances against policies and procedures
ID.BE-1:	Limited	ID.BE-1: The domain's role in the supply chain is identified and communicated Control Rationale: Supply chains can introduce particular risks to a domain and should be managed through partnership mgmt. and contracts
ID.BE-2:	Partially	ID.BE-2: The domain's place in critical services / infrastructure to its clients or sector is identified and communicated Control Rationale: Understand your domain's legal or regulatory obligations running any potential critical infrastructure. This may be targeted by bad actors as a potential weak point and therefore you may need to improve cyber defences.
ID.BE-3:	Partially	ID.BE-3: Priorities for domain's mission, objectives, and activities are established and communicated Control Rationale: The domain's mission, objectives, and activities provide a common understanding of the priorities for the domain's mission, objectives, and activities.
ID.BE-4:	Partially	ID.BE-4: Dependencies and critical functions for delivery of critical services are established Control Rationale: Interdependency of critical systems and degradation of services of one system might result in service disruption to another system.

ID.BE-5:	Partially	ID.BE-5: Resilience requirements to support delivery of domain services are established for all operating states (e.g. under duress/attack, during recovery, normal operations) Control Rationale: Resilience is sufficient to meet with the availability and recovery requirements for the domain's core business.
ID.GV-1:	Partially	ID.GV-1: Domain's Cybersecurity policy is established Control Rationale: Cybersecurity policies are the minimum security standards for any domain. It provides the management with direction and support for protecting systems and assets in accordance with the business needs and security requirements.
ID.GV-2:	Partially	ID.GV-2: Cybersecurity roles & responsibilities are coordinated and aligned with internal roles and external partners Control Rationale: Cybersecurity roles & responsibilities should be assigned and aligned with any existing roles so the accountability of the task is not lost.
ID.GV-3:	Partially	ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed Control Rationale: The domain fully understands its risk and exposure to legal, statutory and regulatory obligations.
ID.GV-4:	Partially	ID.GV-4: Risk management processes address cybersecurity risks Control Rationale: Risk management processes help the domain to identify, prioritise and address cybersecurity risks.
ID.RA-1:	Mostly	ID.RA-1: Asset vulnerabilities are identified and documented Control Rationale: Vulnerable assets should be identified and remediated in a timely manner to reduce the exposure of a potential cyber event
ID.RA-2:	Partially	ID.RA-2: Cyber threat intelligence is received from information sharing forums and sources Control Rationale: Cyber threat intelligence can help inform the domain about the common and severe external threats e.g. APT attacks and zero-day malware.

ID.RA-3:	Partially	ID.RA-3: Threats, both internal and external, are identified and documented Control Rationale: Threat identification is a part of the risk based approach which is used to identify, prioritise and address the security risks for the domain.
ID.RA-4:	Mostly	ID.RA-4: Potential business impacts and likelihoods are identified Control Rationale: Impact and likelihood identification is a part of the risk based approach which is used to identify, prioritise and address the security risks.
ID.RA-5:	Partially	ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk Control Rationale: Risk determination is a part of the risk based approach which is used to identify, prioritise and address the security risks.
ID.RA-6:	Partially	ID.RA-6: Risk responses are identified and prioritized Control Rationale: Prioritising the identified risks for treatment is a part of the risk based approach which is used to identify, prioritise and address the security risks.
ID.RM-1:	Limited	ID.RM-1: Risk management processes are established, managed, and agreed to by domain's stakeholders' Control Rationale: A documented risk management process can help the domain to identify, prioritise and address the security risks.
ID.RM-2:	Partially	ID.RM-2: domain risk tolerance is determined and clearly expressed Control Rationale: When risk levels exceed the domain's risk tolerance, it becomes more critical to take action. Based on the risk tolerance, the domain can determine their own risk treatment plan and give priority to risk mitigating actions.
ID.RM-3:	Partially	ID.RM-3: The domain's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis Control Rationale: The risk tolerance of the domain's should align with the requirements for the domain's role in critical services / infrastructure or its industry sector

ID.SC-1:	Partially	ID.SC-1: Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by domain's stakeholders Control Rationale: Supply chains can introduce particular risks to the domain's and should be incorporated into the risk management plans.
ID.SC-2:	Partially	ID.SC-2: Identify, prioritize and assess suppliers and partners of critical information systems, components and services using a cyber supply chain risk assessment process Control Rationale: In order to manage and minimise supply chain risks, critical suppliers must be identified and evaluated to identify the risks they pose to the domain's.
ID.SC-3:	Partially	ID.SC-3: Suppliers and partners are required by contract to implement appropriate measures designed to meet the objectives of the Information Security program or Cyber Supply Chain Risk Management Plan. Control Rationale: Suppliers must be required to acknowledge and accept their responsibility for the domain's cybersecurity requirements as a condition of doing business.
ID.SC-4:	Partially	ID.SC-4: Suppliers and partners are monitored to confirm that they have satisfied their obligations as required. Reviews of audits, summaries of test results, or other equivalent evaluations of suppliers/providers are conducted Control Rationale: Suppliers must be monitored to ensure they are fulfilling their contracted cybersecurity requirements and meeting any service level obligations.
ID.SC-5:	Partially	ID.SC-5: Response and recovery planning and testing are conducted with critical suppliers/providers Control Rationale: Incident response and recovery are critical functions that must be extended to cover suppliers/providers that support critical functions to ensure that planning and testing and incident response plans cover the entire scope of the domain's resilience plans.

DE.AE-1	Partially	DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed Control Rationale: If a baseline of normal activity is established and recorded it makes it possible to detect anomalous system events and network traffic that indicates an attack, compromise or unauthorised access.
DE.AE-2:	Partially	DE.AE-2: Detected events are analysed to understand attack targets and methods Control Rationale: Analysis of events can reveal actions taken by attackers, identify the extent of damage or data loss and the actions necessary to block, contain, remediate and eradicate an attack and prevent future incidents.
DE.AE-3:	Partially	DE.AE-3: Event data are collected and correlated from multiple sources and sensors Control Rationale: Deploying tools to manage correlation of suspicious events or events of interest across all system and network components will assist in identifying suspicious patterns in information flows throughout the domain's. The history of events is important in this analysis and should be accommodated in any archiving decisions.
DE.AE-4:	Partially	DE.AE-4: Impact of events is determined Control Rationale: An information security event is an event indicating a possible breach of information security or failure of controls. The estimated impact of the event can support decision making on the required actions (e.g. escalation process, trigger disaster recovery procedure, etc.) and the priorities.
DE.AE-5:	Partially	DE.AE-5: Incident alert thresholds are established Control Rationale: Pre-defined incident alert thresholds can be used to detect abnormal activities in a consistent manner. Automatic alerts can notify security team and system administrator upon detection of any events that could signify an attack on an information system.

DE.CM-1:	Partially	DE.CM-1: The network is monitored to detect potential cybersecurity events Control Rationale: Network protection can detect and prevent against attackers traversing a network
DE.CM-2:	Partially	DE.CM-2: The physical environment is monitored to detect potential cybersecurity events Control Rationale: As most of the critical IT equipment are normally housed in a data centre or computer room, adequate protection of the physical operating environment is necessary to prevent unauthorised physical access, damage, theft or compromise of assets, and interruption to the office premises and information systems.
DE.CM-3:	Partially	DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events Control Rationale: Users shall follow the IS policies and be accountable for all their activities. Monitoring and analysing user behaviour can detect unauthorised behaviour by malicious or careless insiders.
DE.CM-4:	Partially	DE.CM-4: Malicious code is detected Control Rationale: Advanced anti-malware solution should be considered, as traditional signature-based antivirus software can be defeated by malicious code (i.e. zero-day attack).
DE.CM-5:	Partially	DE.CM-5: Unauthorized mobile code is detected Control Rationale: Unauthorised software and mobile code may have vulnerabilities that significantly impacts on the security of system.
DE.CM-6:	Partially	DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events Control Rationale: External service provider staff may access / manage critical IT systems containing sensitive data, whether housed in on-premise systems or in systems hosted by the provider or in the cloud.

DE.CM-7:	Partially	DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed Control Rationale: Unauthorized personnel, connections, devices, and software may pose risks and indicate vulnerabilities that significantly impact on the security of the domain's. Their presence may signify an on-going security breach.
DE.CM-8:	Partially	DE.CM-8: Vulnerability scans are performed Control Rationale: For the sake of avoiding attacks through known issues or vulnerabilities, asset vulnerabilities should be identified in a timely manner. Continuous scanning will detect configuration errors immediately, allowing repair before attackers can exploit them.
DE.DP-1:	Partially	DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability Control Rationale: Define the roles and responsibilities to: 1. initiate and control the implementation of the required detection processes within the domain's. 2. ensure that necessary checks and balance are in place. 3. staff are trained to report suspicious behaviour.
DE.DP-2:	Partially	DE.DP-2: Detection activities comply with all applicable requirements Control Rationale: To cope with emerging trends in the threat environment, detection activities should be tested, implemented and regularly reviewed according to the business needs, data classification, risks of emerging threats and other legal / contractual requirements.
DE.DP-3:	Partially	DE.DP-3: Detection processes are tested Control Rationale: To cope with emerging trends in the threat environment, detection activities should be tested, implemented and regularly reviewed according to the business needs, data classification, risks of emerging threats and other legal requirements.
DE.DP-4:	Partially	DE.DP-4: Event detection information is communicated Control Rationale: Ineffective communication of security event detection information may hinder the process of identification, eradication and investigation of security incidents.

DE.DP-5:	Partially	DE.DP-5: Detection processes are continuously improved Control Rationale: To be responsive and adaptive to a changing environment and to new technology, a continual improvement process shall be implemented.
PR.AC-1:	Partially	PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes Control Rationale: Identification and authentication requirements are implemented in order to provide a secure means of access to information and systems.
PR.AC-2:	Limited	PR.AC-2: Physical access to assets is managed and protected Control Rationale: Physical access control can prevent unauthorised physical access, damage, theft or compromise of assets, and interruption to the office premises and information systems.
PR.AC-3:	Limited	PR.AC-3: Remote access is managed Control Rationale: Remote access can introduce the risks of working with mobile computing equipment in unprotected environments, or allowing attackers to gain unauthorised access to systems via network connections.
PR.AC-4:	Limited	PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties Control Rationale: Identification and authentication requirements are implemented in order to provide a secure means of access to information and systems.
PR.AC-5:	Limited	PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate Control Rationale: Network segmentation and segregation can mitigate network intrusion, propagation or lateral movement.

PR.AC-6:	Limited	PR.AC-6: Identities are proofed and bound to credentials, and asserted in interactions when appropriate Control Rationale: An identity proofing process collects and verifies information about a person for the purpose of opening an account or issuing credentials to that person. This prevents the creation and use of fraudulent accounts, especially on web sites used to transact with customers.
PR.AC-7:	Limited	PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction Control Rationale: Strong authentication measures are used to verify user or device credentials for privileged or high value or risky interactions between systems and users / customers.
PR.AT-1:	Limited	PR.AT-1: All users are informed and trained Control Rationale: Awareness and knowledge degrades over time without ongoing refresher training and updates. Providing ongoing information security awareness and training will assist in keeping personnel aware of emerging security risks, incidents and their responsibilities.
PR.AT-2:	Limited	PR.AT-2: Privileged users understand roles & responsibilities Control Rationale: Privileged users need to have adequate awareness and knowledge to carry out their operational tasks and roles and responsibilities.
PR.AT-3:	Limited	PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities Control Rationale: Roles and responsibilities should be defined and third-party stakeholders need to have adequate awareness and knowledge, such that they can carry out their operational tasks and roles and responsibilities in accordance with the domain's requirement.
PR.AT-4:	Limited	PR.AT-4: Senior executives understand their roles & responsibilities Control Rationale: Roles and responsibilities should be defined and adequate awareness and knowledge, such that they can carry out their operational tasks.

PR.AT-5:	Limited	PR.AT-5: Physical and cybersecurity personnel understand roles & responsibilities Control Rationale: Lacking a clear definition and understanding of roles and responsibilities there could be inconsistent interaction with the security group, leading to unsecured implementation of security tools and practices.
PR.DS-1:	Limited	PR.DS-1: Data-at-rest is protected Control Rationale: Business data should have proper protection to prevent unauthorised access. Hard drives and removable media should be encrypted to ensure that data cannot be compromised if the media is lost or stolen.
PR.DS-2:	Limited	PR.DS-2: Data-in-transit is protected Control Rationale: Data communication paths outside the physical protection of a controlled boundary are exposed to the possibility of interception and modification. Communication over public networks should be encrypted to protect against leakage during transmission.
PR.DS-3:	Limited	PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition Control Rationale: Inventory of assets helps ensure that effective protection takes place and to identify lost assets.
PR.DS-4:	Limited	PR.DS-4: Adequate capacity to ensure availability is maintained Control Rationale: Critical systems / services should be implemented with resilience sufficient to meet the availability requirements such that the domain's core business requirements can be met.
PR.DS-5:	Limited	PR.DS-5: Protections against data leaks are implemented Control Rationale: Business data should have proper protection to prevent unauthorised access.

PR.DS-6:	Limited	PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity Control Rationale: Ensuring the authenticity and integrity of content reaching a security domain is a key component in ensuring its trustworthiness. Attackers frequently try to replace software with modified versions to capture data, disrupt system operations or provide unauthorised access mechanisms.
PR.DS-7:	Limited	PR.DS-7: The development and testing environment(s) are separate from the production environment Control Rationale: Development and testing environments, which are often subject to additional security risks, may be a back door to the production environment.
PR.DS-8:	Limited	PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity Control Rationale: Ensuring the integrity of hardware is not tampered with allows confidence data is better protected and prevents the injection of hardware designed to capture / steal information or allow backdoors
PR.IP-1:	Limited	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) Control Rationale: Baseline configuration standards allow the domain's to monitor and control the installation of systems to ensure security controls are correctly implemented.
PR.IP-2:	Fully	PR.IP-2: A System Development Life Cycle to manage systems is implemented Control Rationale: If security requirements are defined properly and identified risks are addressed in the early stage, future rework effort is expected to be immensely reduced and vulnerabilities will be minimised.
PR.IP-3:	Fully	PR.IP-3: Configuration change control processes are in place Control Rationale: A configuration change may impact the overall security risk for the system.

PR.IP-4:	Fully	PR.IP-4: Backups of information are conducted, maintained, and tested periodically Control Rationale: Having a backup strategy in place is a fundamental part of business continuity planning. The backup strategy ensures that critical business information is recoverable if lost.
PR.IP-5:	Fully	PR.IP-5: Policy and regulations regarding the physical operating environment for domain's assets are met Control Rationale: As most of the critical IT equipment are normally housed in a data centre or computer room, adequate protection to physical operating environment is necessary to prevent unauthorised physical access, damage, theft or compromise of assets.
PR.IP-6:	Fully	PR.IP-6: Data is destroyed according to policy Control Rationale: Without proper sanitisation or physical destruction, original data may be recovered and retrieved from the re-used or disposed IT equipment / storage media leading to data leakage.
PR.IP-7:	Fully	PR.IP-7: Protection processes are continuously improved Control Rationale: Continual reviewing and improving the effectiveness and efficiency of protection processes is necessary for ensuring that security protection is responsive and adaptive to changing environments.
PR.IP-8:	Fully	PR.IP-8: Effectiveness of protection technologies is shared with appropriate parties Control Rationale: Sharing incident information and threat intelligence, and exchanging best practices are encouraged with a view to strengthening awareness and information / cyber security capabilities.
PR.IP-9:	Fully	PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans are in place and managed Control Rationale: Business continuity, IR and DR plans can assist in ensuring that critical systems and business functions can be maintained when the system is operating under constraint.

PR.IP-10:	Fully	PR.IP-10: Response and recovery plans are tested Control Rationale: Regular testing is essential for ensuring plans are up-to-date, complete and accurate.
PR.IP-11:	Fully	PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening) Control Rationale: Personnel security can mitigate the risk of insider threats and resource misuse within the domain's.
PR.IP-12:	Fully	PR.IP-12: A vulnerability management plan is developed and implemented Control Rationale: For the sake of avoiding attacks through known issues or vulnerabilities, asset vulnerabilities should be identified and fixed in a timely manner.
PR.MA-1:	Fully	PR.MA-1: Maintenance and repair of domain's assets are performed and logged, with approved and controlled tools Control Rationale: Unauthorised or unmanaged maintenance, repairs or disposal processes may lead to disclosure of sensitive data and impact the integrity of the product or equipment.
PR.MA-2:	Mostly	PR.MA-2: Remote maintenance of domain's assets is approved, logged, and performed in a manner that prevents unauthorized access Control Rationale: Unauthorised or unmanaged maintenance, repairs or disposal processes may lead to disclosure of sensitive data and impact the integrity of the product or equipment
PR.PT-1:	Mostly	PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy Control Rationale: Event logging can (1) help raise the security posture of a system by increasing the accountability for all system user actions (2) increase the chances that malicious behaviour will be detected by logging the actions of a malicious party
PR.PT-2:	Mostly	PR.PT-2: Removable media is protected and its use restricted according to policy Control Rationale: Protection of removable media will reduce the risk of data loss associated with a lost or stolen device.

PR.PT-3:	Mostly	PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities Control Rationale: The principle of least functionality can prevent unauthorised activities such as unauthorised connection of devices (e.g. ssh) and unauthorised transfer of information (e.g. FTP, USB port).
PR.PT-4:	Mostly	PR.PT-4: Communications and control networks are protected Control Rationale: Network protection can (1) prevent unauthorised access to internal network by plugging into a network port (2) prevent against attackers traversing a network and
PR.PT-5:	Mostly	PR.PT-5: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations Control Rationale: Critical business operations dependent on systems require reliable systems, applications and communications that allow uninterrupted operations despite component or facility failures.
RS.RP-1:	Mostly	RS.RP-1: Response plan is executed during or after an event Control Rationale: Response plans covering attack scenarios can shorten the response time and ensure a consistent outcome to mitigate the impact of an incident. Good incident management skills require regular practice.
RS.CO-1:	Mostly	RS.CO-1: Personnel know their roles and order of operations when a response is needed Control Rationale: Incident response team members including external third parties should know their roles and are well-trained for the order of operations to shorten the response time. Automation should be used where possible to ensure all required operations are executed.
RS.CO-2:	Mostly	RS.CO-2: Incidents are reported consistent with established criteria Control Rationale: Reporting channels (e.g. helpdesk, system, firewall, IDS, MSSP) and criteria (e.g. defined type of incident, impact analysis, thresholds as abnormal events) should be established in order to investigate the cyber incident effectively.

RS.CO-3:	Mostly	RS.CO-3: Information is shared consistent with response plans Control Rationale: Security event information should be shared with stakeholders and management in order to detect and respond to security incidents effectively. The information to be shared with each stakeholder should be documented in plans to ensure information is only communicated as and when required and to avoid mistakes.
RS.CO-4:	Mostly	RS.CO-4: Coordination with stakeholders occurs consistent with response plans Control Rationale: Cyber drill test, or incident report should demonstrate the coordination with stakeholders according to the defined response plan (e.g. escalation procedure) to ensure the response to incident is effective.
RS.CO-5:	Mostly	RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness Control Rationale: The domain's can share the security-related information including threats, vulnerabilities and incident with external stakeholders.
RS.AN-1:	Mostly	RS.AN-1: Notifications from detection systems are investigated Control Rationale: Potential security events are triggered from detection systems or reported by staff and the response team must investigate the events in timely manner.
RS.AN-2:	Mostly	RS.AN-2: The impact of the incident is understood Control Rationale: Response team should understand the impact of each incident according to the attack nature and affected systems. Impact Analysis Matrix and Incident Reporting Template can facilitate the impact analysis.
RS.AN-3:	Mostly	RS.AN-3: Forensics are performed Control Rationale: Forensic investigation should be performed in particular for cyber crimes or targeted attacks. It can confirm the root cause and impact to the domain's systems.

RS.AN-4:	Mostly	RS.AN-4: Incidents are categorized consistent with response plans Control Rationale: The defined type of incident will trigger the specified responsible team and third parties for incident response. Defined prioritisation will enable a rapid response for significant cybersecurity incidents or vulnerabilities.
RS.AN-5:	Mostly	RS.AN-5: Processes are established to receive, analyse and respond to vulnerabilities disclosed to the domain's from internal and external sources (e.g. internal testing, security bulletins, or security researchers) Control Rationale: domain's should establish procedures and responsibilities to ensure timely and appropriate follow-up when vulnerabilities are disclosed to them.
RS.MI-1:	Mostly	RS.MI-1: Incidents are contained Control Rationale: Appropriate steps must be taken to contain and control an incident to prevent further unauthorized access or keep the incident from escalating. Incident response plans must be developed to guide IR teams and ensure they are well trained.
RS.MI-2:	Mostly	RS.MI-2: Incidents are mitigated Control Rationale: Appropriate steps must be taken to mitigate the impact from a security incident and return to normal operations.
RS.MI-3:	Mostly	RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks Control Rationale: The domain's should develop process to review newly identified vulnerabilities, assessing their impact and the risks if not immediately remediated.
RS.IM-1:	Mostly	RS.IM-1: Response plans incorporate lessons learned Control Rationale: Learning from security incidents and updating controls and plans not only reduces the likelihood or impact of future incidents, but also provides input to update the risk management strategy in order to reduce the domain's-wide level of risk.

RS.IM-2:	Mostly	RS.IM-2: Response strategies are updated Control Rationale: Response strategies should be regularly reviewed and updated according to the capabilities and detection system changes for incident response.
RC.RP-1:	Mostly	RC.RP-1: Recovery plan is executed during or after a cybersecurity incident Control Rationale: Following well-planned and documented recovery processes and procedures minimises impact and ensures timely restoration of systems or assets and operations affected by cybersecurity events.
RC.IM-1:	Limited	RC.IM-1: Recovery plans incorporate lessons learned Control Rationale: Learning from security incidents and updating controls and plans enables faster recovery and reduced impact of future incidents.
RC.IM-2:	Limited	RC.IM-2: Recovery strategies are updated Control Rationale: Recovery strategies should be regularly reviewed and updated based on lessons learned and development of new recovery and mitigation tools & technologies.
RC.CO-1:	Limited	RC.CO-1: Public relations are managed Control Rationale: Plans for public relations activities in the event of various cyber incidents should be well prepared and address legal, regulatory and reputational protection.
RC.CO-2:	Limited	RC.CO-2: Reputation is repaired after an event Control Rationale: The trust of customers, suppliers, shareholders, regulators and other stakeholders must be preserved or won back during / after a security incident.
RC.CO-3:	Limited	RC.CO-3: Recovery activities are communicated to internal and external stakeholders as well as executive and management teams Control Rationale: Business operations must continue during and after an event while efforts are underway to restore full operations and recover from damage. Regular communication through all stages of an incident ensures internal parties and all stakeholders are informed of progress and conduct continuity and recovery operations accordingly.