Information Technology Strategy and Policy Overview

PYZ Technology

Adam Nutt

CIS519

Danny Underwood

**Executive Summary**

As PYZ Technology begins its next steps into maturity as a company, partnering with various levels of government and eyes on reaching the open market, there are critical steps that the company must take to safeguard intellectual property as well as other data and assets.

These measure will consistent of newly developed policies with the goals of protecting the company from outside threats such as hackers, data breaches, legal challenges and other events that could result in the stoppage of critical business activities while also working to keep PYZ Technology compliant with federal regulations in order to maintain federal contracts.

The need for new and expanded policies serves in the best interest of PYZ Technology, its staff, third party vendors and government clients. Policies will establish appropriate guidelines for handling and storing data, device and application usages, setting up passwords. These policies shall be reviewed and adapted as determined by the Information Security Team on a two year basis, or as needed to address vulnerabilities, changing compliance regulations, technological advances or in response to events causing stoppage of critical business.

**The Need for a Strategic Plan**

A strategic plan is a vital tool for any business or company to establish a path forward to grow the company while setting key goals and objectives to track progress and set a direction for the business. A strategic plan will not only lay out long-term and intermediate goals, but can be used to shape day-to-day and weekly agenda items contributing to achieving set goals and meeting key deadlines.

**Method/Model Recommended**

I would recommend using a hybrid model that will address current needs and further the company's ability to grow. The models recommended would be the goal model, alignment model and the CMMI model. These models used in relation to one another will connect the different segments of the business to ensure they are working together in driving the business forward, setting attainable goals for sustainable growth and meeting requirements established by the federal government for companies executing government contracts.

**Why This Method/Model**

The CMMI is the Capability Maturity Model Integration which helps organizations streamline process improvement and encourage productive, efficient behaviors that decrease risks in software, product and service development (White, 2021). It is a common requirement for Department of Defense and other government contracts for software development. It works to not only improve the process side of the business, but also performance by establishing goals and a framework that promotes efficiency and productivity, partnering effectively with the goals model. The alignment model will help to weave together individual segment goals and tasks with other departments to ensure that they not only meet their objectives, but collectively contribute to the overall goals of PYZ Tech.

**Link to Organizational Strategy**

The organizational strategy will build out the framework for these strategies that will ultimately support the overall strategies. As these strategies work to identify weakness and areas of improvement, there will be a constant flow of updates to the strategies to ensure that they are as effective as possible and that the appropriate measures are being taken. Further, it will ensure that PYZ Tech and its CMMI model, as well as business actions, are within the necessary compliance for the contract, receiving FDA approval and protecting sensitive data from leaks, theft and bad actors.

**Governance Framework**

The information governance for PYZ Technology is an important framework to establish in order to protect the company from cyber incidents, preserve intellectual and financial property and other key information and data. While all components are vital and can even build off of each other, a few stood out most in establishing this framework for the plan ahead.

**Security**

The security of the company from cyber attacks, loss of information and other assets is critical to success, especially early into the life of the company. According to the U.S. Congressional Small Business Committee, 71% of cyber attacks occurred at businesses with fewer than 100 employees (Segal, 2016). While there are a number of measures that can be implemented by the team, it will be equally important that all staff is in steps with these measures such as reporting phishing attempts, creating safe and strong passwords and practicing appropriate behavior when using company technology or when used on mobile devices. We will be able to utilize other tools to protect the company such as firewalls, antivirus and anti-malware software, two-factor authentication as well as regularly backing up company data.

**Records and Information Management**

The management of records and information will at times fall onto staff as well so we must ensure that appropriate guidelines are not only established, but practiced by all. Developing an effective management system will add in protecting the company as well as minimize risk, execute processes more efficiently and quickly. The data administrator will play a key role in developing the plan necessary to help us remain in compliance and protect the company and its data.

**Data Classification Taxonomy**

A robust Records & Information Management (RIM) strategy depends on a clear Data Classification Taxonomy, which dictates how each data asset is labeled, stored, accessed, and ultimately disposed of. In this framework, four distinct classification levels—Public, Internal-Use Only, Confidential, and Highly Confidential/Restricted—are defined based on the sensitivity, regulatory implications, and potential impact of unauthorized disclosure.

Public data consists of information that is intended for broad consumption or is legally required to be made public. Examples include corporate marketing materials, published annual reports, and press releases. Public data may be freely shared externally without approval, and it is retained according to a minimal archival schedule (for instance, retained for three years before disposal), since its unauthorized disclosure poses little to no risk.

Internal-Use Only data encompasses operational information that is not intended for public release and carries minimal risk if exposed. Typical examples include internal process documentation, meeting minutes, and a non-sensitive employee directory. Access to Internal-Use data is restricted to authenticated employees, and external sharing is prohibited unless explicitly approved. Such data is retained until it is superseded, generally for up to five years, before being archived following standard retention guidelines.

Confidential data represents sensitive business information whose unauthorized disclosure could cause measurable harm, financial, reputational, or operational, to the organization. Examples include sales forecasts, vendor contracts, employee personally identifiable information (PII), and internal budgets. Confidential data must be stored in encrypted repositories, protected by two-factor authentication, and accessed strictly on a need-to-know basis. Any external sharing of Confidential data requires manager approval and is subject to encryption in transit. Retention schedules for Confidential data are defined by business-unit and regulatory requirements, and periodic reviews (at least annually) confirm that only necessary information is held.

Highly Confidential/Restricted data is defined as information that, if compromised, could cause severe legal, financial, or reputational damage to the organization. This category includes trade secrets, proprietary algorithms, nonpublic strategic plans (such as M&A discussions), and protected health information (PHI) covered by HIPAA. Access to Highly Confidential data is granted only through a formal approval workflow and stored in secure, zero-trust environments with multi-party encryption keys. Retention is limited to the duration of the business need, with immediate, secure destruction required once the data is retired. Any exception to these rules, such as temporary external collaboration, demands a documented approval from the Data Governance Lead and a signed non-disclosure agreement.

To operationalize this taxonomy, the Data Governance Committee oversees a formal classification process. First, a comprehensive data discovery exercise identifies new or unclassified data stores across file shares, databases, and BI dashboards. Data Stewards then assign an initial classification based on content and context. Classification labels such as “CLASSIFICATION: Confidential” are embedded as metadata tags within document properties, database fields, and analytics outputs. The Data Custodians in IT enforce controls (for example, encryption, network access restrictions, or Data Loss Prevention policies) based on the assigned classification level.

A quarterly review cycle ensures that no data remains misclassified: Data Stewards reconvene to re-evaluate any asset whose status may have changed, for instance, a Confidential project that has since been publicly released. If reclassification is required, automated workflows adjust encryption, access controls, and retention schedules accordingly. Finally, automated enforcement through DLP rules at both network and endpoint layers prevents unauthorized exfiltration of Confidential or Highly Confidential data; any necessary exceptions are documented, approved by the Data Governance Lead, and tracked through an exception log.

**Litigation Readiness**

With our technology and its purposes being controversial, we will need proper litigation readiness in the event of any legal disputes, challenges or changes to laws. Activist groups and legislators around the country could take serious issue with Y2X. As Thurman Legal notes, “litigation readiness is a detailed and structured ‘how-to' process for ensuring the proper creation, organization, preservation, analysis and immediate access to critical information and evidence necessary to respond to litigation or regulatory investigations”. This plan should consist of components that answer these five questions:

1. What laws apply to PYZ Tech?

2. What policies and procedures should be implemented to ensure compliance with these laws?

3. What documentation should be maintained to prove compliance?

4. How does PYZ Tech train and track all employees in regards to compliance?

5. How are we monitoring outside sources regarding our compliance?

**Regulatory Compliance**

While working under government contracts, ensuring we are within compliance is vital to retaining the contract. Under the Department of Defense’s Cybersecurity Maturity Model Certification and President Biden's Executive Order to improve the nation's cybersecurity new, more strict guidelines are in place that we must make sure we are meeting or face serious risk from outside sources as well as to the contract itself. New regulations relating to collecting and preserving data as well as reporting and sharing data related to cyber attacks and incidents are a new standard as well as ensuring our vendors have appropriate certification as well. This is also a changing area that will take effort to monitor going forward. The legal team as well as the network manager will need to work to ensure compliance.

**Strategy plan**

**Strategy Vision**

When developing a strategic vision, PYZ must take stock of their current situation in terms of staffing, technology, as well as a clear, honest approach to view the future and where the company should be heading towards. As the vision is established, it is important to keep the main drivers of security, record and information management and regulatory compliance top of mind. Developing an appropriate vision, it is important to establish realistic and tangible goals while being honest with the landscape of the industry, the company and the current contracts. While the goals should remain top of mind, it is equally important to adapt as needed. Because of the nature of the technology PYZ produces, there may be challenges in the courts, through legislation or public perception that can negatively impact the ability to grow and this must be of concern by all decision makers with readiness plans to respond to any changes.

**Roles and Responsibilities**

In the planning process, it would be advantageous to expand the decision making beyond the traditional leadership team. CIO, CEO and CFO are key figures as well as including the IT leadership team of the data administrator, systems manager and database manager, but to follow Harvard University's lead, other key figures from different departments should be included to help draft and ultimately assist in implementing key points from the plan as well as communication to employees and ensuring the necessary tracking and compliance are in order. Others to include at certain phases of development would be the head of HR, the marketing manager and product development manager.

**Data Governance Committee Structure**

To ensure consistent decision-making and clear accountability for data policies across the organization, a formal Data Governance Committee (or Council) must be established. This Council is chaired by the Data Governance Lead, who serves as the day-to-day steward of governance activities, and is sponsored at the executive level by either the Chief Data Officer or the Chief Information Security Officer (CISO), depending on organizational structure. The Executive Sponsor’s role is to provide strategic direction, secure budgetary resources, and champion data governance at the highest levels of leadership. Biweekly or monthly, the Data Governance Lead convenes the Committee to review policy updates, address emerging data risks, and monitor key performance indicators (KPIs) tied to data quality, compliance, and stewardship.

Supporting these two roles are Data Stewards, each assigned to a business domain such as Finance, Human Resources, or Sales, who bear responsibility for day-to-day data quality, metadata management, and ensuring that domain-specific policies are followed. These Stewards meet regularly (for example, in biweekly domain review sessions) to coordinate with Data Custodians in IT/Security, who are charged with implementing technical controls like access provisioning, encryption, and backups. In parallel, a Legal/Compliance Representative must sit on the Committee to validate that each policy aligns with applicable regulations (for example, CMMC, HIPAA, or GDPR) and to oversee any litigation-readiness activities that arise. The Records & Information Manager oversees retention schedules, classification workflows, and archival or destruction activities. Finally, Business Unit Liaisons, selected “power users” from key departments, participate to provide frontline feedback on data usability and to pilot new processes before organization-wide rollout. In larger organizations, a dedicated Project Manager may be appointed to coordinate deliverables, track timelines, and ensure all action items from Committee meetings are completed.

Below is a high-level RACI matrix that summarizes responsibilities for core governance activities. This table can be used as a reference when assigning accountability and clarifying who should be consulted or informed during each phase of policy development, enforcement, or compliance review.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| | **Activity** | **Exec Sponsor** | **Data Gov Lead** | **Data Steward** | **Data Custodian** | **Legal/Compliance** | **RIM Manager** | **Business Liaison** | **Project Mgmt** | | --- | --- | --- | --- | --- | --- | --- | --- | --- | | Policy Development & Approval | A | R | C | C | C | C | I | R | | Data Quality KPI Definition | I | R | A | C | I | I | I | C | | Data Classification Schema Creation | I | R | A | C | C | C | I | C | | Incident Response Plan Review & Signoff | A | R | I | A | C | I | I | C | | Regulatory Compliance Audit Preparation | I | R | C | C | A | C | I | I | | Retention Schedule Publication & Enforcement | I | R | I | C | C | A | I | I | | Ongoing Training & Communication Rollout | I | R | C | C | I | I | A | C | |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |

**Process and Procedures**

Another area where an expanded team will be useful is through process and procedures. This will enable department leadership to implement the appropriate measures that will contribute to the security of the company and its assets as well as providing employees with a clear direction and understanding of what the company goals are and how they and their roles factor into those goals. Following the necessary procedures not only contributes to the company's security and performance, it will also ensure we remain within the regulatory compliance framework for the government contracts and can be a way to build trust with employees as well as potential customers for the Y2i product.

**Strategic Plan**

The strategic plan will be one of the most vital tools for the company as we navigate through this new sector. Initially we will need to identify security groups, how they function in the organization, evaluating resources and how they are currently being allocated and how they may need to be scaled up, down or reallocated. All factors and decisions must drive us toward each milestone and contribute to the broader company goals.

**Strategy Formation**

In this phase, we will work to establish goals and metrics for the departments and the company overall. This phase will rely on the other departments in helping to shape specific goals that contribute to the company goals and set forth the expectations for the departments and staff. The goals will be firm, but remain flexible to change as needed. This is where we can factor in concerns and bottlenecks that could cause issues down the line such as procurement of materials and supply chain constraints. Given these concerns, it would be to our benefit to have certain measures in place to help adapt to these hurdles if and when they come such as having backup plans for approved and certified vendors.

**Security Convergence Plan**

Having a detailed security convergence plan will work to protect the company, records and information as well as employees. This will serve to protect the physical nature of the business for events such as severe weather, fire and other events. This will include necessary alarms, key-accessed entry to the building and security staff. The IT team will serve as a form of security for our data, records and other sensitive and staff will play a role in complying with the guidelines set forth by IT. These work to mitigate and reduce risk while ensuring compliance and contributing to the broader goals.

**Change Management**

In change management, it will be necessary to evaluate the need for change and develop appropriate strategic goals and performance indicators before preparing the company for the change. Having the appropriate management of departments sit in on these as stakeholders is valuable to the success of implementation of change. With the potential for litigation and legislative changes, we must be ready and willing to change in a manner that retains our staff, allows us to drive as close to initial goals as possible or develop new goals out of this new compliance.

**Implementation**

This will require buy-in from staff in order to be successful. Including the necessary stakeholders early on in the drafting stages should contribute to this, but it is not something we can simply rest on. It will take company-wide partnership to integrate the plans as designed and we must effectively plan for any headaches and set backs as adjustments are made whether it's as individuals or from technological adjustments.

**Scorecard**

Having a well-designed scorecard will work to align strategic goals with the overall vision in measurable outputs across the organization. Communication will be key from department management so staff are informed with how their performance is meeting the expectations needed for department and company success and compliance.

**Feedbacks, Tracking and Control**

Monthly and quarterly tracking will work to ensure compliance as well as track how we are reaching or falling short of our initiatives. It would be to the benefit of all involved for either weekly or monthly 1-on-1 meetings between department managers and staff to assess performance and develop or adapt goals around changes and address and needs or concerns, whether it be from the staff or from upper management down. Middle management will play crucial role in implementing as well as progressing through the strategic plan we will set forth.

**Policy Lifecycle**

**Policy Created**

As policy is developed, it is important to have consideration for specific guidelines as well as agents of changes such as regulatory requirements, legal and legislative challenges and technological advances. Considering the industry as well as the potential controversy around PYZ Tech products, developing effect policy must also remain flexible to change. Policy should be reflective of the company’s goals and serves to drive towards those goals through each phase of the lifecycle, as well as addressing any company needs or weaknesses.

**Published and Communicated**

As policy guidelines become finalized, the distribution and implementation of these standards is a crucial phase. Communication must be clear for all staff with the appropriate measures given to leadership to assist in the implementation. They will need to educate staff on the standards and procedures while enlisting buy-in from them in order to effectively implement them. As staff work, they may develop their own process within their role and become accustom to how they complete tasks. This process will need to firmly establish these procedures so that any aspects of a n employee's work process remains within the guidelines as well as regulatory compliance.

**Periodic Review**

As these policies are implemented, a consistent monitoring of compliance as well as effective and efficiency. Review cycles should be on a monthly basis so we are able to accurately make adjustments as necessary. Having quarterly and annual reviews will be of importance with monthly reviews providing insight into trends, allow us to spot any errors, actions of non-compliance and draw awareness to areas of concern or weakness.

**Revised/Retired**

Given the industry and the products, change is inevitable. Coupled with advances in technology, information security and threats, certain policies may either become out of date, no longer applicable, or become less effective. Through review, we can highlight what changes may need to be made in order to remain in compliance with regulations, shape our work to abide by legislative changes, and address threats and opportunities. This could lead to revising the policy to better address the issue, resulting in returning to the published/communicated phase, or may even need to be replaced by new policy, restarting the cycle on this specific policy.

**Policy Framework**

**Identify**

In this stage of the framework, team members must be able to effectively identify goals for the company, guidelines, regulatory requirements and risk assessment. To develop effective policy, it must drive towards company goals, ensure compliance as well as protect company assets.

**Protect**

For specific policy, access may be limited to the appropriate parties with an overarching function of preserving the security of data and assets. We must ensure that it has been communicated as well as providing applicable trainings are provided whether its for rolling out new policy or providing review to maintain employee participation in procedures.

**Detect**

Through continuous monitoring, we will be able to spot trends, identify areas of weakness or inappropriate or risky activities. Whether internal or external, any activity that compromises PYZ Technology can be identified and addressed as the situation calls for.

**Respond**

Having a plan ready to combat nefarious or suspicious activity serves to protect PYZ Tech and mitigate any risk to data assets and other documents and property. It will be crucial to acquire accurate details on the action inflicted in order to evaluate the failures of the procedures in place and how we can work to improve upon them going forward. There may also be the need to respond to changes towards the products may it be certain aspects of it or the product overall.

**Recover**

Having proper backup for data and information serves to better protect the company alleviate recovery. It is not only appropriate, but essential to provide necessary information to staff as we know it and develop a proper response to keep staff alert and implement any changes to help further protect the company. Relating to legal challenges, a recovery plan would be dependent on court rulings or the passage of new laws. To have an effective plan available, during these events leadership must be crafting adjustments or new plans centered around potential outcomes and how they may impact certain goals.

**IT Guidelines and Policies**

**Acceptable Use**

Please read and follow the following Acceptable Use Policy.

Violations may result in termination of access, disciplinary review, termination of employment and possible legal action.

* Keep your computer up to date . Ensure all updates have been completed.
* Report all suspicious emails. Do not click on any suspicious links or emails from unknown sources.
* Refrain from utilizing unapproved websites.
* Do not allow any non-PYZ Technology employee to access your devices.
* Never share login information or passwords

**Access Control**

Specific access will be provided to employees based on business requirements, job function, responsibilities, or need-to-know. All additions, changes, and deletions to individual system access must be approved by the appropriate supervisor and technical staff. Account creation, deletion, and modification as well as access to protected data and network resources is completed by the Server Management team.

**Mobile Device Usage**

This policy defines standards, procedures, and restrictions for any and all end users with legitimate business uses connecting mobile devices to PYZ Technology ’s corporate network, digital resources, and data. The mobile device policy applies, but is not limited to, all devices and accompanying media that fit the following classifications:

* Smartphones
* Laptop, desktop and notebook computers
* Tablets
* Any other mobile device capable of storing corporate data and connecting to a network

The policy applies to any company-provided mobile device that is used to access corporate resources. No personal devices are permitted to be used.

The primary goal of this policy is to protect the integrity of the confidential client and business data that resides within PYZ Technology’s technology infrastructure, including internal and external cloud services. This policy intends to prevent this data from being deliberately or inadvertently stored insecurely on a mobile device or carried over an insecure network where it could potentially be accessed by unauthorized resources.

A breach of this type may result in loss of information, damage to critical applications, loss of revenue, damage the company’s public image, breach our data privacy requirements, and violate data privacy laws. Therefore, all employees, contractors, or personnel using a mobile device connected to PYZ Technology’s corporate network, and/or capable of backing up, storing, or otherwise accessing corporate data of any type, must adhere to company-defined processes and policies in doing so.

Failure to comply can result in termination of employment or contract and potential legal action.

**Change Management & Incident Response**

Change Management seeks to minimize the risk associated with changes pertaining to the addition, modification or removal of anything that could have an effect on company IT services.

Changes are to come through the IT department and can be requested through appropriate channels.  The change should not be completed until reviewed and approved with documentation identifying the scope of the change, areas affected, back-out process, testing completed, communication plan and planned date of deployment.  This to be done at a level to ensure the scope as described can be accomplished and to provide assurance that the change will have the desired result and not compromise the security of PYZ Technology’s systems.

The purpose of this policy is to:

* Ensure security of company data and assets
* Reduce the impact of changes on other tasks/projects
* Promote communication and collaboration regarding change items
* Minimize the likelihood of outages
* Maintain compliance to applicable regulations

**Remote Access**

All users and administrators accessing High Security Systems must abide by the following rules:

* No modems or wireless access points are allowed on unapproved remote access technology.
* All remote access must be authenticated and encrypted through the PYZ Technology’s VPN.
* All remote access will be accomplished through the use of two factor authentication; a username and password or PIN combination, and a second method not based on user credentials, such as a certificate or token through approved vendor.
* Any machine used for remote access must have antivirus software installed and running.
* Access will be disconnected automatically after 24 hours. The employee must reestablish access again through the PYZ Technology VPN.

**Email/Communication**

* Any and all use of email must be compliant with PYZ Technology’s policies on ethical conduct and security of business data.
* All use of email must be in line with proper business practices and relevant to job duties.
* PYZ Technology email addresses or systems shall not be used for creating, distributing or accessing any offensive or illegal material, including but not limited to material with offensive comments about gender, race, age, sexual orientation or religious beliefs.
* Any offensive material received in email must be reported to the IT Department and Human Resources without undue delay.
* Usage of company-owned email addresses and systems for personal or any non-company use is prohibited.
* PYZ Technology may monitor and record any and all email messages received or sent by email addresses or systems owned or operated by PYZ Technology.
* PYZ Technology does not necessarily monitor all email activity, but retains the right to do so.

**Data Management**

PYZ Technology will develop and manage data and information for the purposes of research and development of new products and services analysis and to assist in decision making. Data and other intellectual property are assets of PYZ Technology. Employees are to handle data and information appropriately and securely with guidance of the provided policies and procedures.

All staff must access and use data assets in a manner to protect the company, it’s assets and themselves.

Staff are expected to:

* Comply with all regulations and requirements established by the company, law or contractual agreement.
* Data must be used for intended purposes only by those with approved access.
* Data is to be collected, stored and disposed of by approved means to avoid risk of exposure or loss of assets

**Documentation**

Policies and procedures are to be documented and accessible through the company intranet for employee access. New and revised policies and procedures will be communicated to the appropriate parties and updated on the company intranet accordingly. Any and all outdated policies or procedures will be removed and communicated to the appropriate parties within a reasonable time frame. These policies and procedures will then be archived accordingly.

**Incident Response Procedures**

Effective incident response is critical to preserving data integrity, maintaining stakeholder trust, and ensuring timely remediation when a security event occurs. The organization’s Incident Response (IR) process is divided into six distinct phases—Preparation, Identification & Detection, Containment, Eradication, Recovery, and Lessons Learned—each with clearly defined tasks, roles, and timelines.

Preparation requires that an IR team be constituted with defined roles and responsibilities, and that contact lists and escalation matrices be maintained and reviewed at least quarterly. This team conducts semi-annual tabletop exercises to simulate common scenarios, such as malware outbreaks or unauthorized data access, and confirms that logging, monitoring, and alerting systems (for example, a Security Information and Event Management platform) feed into a centralized dashboard accessible by the Forensics Lead.

During Identification & Detection, automated alerts (for instance, unusual login patterns or spikes in data exfiltration) are triaged by the Forensics Lead within 15 minutes of generation. At that point, the Incident Commander, typically the Data Governance Lead or a CISO delegate, anchors the classification of severity (Low, Medium, High, or Critical) according to potential impacts on confidentiality, integrity, and availability, and immediately notifies all IR stakeholders. This rapid classification ensures that the appropriate resources are allocated without delay.

The Containment phase involves both short-term and long-term activities. In the first two hours of containment, the IT Operations Lead (acting as Data Custodian) isolates affected network segments or endpoints, disconnecting compromised servers or blocking malicious IP addresses, and collaborates with the Forensics Lead to gather forensic evidence (for example, memory dumps and system logs). Simultaneously, temporary fixes such as patch deployments or forced rotations of compromised credentials are applied. Longer-term containment, which may extend from several hours to a few days, focuses on reestablishing a secure environment by standing up hardened backup systems and deploying additional access control lists until the full remediation plan is ready.

Once a system is isolated, the Eradication phase seeks to eliminate the root cause. The Forensics Lead conducts a comprehensive analysis, identifying malware strains, misconfigurations, or unauthorized access points, and remediates these issues by removing malicious code or disabling illicit user accounts. Post-remediation vulnerability scans are run to verify that the threat has been fully eradicated.

In Recovery, the IT Operations Lead restores affected systems from validated, clean backups, and the Business Unit Liaison coordinates user acceptance testing to ensure that business processes can resume without lingering security gaps. Over the subsequent five-day period, continuous monitoring is maintained to quickly detect any signs of reinfection or re-compromise before returning the environment to full production status.

Finally, during the Lessons Learned or Post-Incident Review, the Incident Commander convenes the IR team within five business days of containment. This session documents a detailed incident timeline, root cause, response steps taken, and any identified process gaps or technology shortcomings. The Data Governance Lead then updates the IR playbook, policies, and technical controls to address deficiencies, and circulates a concise executive summary to the Data Governance Committee and Executive Sponsor within ten business days.

Below is a standardized Incident Response checklist, which assigns ownership and timelines to each critical task in the process.

| **Phase** | **Task** | **Owner** | **Timeline** |
| --- | --- | --- | --- |
| **Preparation** | Maintain updated IR contact list & escalation matrix | Data Governance Lead | Ongoing (review quarterly) |
|  | Conduct vulnerability scans and ensure SIEM alerts active | IT/Security (Custodians) | Weekly |
|  | Perform tabletop exercises | Incident Commander | Semi-annually |
| **Identification** | Triage incoming alerts (SIEM, user reports) | Forensics Lead | < 15 minutes per alert |
|  | Classify severity (Low, Medium, High, Critical) | Incident Commander | Immediately |
|  | Notify all IR stakeholders | Communications Lead | Within 1 hour |
| **Containment (ST)** | Isolate network segments & compromised endpoints | IT Operations Lead | Within 1–2 hours |
|  | Collect forensic snapshots | Forensics Lead | Within 2–4 hours |
|  | Block malicious IPs / accounts | IT Operations Lead | Within 2–4 hours |
| **Containment (LT)** | Stand up alternate secure environment if needed | IT Operations Lead | Within 24 hours |
|  | Deploy interim patches or ACL changes | IT Operations Lead | Within 24 hours |
| **Eradication** | Identify & remove root cause (e.g., malware, misconfig) | Forensics Lead | Within 48 hours |
|  | Run vulnerability scans post-remediation | Forensics Lead | Within 48–72 hours |
| **Recovery** | Restore systems from clean backups | IT Operations Lead | Within 72 hours |
|  | Validate data integrity & perform user acceptance testing | Business Liaison | Within 96 hours |
|  | Reconnect network segments and monitor for re-infection | IT Operations Lead | Ongoing (5 days) |
| **Lessons Learned** | Conduct After-Action meeting, document timeline/gaps | Incident Commander | ≤ 5 business days |
|  | Update IR playbook, revise policies, communicate improvements | Data Governance Lead | ≤ 10 business days |
|  | Report to Executive Sponsor & Data Governance Committee | Data Governance Lead | ≤ 10 business days |

**Disaster Recovery**

The CIO and system administrators will create and implement a Disaster Recovery Plan. This plan must be periodically tested and the results should be used as part of the ongoing improvement of said plan. The recovery plan will seek to identify and protect against risks to critical systems and sensitive information in the event of a disaster while providing contingencies to restore information, systems and business functions.

Disaster recovery planning ensures:

Adequate management structure is in place to prepare for, mitigate and respond to a disruptive event using personnel with the necessary authority, experience, and competence

Documented plans, response and recovery procedures are developed and approved, detailing how the organization will manage a disruptive event and will maintain its information security to a predetermined level, based on management-approved information security continuity objectives.

Disaster Recovery plan includes the following:

* Business and systems impact analysis
* A classification system to identify critical systems and essential records
* Safeguards providing protective measures such as redundancy, fire suppression, surge protection, and environmental measures to protect sensitive equipment from dust, temperature, water damage or humidity
* Backups and offsite storage, such as cloud storage
* Contingency plans for different types of disruptions to Information Resource and systems availability
* Organizational responsibilities for implementing the disaster recovery plan
* Procedures for reporting incidents, implementing the disaster recovery plan, and escalating response to a disaster
* Training, testing, and improvement by CIO and systems administrators
* Annual review and revision by CIO and leadership team

**Policy Enforcement**

As our policies become defined, we can enable software to assist in the enforcement of these policies. We will need to establish a centralized point of control in the network for the enforcements to operate. This will be able survey the connection request and either confirm or deny access. We would be able to determine the consequences of violations from simply denying or disconnecting access to even full out block IP addresses. There would be the capabilities to determine access and permissions on certain applications to ensure that information is protected and that staff are operating within their assigned roles.

**Sources:**

White, Sarah K. “What Is CMMI? A Model for Optimizing Development Processes.” CIO, 1 June 2021, <https://www.cio.com/article/274530/process-improvement-capability-maturity-model-integration-cmmi-definition-and-solutions.html/amp>.

CMOE. “Strategic Alignment.” CMOE, 22 Sept. 2020, https://cmoe.com/glossary/strategic-alignment/#:~:text=Strategic%20Alignment%20Models&text=An%20alignment%20model%20is%20a,that%20have%20to%20be%20managed

Segal, Chelsea. “8 Cyber Security Best Practices For Your Small To Medium-Size Business.” Cox Blue, 2016, <https://www.coxblue.com/8-cyber-security-best-practices-for-your-small-to-medium-size-business-smb/amp/>.

Wilkins, Jesse. “What Is the Value of Records and Information Management?” AIIM, The AIIM Blog, 18 Feb. 2021, <https://info.aiim.org/aiim-blog/what-is-the-value-of-records-and-information-management?hs_amp=true>.

Thurman, Michael. “Litigation Readiness: Thurman-Legal.” Thurman Legal, 2020, https://www.thurman-legal.com/litigationreadiness.

Stern, Dawn E., et al. “Cybersecurity Obligations for Government Contractors – Focus on Them before the Government Focuses on You: Insights: DLA Piper Global Law Firm.” DLA Piper, DLA Piper, 22 Sept. 2021, https://www.dlapiper.com/en/us/insights/publications/2021/09/cybersecurity-obligations-for-government-contractors-focus-on-them/.

F5. (2022). *What is policy enforcement?* F5. Retrieved from <https://www.f5.com/services/resources/glossary/policy-enforcement#:~:text=In%20a%20computing%20context%2C%20policy,policy%20definition%2C%20application%2C%20and%20management>

Goggin, Michael. “How to Craft Your Company's Strategic Vision.” ClearPoint Strategy, 9 July 2021, <https://www.clearpointstrategy.com/strategic-vision/>.

Miller, Kelsey. “5 Critical Steps in the Change Management Process: HBS Online.” Business Insights Blog, 19 Mar. 2020, <https://online.hbs.edu/blog/post/change-management-process>.

Callinan, Peggy. “CIO Council Updated IT Strategic Plan.” Harvard University , Apr. 2015, <https://web.archive.org/web/20180212155530/https://huit.harvard.edu/files/huit/files/april2015_cio_council_strategic_plan_update_final_0.pdf>

Brecht, D. (2021, November 24). Best practices for implementing an IT/cybersecurity policy. Infosec Resources. Retrieved from https://resources.infosecinstitute.com/topic/best-practices-implementing-itcybersecurity-policy/

Kirvan, P. (2021, December 21). Top 10 IT security frameworks and standards explained. SearchSecurity. Retrieved from <https://www.techtarget.com/searchsecurity/tip/IT-security-frameworks-and-standards-Choosing-the-right-one?amp=1>

CISA. (2022). Cybersecurity framework. CISA. Retrieved from <https://www.cisa.gov/uscert/resources/cybersecurity-framework>

Spearstone. (2022). *Mobile device management policy examples | spearstone*. Spearstone. Retrieved from https://spearstone.com/mobile-device-management-policy-examples/

Bolland, E. (2021, September 14). *Example of an email policy and why it is important to cyber-security*. usecure Blog. Retrieved from https://blog.usecure.io/what-is-an-email-policy-and-should-my-company-have-it?hs\_amp=true

Biswas, P. (2021, March 31). *Example of disaster recovery policy*. PRETESH BISWAS. Retrieved from https://preteshbiswas.com/2020/02/01/example-of-disaster-recovery-policy/