BALDWINSVILLE
CENTRAL SCHOOL DISTRICT

Information Technology General Controls Assessment Findings Report

May 2019

Contents

Introduction

During April 2019, Bonadio & Co., LLP (Bonadio) performed an Information Technology General Controls Assessment review surrounding financial and general information systems, administrative controls, and physical security for the Baldwinsville Central School District (BCSD or the District) as part of the internal audit program being performed by Bonadio. As part of that request, we performed testing along with an inquiry and observational assessment of the information technology/infrastructure surrounding user access review, vendor management review with a focus on NY ED Law 2d and a basic NIST Cybersecurity review/gap assessment surrounding controls in place at the District. Our work was conducted through on-site/off-site efforts, walk-throughs, and inquiry-based reviews of BCSD controls and processes. The work included inquiries with key IT/IS personnel and, where noted in the report, basic testing of the physical, administrative, and technical controls that were communicated to be in place

The purpose of the assessment is to provide BCSD with an understanding of the possible gaps found within the scope of work and the controls surrounding access, vendor management, data privacy, data security, and regulatory compliance risks. Our work was limited to the specific procedures and analysis described herein and was based only on the information made available during our reviews. Accordingly, any lack of information supplied or changes in circumstances after this date will affect the findings outlined in this report. This engagement was performed as a point in time assessment and does not make a declaration of assurance for any points not reviewed.

Our report is intended to provide support regarding general guidance in mitigating the identified, but not all, threats and gaps in controls to reduce the possible adverse effect on impermissible disclosures, un-approved or unknown access to data, weak information security, and non-compliance with data security laws in the overall IT/IS infrastructure. This report and all deliverables from Bonadio & Co., LLP (Bonadio) are intended solely for the District’s internal use and benefit and are not intended to, nor may they be relied upon, by any other party (Third Party). This report can be used to help support the District’s actions in identifying areas where ITGC controls designed to support the District’s efforts may need to be implemented, or where existing implementations may need to be improved; however, the District’s management has final responsibility for all actions and compliance activities, as well as selection of controls.

This document contains highly sensitive and confidential information that should be communicated to external parties with due care and only under a confidentiality agreement. The enclosed material in this document and any of the referenced documents are proprietary, confidential information regarding the technologies, systems, and security operations and protections at BCSD. **The information in this report is being identified as protected under the NYS Public Officers (FOIL) Law § 87(2)(i).** That law allows that information regarding an entity’s systems and technology security information may not be disclosed as part of a FOIL request if such a disclosure "would jeopardize an agency’s capacity to guarantee the security of its information technology assets, such assets encompassing both electronic information systems and infrastructures.”

THE ENCLOSED MATERIAL IS PROPRIETARY AND CONFIDENTIAL INFORMATION AND IS THE PROPERTY OF BALDWINSVILLE CENTRAL SCHOOL DISTRICT. The enclosed material may not be disclosed, reproduced, or used in any manner whatsoever, other than by the addressee and the addressee’s authorized employees or representatives of the addressee who are directly responsible for evaluation of its contents, solely for the limited internal business purpose for which it is being transmitted to the addressee. Any trademarks used are the property of their respective owners.

This document and all others referenced within this document contain highly sensitive and confidential information that should be communicated to internal and external parties only with extreme care. The enclosed material in this document and any of the referenced documents are proprietary, confidential information regarding the technologies, systems, and security operations and protections at BCSD and should be treated as completely confidential and protected as such.

Introduction (Continued)

The output from the work efforts, documentation, reports, and findings surrounding this engagement are the property of BCSD and BCSD may choose to disclose those findings or documents.

Any statements of compliance are the responsibility of BCSD and the applicable regulatory and enforcement authorities.

The assessment was undertaken with the following key understandings:

- BCSD stores, processes, and transmits sensitive and other personally identifiable information (PII) consisting of electronic and physical data that is required to be managed appropriately and protected based on the laws and regulations affecting BCSD.
- The financial system used by BCSD, WinCap, is supported and maintained by Onondaga-Cortland-Madison BOCES (OCM).
- The student information system (SIS) used by BCSD, SchoolTool, is hosted and maintained by OCM.
- Not all controls in place at OCM were assessed as part of this review.

Assessment Processes

Bonadio incorporated information systems and data assurance standards to support the assessment of the controls communicated in place within the District. These standards, at times, included the processes and assessment guidelines detailed by the following:

- Information Systems Audit and Control Association (ISACA)
- Certified Information Systems Auditor (CISA) procedures, standards, and guidance
- The State and Federal laws, compliance actions, regulations, and standards affecting BCSD
- NIST information assurance and data security practices

The referenced processes, controls, documents, and data can be supplied upon request.

Introduction (Continued)

Bonadio used guidance supplied by regulatory and legal standards to assess the compliance controls in place within the District and to complete our assessment. They included at least the following:

- FERPA
- PCI DSS v3.2
- New York State data privacy and security laws
- CIPA
- COPPA

Definitions

NPI – Non-Public Information

PII – Personally Identifiable Information

FTC – Federal Trade Commission

InfoSec – Information Security

IT/IS – Information Technology/Information Systems

ITGC – Information Technology General Controls

ISP – Internet Service Provider

SOD – Segregation of Duties

WISP – Written Information Security Program

CSIRT – Computer Security Incident Response Team/Plan

E-Banking – Electronic Banking

SSAE18 – Statements on Standards for Attestation Engagements #18

SOC Report – Service Organization Control Report

Cybersecurity – A management system that is intended to being information security under explicit management control

PCI DSS – Payment Card Industry Data Security Standard

VPN – Virtual Private Network

BCP – Business Continuity Plan

DRP – Disaster Recovery Plan

BIA – Business Impact Analysis

IPS – Intrusion Prevention Software/System

Client Involvement

Bonadio met with several members of BCSD’s management and IT operations team including Jamie Rodems, Assistant Superintendent for Management Services; Tiffany Turner, School Business Official; John Cerio, Network Administrator; Richard DeLisle, Director of Technology; and others as necessary.

Controls in Operation and Processes Observation

Within every assessment, it is highly desirable to identify and communicate the areas that have been recognized as being effectively implemented and in operation at the time of the assessment. BCSD should understand that without these processes and controls, the overall risk posture in all areas assessed would be significantly negatively impacted. We have identified multiple areas where controls exist for risk management; however, it is critical to consistently and regularly assess these areas as they could easily lose their efficacy. Our review identified the following as not only being designed and operating effectively; but additionally as highly desirable repeatable practices and processes that need to be continued since they are seen as meeting or exceeding industry expectations and helping to significantly reduce the threat posture of the systems and data under the identified controls.

- Bonadio's interaction with BCSD identified an unquestioned willingness to actively "do the right thing".
- The BCSD personnel interfaced with are dedicated to protecting key assets.
- BCSD IT personnel express a great interest in improving processes, and actively seek input and expertise from outside sources.
- The process for provisioning, modification, and removal of user accounts utilizes a documented form.
- BCSD leverages the services of the OCM to streamline its internal processes.

ITGC Findings and Recommendations Overview

This report provides reasonable but not absolute information, findings, suggestions, and remediation advice regarding the matters below and other matters. The following observations have been identified as many of the key areas that management may wish to address as soon as reasonably possible. Individual recommendations are located in each section. Bonadio is available at any time to discuss each area and findings in more detail, supply reasoning behind findings, or otherwise communicate needed data and information to assist BCSD in mitigating any particular threat.

It is noted, and should be communicated to management, that an assessment at this level has not recently been performed by BCSD. In many instances, the areas and information reviewed by Bonadio may have identified previously undisclosed threats, potential new and desirable core security practice data assurance controls, and information assurance processes that may not have undergone any formal audit or testing in the past. Management's expectations should be tempered with this information and this lack of a recent assessment should be taken into consideration.

PLEASE NOTE: Core to any effective information security strategy is choosing a data security framework. Bonadio strongly urges BCSD to implement the controls identified in an industry standard (such as PCI DSS, ISO27001/2, NIST SP800-53, etc.) information security framework for all information infrastructure devices, applications, and systems.

The recommendations in this report are being supplied as possible and/or suggested mitigation or control enhancement requirements. A lack of recommendation does not imply that District may skip or otherwise not implement the needed controls or other changes. Senior management may opt to apply controls that have been chosen independently of our recommendations to mitigate the areas of possible information risk or regulatory non-compliance identified in this report.

Risk Level Definition

Critical risk areas are those items that individually, or in aggregate, pose an obvious vulnerability to the controlled access and protection of non-public information (NPI, PII, ePHI, etc.), non-compliance weakness, or a significant potential for uncontrolled or considerable risk of loss of availability, confidentiality, and integrity of sensitive and confidential information.

High risk areas are those where multiple control deficiencies or a single significant deficiency or weakness within the control structure have a potential to expose concerns that by themselves or in combination with other weaknesses have a significant risk of loss of data and NPI, regulatory sanction, or other reasonable weaknesses in information availability, confidentiality, or integrity. High risk areas likewise normally pose a risk of non-compliance to a regulation.

Moderate and other risk areas are those where a single control deficiency within the infrastructure has a minor but more than insignificant risk for loss of data and NPI, regulatory concern, or other minor availability, confidentiality, or integrity concerns.

Key Critical Risk Findings

Vendor Management

BCSD leverages a number of relationships with third party vendors. The most notable vendors include OCM and Google. The District does not have a universal and repeatable process for initial and ongoing vendor and vendor contract management risk assessments. BCSD does not actively request or review any assurance documentation from vendors, such as an SSAE18 SOC 2 report. BCSD has limited vendor management controls and processes in place that are required under Ed Law 2d. Likewise, BCSD has not inventoried all areas and systems in which student data is stored or processed.

Risk Assessment

Third party vendors are responsible for at least 50% of data breaches. Without effective and measured processes, weaknesses in vendor controls have the ability to significantly negatively impact BCSD, the data that it relies upon, and its reputation. Use of third parties reduces management's direct control of activities and may introduce new or increase existing risks, specifically operational, compliance, reputational, strategic, and other interrelated risks. Increased risk most often arises from greater complexity of the District's environment, ineffective risk management by BCSD, and inferior performance by the third party.

Recommendation

BCSD should, at least annually, risk assess all vendors that interact in any way with BCSD's sensitive or legally protected information such as PII. Additionally, BCSD should:

1. Require all vendors or third parties who access protected student data to contractually comply with Ed Law 2d security and reporting requirements
2. Have a single point of contact for vendor contract and assurance management.
3. Require the correct control assurance documentation (i.e., SSAE18 SOC1, SOC2 Type 2 for Security, Availability, Confidentiality, and Privacy principles, ISO27001, 27002, etc.) from all vendors that have access to PII. The reports should be reviewed for identified risks, and then BCSD should determine if these risks affect the vendors' ability to perform their responsibilities while maintaining the confidentiality, security, and availability of BCSD's data, and if the controls are found to be deficient, alternatives for controls or alternative vendors need to be pursued.
4. Perform reviews and risk ranking prior to hiring a vendor, as well as at least annually thereafter for any key vendor.
5. Contractually require vendors to have 100% of all portable devices capable of accessing, storing, or processing BCSD data to be encrypted at all times.
6. Adopt risk management processes commensurate with the level of risk and complexity of its third-party relationships.
7. Ensure comprehensive risk management and oversight of third-party relationships involving critical activities.
8. Have a measureable, repeatable, and effective risk management process throughout the life cycle of the relationship including:
    a. Plans that outline BCSD's strategy, identify the inherent risks of the activity, and detail how BCSD selects, assesses, and oversees the third party.
    b. Proper due diligence in selecting a third party.
    c. Written contracts that outline the rights and responsibilities of all parties.
    d. Ongoing monitoring of the third party's activities and performance.
    e. Contingency plans for terminating the relationship in an effective manner.
    f. Clear roles and responsibilities for overseeing and managing the relationship and risk management process.
    g. Documentation and reporting that facilitates oversight, accountability, monitoring, and risk management.
    h. Independent reviews that allow BCSD's management to determine that BCSD's process aligns with the vendor's strategy and effectively manages risks.

Management Response:

The District's Director of Technology is the Data Privacy Officer. In this role the Director Technology will:

- Be the Point of Contact for Vendors who house PII
- Communicate with vendors and obtain assurances for compliance with ED Law 2D
- Keep assurances on file and review annually.
- Maintain a database of Risk Assessments that will be used to house information on physical and data risks.

Encryption Controls

Bonadio determined that BCSD is currently utilizing Google products for storage of a significant amount of sensitive information, such as emails and other documents; however, automatic encryption of external email is not enabled. Emails that contain sensitive or confidential information may not be encrypted. It was communicated that while mobile devices (such as laptops, Chromebooks, smartphones, and tablets) used by District personnel to access this information are encrypted, desktops are not encrypted.

Risk Assessment

Failure to encrypt sensitive data at rest or in transit significantly increases the risk of loss or theft of confidential and legally controlled data.

Recommendation

BCSD should consider disabling the ability of users with access to sensitive data to download files to their local devices. Any users with the ability to download sensitive information should be required to have encryption enforced on their respective devices. The District should not utilize any “free” applications, from Google or other web-based services, to store, transmit, or share sensitive data, as privacy and data security cannot be ensured. BCSD should consider encryption of servers and ensure all emails that may contain confidential or sensitive information are encrypted.

Management Response:

The District has a Policy to force all email to use end-to-end encryption enabled for all staff. If the receiver does not support end-to-end encryption the email will not be sent.

The District is considering and reviewing policies to limit data transfer to local devices. As these recommendations could have an impact on business continuity, the Director of Technology and Network Administrator will test and evaluate each proposed control as to its efficacy and impact on business continuity.

The District is considering the use of Windows EFS to encrypt data on local servers and is beginning to test this in the Summer of 2019.

The impact of encrypting desktop hard disks on Windows devices is being evaluated as well as imaging operations. We are currently testing encrypting hard disks on Windows and Mac laptops that leave the district.

Change and Patch Management

Bonadio identified that patches and updates to applications and network devices are implemented via ZENworks. It was communicated that patching performed at the District is not audited for all applications and systems on a regular basis. Per review of vulnerability scan results performed by Bonadio while onsite, it was determined that a number of critical and high severity Microsoft patches were not applied to the devices scanned.

Risk Assessment

Updating applications to the latest version is essential to maintain security and prevent unauthorized network access. Out-of-date software provides exploitable security flaws that could allow entry to sensitive information by unauthorized parties. Failure to audit all of BCSD’s network devices for up-to-date software increases the risk that some of the systems may not be patched in a timely manner.

Recommendation

BCSD should conduct regular patch audits for all systems and applications to ensure that software remains up-to-date. BCSD should review the patching procedures in place to ensure that the systems used by BCSD are kept up-to-date.

Management Response:

The District has developed and implemented policies and procedures with regards to patch audits and patching procedures.

Key High Risk Findings

Information Systems Disaster Recovery and Business Continuity

BCSD utilizes Commvault to perform backups of local data from its main data center located in the transportation building to the cloud. The District does not perform formal restoration tests on a regularly scheduled basis to ensure the integrity of the backups.

It was determined by Bonadio that the District has not performed a Business Impact Analysis (BIA) to identify and prioritize the systems in use. It was likewise communicated that while formalized continuity documentation (i.e., Disaster Recovery Plan (DRP) and Business Continuity Plan (BCP)) is in place, the plans do not show evidence of District review. It was communicated that the OCM has a documented DRP and BCP that is currently in place; however, OCM plans were not shared with Bonadio as part of this assessment.

Risk Assessment

If BCSD were to suffer a significant physical or technological disaster, it is not unreasonable to believe the information used to perform day to day business functions would be unavailable for an unacceptable length of time. It should be noted that the backup processes for systems hosted offsite at OCM were not evaluated as part of this assessment. It should be noted that several laws to which the District is subject may require a full and tested disaster recovery and business continuity plan and that operations during an emergency must maintain data security and privacy at all times. Not performing a BIA increases the risk that management could be unable to make an informed decision regarding risk exposure and acceptable mitigation techniques, which could lead to service disruptions in the event of an issue.

Recommendation

BCSD needs to perform a full BIA that includes all lines of business, locations, and departments. The BIA should be conducted by personnel with material knowledge of BCSD operations, not just the information technology team. The BIA should include financial impact statements based on known or suspected risks and their impact to business functionality. This BIA plan should be used to update current disaster recovery and business continuity procedures. The plans need to be tested at least annually. Further, the DRP and BCP should be updated at least annually and take into account all changes in the infrastructure, personnel, and processes at BCSD.

Management Response:

The Director of Technology will interview each department director to determine critical systems. The levels of risk, impact on functions, management of risks and mitigating actions will be determined.

User Access Recertification

Bonadio identified that network and SchoolTool user access accounts are managed by the District. The District utilizes a documented access change request form for adding, modifying, and removing user access accounts. In addition, user accounts for the systems in use by BCSD are reviewed annually; however, it was communicated that reviews and audits of user accounts are not formally documented.

Risk Assessment

Failure to document the reviews of user access rights makes it difficult to ensure operational effectiveness, as it cannot be proven that full reviews are being conducted.

Recommendation

BCSD should formally document its annual recertification of all users to ensure that each user’s access level is agreeable to their specific job. Additionally, BCSD should review the user access policies in place to ensure that current BCSD procedures are kept up-to-date.

Management Response:

The Director of Technology will certify that user access was reviewed. A written policy will be developed to drive the certification.

Password Parameters

Per review of the District's network policies, it was determined that the District currently enforces moderately strong password requirements. Staff passwords require a minimum of eight characters, expire after 90 days, and lockout users for 30 minutes after 10 invalid login attempts.

Risk Assessment

The enforcement of strong password configurations is a significant layer of protection for system access. Without the implementation of strong password configurations such as password complexity, expiration, history, lockout threshold, and lockout duration, there is an increased risk of unauthorized access to systems and data.

Recommendation

BCSD should configure password settings for network and application access to be sufficiently complex. This would include a password minimum length of ten to twelve characters with a requirement that each password must contain upper and lower case letters, numbers, and special characters. In addition, passwords should be changed no less frequently than every 90 days. Users should be prevented from reusing at least their previous four passwords. Systems and applications should lock after three incorrect attempts and should require an administrator to unlock the account.

Management Response:

The Director of Technology will review recommendations. Parameters for passwords for District Staff is set at a minimum of eight characters with a combination of upper case, lower case, numbers and a symbol. Lockout after ten unsuccessful attempts to login will be changed to five unsuccessful attempts.

Incident Response Plan

It was determined by Bonadio that while OCM has formalized incident response procedures in place, the District does not have a documented plan in place that outlines the procedures to be followed in the event of an IT or cybersecurity incident.

Risk Assessment

Without tracking and reporting of security incidents at the District level, there is a possibility for incidents to go unresolved or undetected. This presents the potential for data loss and system down time at the District.

Recommendation

BCSD should draft, approve, and implement a plan to respond to any IT security incidents that occur at the District. This type of plan will help to minimize the effects of an incident, as well as reduce the amount of downtime incurred. The plan should include procedures for the Identification, Containment, Root Cause Analysis, Eradication, and Return to Normal Operations for each identified incident, in addition to a corrective action plan in the aftermath of an incident in order to ensure that a similar event is less likely to occur in the future.

Management Response:

The Director of Technology will interview each department director to determine critical systems. The levels of risk, impacts on functions, management of risks, and mitigating actions will be determined from the findings of the interviews.

Key Moderate Risk and Other Findings

Information Security Training

Bonadio identified that while BCSD communicates basic information security awareness tips to staff via email, a comprehensive and ongoing IT security awareness training program is not in place for all District employees.

Risk Assessment

All employees of BCSD are responsible for data security, as the protection of the District's data is dependent upon the actions of every employee. Failure to train all employees in the risks associated with information technology, along with the best practices for protecting BCSD data, significantly increases the likelihood of a data security event.

Recommendation

BCSD should create and implement a training program for all employees in which the risks of information technology, as well as the efforts each employee can put forth to increase security, are communicated to staff. This type of training should be conducted at least annually.

Management Response:

The Director of Technology will contact vendors and inquire about an online training program for all staff. This would be in addition to the bi-monthly Cybersafe Workforce tips that are currently delivered via email and the monthly MS-ISAC newsletter. This online training would replace the current online training that was developed and implemented by the Director of Technology in 2014-15.

Performance of Regular Risk Assessments

Bonadio determined that the District's last assessment of IT controls was in 2016.

Risk Assessment

Failure to perform regular (suggested at least annually) risk assessments increases the likelihood that systems and data may not be maintained to a level that provides management with the appropriate information to operate and exercise its fiduciary responsibility.

Recommendation

BCSD should develop and implement a comprehensive risk assessment process, either internally or through the use of a third party. Once established, this assessment should be performed on an ongoing basis (at least annually) to identify new and potential risks and mitigation strategies. In addition, effective regulatory oversight requires the establishment of an independent review process to ensure that compliance with laws and regulations is part of the overall ERM process. Bonadio would recommend that the assessment likewise be completed at any significant infrastructure change.

Management Response:

The Director of Technology will interview each department director to determine critical systems. The levels of risk, impacts on functions, management of risks, and mitigating actions will be determined from the findings of the interviews. This will be completed annually and will continue to utilize the services of an independent auditor to test systems.

Laws, Regulations, and Standards Findings

BCSD receives, stores, processes, and transmits a growing amount of verbal, written, and electronic legally or regulatory protected information. A majority of the controls needed to enforce data privacy and security, based on those other laws and regulations, were missing the appropriate policies, procedures, and enforced protections.

The following laws, regulations, and standards, at minimum, are seen as potentially applying to the data and infrastructure at the District:

- New York State data privacy and cybercrime laws
- Family Educational Rights and Privacy Act (FERPA)
- TEACH Act/Digital Millennium Copyright Act
- Computer Security Act of 1987
- The Privacy Act of 1974
- Payment Card Industry Data Security Standard (PCI DSS)

Risk Assessment

Most enforcement actions surrounding compliance with the laws and regulations stem from a breach of protected PII in verbal, written, or electronic form. Based on the information reviewed, the lack of enforced policies, and the minimum understanding of the rules requirements across the personnel and departments affected by the laws (IT, HR, Business Office, etc.), BCSD is likely exposed to significant fines, sanctions, and the resulting financial and reputational damage.

Recommendation

BCSD needs to perform a full and complete assessment of all the laws and regulations that it is required to meet. The considerations for those laws must be applied equally against its vendors when the vendor has any material impact on data storage, transmission, management, or processing.

Management Response:

The District will continually review, assess and apply all laws associated with data management, transmission and processing. The Director of Technology will develop policy documents to ensure compliance with the law.

Vulnerability Scan Findings

Internal technical vulnerability assessments and penetration tests are not performed on a regular basis by BCSD.

Technical vulnerability scans were performed on a subset of the server and workstation assets at BCSD; the summary of the findings is below. These items are a subset of all items found. Full vulnerability scan details and remediation steps have been provided to BCSD in a separate report.

The vulnerabilities included the following:

- There are multiple missing Windows security patches.
- There are multiple missing Java security patches
- There are multiple TCP vulnerabilities that may allow for a denial of service attack.
- The Apache web server is affected by multiple vulnerabilities.
- SSL vulnerabilities exist that may allow for man-in-the-middle attacks and disclosure of sensitive information.
- The SNMP server is using default community names.

Risk Assessment

A lack of mitigated vulnerabilities increases the risk of unintended loss, compromise, or a loss in integrity of data. The lack of mitigated vulnerabilities significantly increases the ease with which a malicious internal or external entity could access, copy, delete, and exfiltrate BCSD data.

Recommendation

All systems with any role in storing, maintaining, or accessing sensitive or confidential data must be regularly (at least quarterly) scanned and vulnerabilities must be mitigated as needed. BCSD IT staff should review the vulnerability scan documents provided to BCSD by Bonadio.

Management Response:

The District has purchased a program to perform regular vulnerability assessments and penetration tests. The District has also purchased an additional software that performs virus protection.

The District deploys security patches once a month or if a critical bulletin is released the District will patch immediately.

Appendix 1: COBIT Controls Matrix

COBIT is a business framework for the governance and management of enterprise IT. This incorporates the latest thinking in enterprise governance and management techniques, and provides globally accepted principles, practices, analytical tools, and models to help increase the trust in, and value from, information systems. COBIT builds and expands other major frameworks, standards, and resources, including ISACA's Val IT and Risk IT, Information Technology Infrastructure Library (ITIL®), and related standards from the International District for Standardization (ISO). The matrix below is one tool for measuring enterprise IT conformance with COBIT expectations and the multiple levels of controls assurance defined as:

Basic - There is evidence that the enterprise has recognized that the issues exist and need to be addressed. There are, however, no standardized processes; instead, there are ad hoc approaches that tend to be applied on an individual or case-by-case basis. The overall approach to security management is disorganized.
Developing - Processes have developed to the stage where similar procedures are followed by different people undertaking the same task. There is limited or no formal training or communication of standard procedures, and responsibility is left to the individual. There is a high degree of reliance on the knowledge of individuals and, therefore, errors are likely.
Adequate - Procedures have been standardized and documented, and communicated through training. It is, however, left to the individual to follow these processes, and it is unlikely that deviations will be detected. The procedures themselves are not sophisticated but are the formalization of existing practices. It is possible to monitor and measure compliance with procedures and to take action where processes appear not to be working effectively. Processes are under constant improvement and provide good practice. Automation and tools are used in a limited or fragmented way.
Advanced - Processes have been refined to a level of best practice, based on the results of continuous improvement and maturity modeling with other enterprises. IT is used in an integrated way to automate the workflow, providing tools to improve quality and effectiveness, making the enterprise quick to adapt.

The matrix below is a proprietary tool used by Bonadio that incorporates the functions of COBIT, ITAF, and Risk IT. Our measurement of each control level is highlighted in green. It is noted that the controls being discussed are those outside those in place for PCI DSS.

Management: Leadership				
Leadership: Oversight				
Indicator\Status	**Basic**	**Developing**	**Adequate**	**Advanced**
Security Goals	Mgmt. provides minimal direction and oversight on IT-related security issues.	Mgmt. develops a basic mission statement on security.	Mgmt. articulates a clear mission statement on security.	Mgmt. articulates a clear mission statement on security that is integrated with policy and overall mission.
	Mgmt. acknowledges efforts made by IT Director to meet governing security and confidentiality regulations.	Mgmt. authorizes IT Director to ensure compliance with governing security and confidentiality regulations.	Mgmt. authorizes IT Director and security team to ensure compliance with governing security and confidentiality regulations.	Mgmt. authorizes IT Director and security team to ensure compliance with governing security and confidentiality regulations.
			Mgmt. is periodically involved in high level security planning.	Management regularly provides oversight of high level security planning.

Legal Compliance	Initial effort has been made to bring IT installations into compliance with security-related laws (FERPA, CIPA, HIPAA, etc.), but actual level of compliance is not clear.	IT unit attempts to manage compliance security-related laws (FERPA, CIPA, HIPAA, etc.) as far as major vulnerabilities are concerned (content filtering, confidential databases)	Security team assists with identifying potential concerns for compliance with all State and Federal Laws (FERPA, CIPA, HIPAA, etc.). IT unit makes such compliance part of its protocol for new installations and periodic security reviews.	Security team or external auditor verifies full compliance with all State and Federal Laws (FERPA, CIPA, HIPAA, etc.). Compliance review is a routine component of new installations and periodic reviews.
Policy Implementation	Policy governing security efforts is limited to general statements that may be challenging to translate into specific security measures.	Policy governing security efforts provides a basic sense of direction for implementing security. Some policy areas may be missing (e.g., enforcement procedures for security violations)	Policy governing security efforts provides adequate direction for implementing security measures. Some policy areas out of date or lack clarity. Leaders specifically authorize the IT unit to enforce policy	Policy governing security efforts provides effective direction with sufficient clarity to ensure appropriate implementation. Leaders specifically authorize IT unit to enforce policy. Security Team provides additional oversight.

Leadership: Support

Indicator\Status	**Basic**	**Developing**	**Adequate**	**Advanced**
Budget and Human Resources	No support specifically earmarked for security.	Security is not a budget line item, but some purchasing reflects security needs.	Key security-related items included in budget planning.	Strong needs integrated into all IT budgeting.
Communication	Little or no leadership communication on security issues.	Leadership occasionally delivers security messages to stake holders.	Leadership regularly delivers clear message to stakeholders.	Leadership effectively and frequently incorporates security message in to stakeholder communication when appropriate.

Management: IT Security Management

IT Security Management: Security Team

Indicator\Status	Basic	Developing	Adequate	Advanced
Charter & Responsibilities Membership	No formal security team exists.	Ad hoc Security Team lacks formal authorization.	Security Team is authorized by the administrators to develop a security plan and oversee its implementation.	Security Team is authorized by the board or committee to develop a security plan and oversee its implementation.
		Ad hoc Security Team includes: management and IT Staff	Security Team members include representatives from: management, C suite, Staff, IT Staff, Experts	Security Team members include: CIO/CFO, other C suite, IT Director, ISO, Privacy Officer, Compliance Officer, External Experts.
		IT staff and leadership confer on security requirements on an ad hoc basis.		

IT Security Management: Security Planning

Indicator\Status	Basic	Developing	Adequate	Advanced
IT Planning in general	Little or no comprehensive IT planning.	IT planning includes consideration of security.	IT planning includes security as a component. Security provisions included in contracts with vendors, consultants, and outsourced services are reviewed for compliance with security requirements.	IT planning fully integrates security requirements. All security provisions included in contracts with vendors, consultants, and outsourced services are reviewed for compliance with security requirements. Specific security planning is fully coordinated with IT security planning.
Security Plan	Security practices exist without a formal security plan	Security plan may exist only as an internal IT department document. Plan includes occasional network testing, but validity of plan has not been verified.	Security plan written or reviewed in past 24 months. Plan is derived from asset-based risk assessment process and includes end-user training and communication includes periodic testing and monitoring.	Security plan revised or reviewed in past 12 months and discussed and approved by leadership and board. The Plan is derived from asset-based risk assessment process; links goals and policies, end-user training, and communication; and includes periodic testing and monitoring of all data and third parties.

Security Audit	No security audit completed within past 36 months.	Internal security audit completed within past 36 months.	Internal security audit completed within past 18 months. Scope of audit linked to security plan. Provides budget support for security measures.	Security audit completed by qualified independent consulting group within past 12 months; internal audit completed within past 3 months. Scope of audit governed by a comprehensive security plan, focuses on laws, regulations, and compliance, and is used for ongoing risk assessments and remediation.

IT Security Management: Security Implementation

Indicator\Status	**Basic**	**Developing**	**Adequate**	**Advanced**
IT Staffing Levels	Insufficient numbers to expand IT services. IT staff may be non-dedicated or part-time.	Full-time staff. Additional staff is needed to address all IT services or expand service.	IT staff maintains IT systems and performs procedures efficiently.	IT systems operate at a high level of reliability due to effective organizational practices; further reduction in staff-to-equipment ratios may produce only slight improvement in service levels.
Staff competency	Insufficiently trained in desktop support or network management.	Job descriptions indicate mixed network and desktop support roles without specific mention of security-related tasks.	Clear division of responsibility between network and desktop support with clear assignment of responsibility for security tasks and roles.	Clear division of responsibilities, including security-related tasks. Additionally, IT staff are cross-trained to provide backup support.
Security Staffing	No one specifically assigned to attend to security.	CTO or other management staff also deals with security.	A senior staff person is assigned to manage security.	A Chief Security Officer with an appropriate team of specialists is in place with the commensurate authority.

Technology: Architecture and System Design

Architecture and System Design: Overview

Indicator\Status	Basic	Developing	Adequate	Advanced
Architecture: Overview	Architecture at basic stage; shortcomings exist in all areas (Perimeter Security, WAN security, Internet connection).	Architecture lacks capacity for growth or implementation of stronger security measures; shortcomings exist in two or more areas (Perimeter Security, WAN security, Internet connection).	Appropriate Architecture: solid functionality exists, but compared with advanced level, shortcomings exist in one or more areas (Perimeter Security, WAN security, Internet connection).	Appropriate Architecture with room to grow.

Architecture and System Design: Perimeter Defenses

Indicator\Status	Basic	Developing	Adequate	Advanced
Firewall	Firewall software not present at all network entry points.	Perimeter/intrusion defense: installed.	Perimeter - intrusion defense: fully configured.	Perimeter/intrusion defense: a layered monitored strategy from desktop to firewall provides fully integrated protection.
Virus protection	Virus protection is not installed on all network-connected devices.	Virus protection installed on all devices; centrally-managed updates for at least half of client computers; all other computers receive regular, automated updates.	Centrally managed, integrated virus protection firewall, intrusion detection is deployed to most workstations.	Centrally managed, monitored integrated virus protection, firewall, intrusion detection for all workstations, servers, portable and remote devices.
Content filtering and Spam control	Content filtering may have been implemented at some locations, but implementation is not monitored appropriately.	Content filtering has been implemented for all locations, but monitoring is sporadic.	Content filtering is properly monitored for effectiveness, but impact on throughput is unknown.	Content filtering is handled with devices capable of delivering a high level of effectiveness without significantly impacting network performance.
VPN	No VPN configured	No VPN or insufficient VPN controls	VPN permits a limited number of users to access the network remotely	VPN configured for full secure access.
Wireless Access control	Wireless Access: Reliance on end-user caution or light, localized usage to limit risk.	Wireless access may be spreading faster than it can be properly controlled. Not all access points are properly configured.	Wireless access is properly configured; Secondary strategies may include non-technical tactics (e.g., powering off access points over weekends). Intrusion risks are balanced against accessibility.	Wireless access properly configured; secondary strategies (VPN, segmentation) provide additional layer of security. Intrusion risks are minimized by monitoring and strong authentication.
Segmentation	Segmentation: no network segmentation beyond building-level.	Segmentation: no network segmentation beyond building-level.	Segmentation: network segmented for certain tasks.	Segmentation: centrally-managed building LANs, switches, servers.

Authentication and Authorization	Authentication - authorization: not available	Authentication & authorization: Not managed via the WAN, if at all. End users have no access beyond local LANs to WAN resources (except to specific systems).	Most authentication is performed but system-wide implementation may be incomplete	Full automated and audited authentication.
Redundancy	Redundancy: servers may lack reliability; no or limited spare parts on hand for critical network devices.	Redundancy: some critical servers have at least RAID 5 reliability; some spare parts on hand.	Redundancy: most critical servers are protected by redundant units. Spare components may not be available for all critical network devices.	Redundancy: all critical servers are protected by redundant units. Spare components are available for all critical network devices.
Standardization	Standardization: Building LANs not standardized, require local maintenance.	Standardization: Building LANs not standardized, require local maintenance.	Standardization: Most but not all building LANs, switches, servers support remote management.	Standardization: standardized hardware, network configuration.
Remote Management	Remote Management: WAN lacks remote monitoring and management of routers, switches, and LAN servers.	Remote Management: Existing WAN devices may not support remote monitoring and management. As WAN expands, new devices will support remote management; legacy devices may remain in service past "retirement" age.	IT Plan implemented to eliminate legacy devices that cannot be remotely managed.	Remote Management: All routers, switches, and LAN servers are remotely monitored and managed.
Architecture and System Design: Internet				
Indicator\Status	**Basic**	**Developing**	**Adequate**	**Advanced**
Bandwidth	Bandwidth (dial-up, cable, or DSL) is insufficient. Bottlenecks occur frequently.	Bandwidth (cable, DSL, frame relay, or T1), while improved, may not be sufficient for rapidly-growing use. Lack of reliability inhibits user confidence.	Bandwidth is adequate for current requirements but may lack capacity for future expansion. Reliability, while improved, is still an issue for some users.	Bandwidth is adequate for current requirements and expandable for future growth. Users have full confidence in the network.
Internet Infrastructure	No redundant internet access.	No redundant internet access.	Backup internet access on line (cable, DSL) for critical functions.	Backup internet access on line (cable, DSL) for critical functions.

Technology: IT Operations				
IT Operations: WAN and LAN management				
Indicator\Status	Basic	Developing	Adequate	Advanced
IT Operations: Overview	Most time spent on urgent problems.	IT operations include time allocated for some monitoring and maintenance.	Standards and procedures in place: IT operations include time allocated for routine monitoring and maintenance.	Efficient, growth-oriented operation: IT operations include time allocated for routine monitoring and maintenance.
Backups	Backups may not include all mission-critical servers.	Daily and weekly backups. Off-site storage not regularly tested.	Consistent backups including off-site storage; periodic testing done.	Consistent backups including off-site; DR Plan routinely tested. File restoration practice included in crisis management preparedness and testing.
Routine Network Monitoring and Testing	Minimal scheduled network checks. No file integrity testing. No capacity for password/access testing	Daily checks for virus protection, network services, backup status.	Daily checks for network intrusion, virus protection, network services, backup status. Monthly file integrity testing.	Live monitoring for network intrusion, virus protection. Daily checks on network services, backup status. Maintenance logs kept. Monthly file integrity testing. Password testing every 60-90 days. Twice-yearly wireless network intrusion detection
Major Systems maintenance	Major services (email, internet access) occasionally unavailable for 8 hours or more.	Major services (email, internet access) rarely unavailable for 8 hours or more.	Major services (email, internet access) rarely unavailable for more than 4 hours.	Major services (email, internet access) rarely unavailable for more than 2 hours.
Documentation	No daily maintenance and monitoring logs. System documentation is largely absent. Equipment inventory managed at the building level.	Maintenance logs kept. System documentation is minimal; knowledge of system configuration is highly dependent on individuals. Client computer inventory managed at building level; all network components managed by central IT group.	Maintenance logs kept. System documentation is maintained for critical services and network management. Computer inventory managed at 100% level.	Maintenance logs kept and reviewed by management. System documentation is maintained for all services and network management and users assets. Client computer inventory reviewed for applicability to job role and managed 100%.

External Partners & Vendors	External partners' or vendors' security practices are not known or verified.	External partners' or vendors' security practices: documentation exists but practices are not verified.	External partners' or vendors' security practices: vendors assert that federal, state, and requirements are met. Vendor credentials are checked.	For all external partners' or vendors' security practices: external audit reports verify that federal, state, and requirements are met and reports are suppled and reviewed at least annually. Redundant systems are in place; emergency procedures for service restoration are established. If required, all code is escrowed.
IT Operations: End User Support				
Indicator\Status	**Basic**	**Developing**	**Adequate**	**Advanced**
End User Security: Overview	Unenforceable	Increasing, not verifiable:	Widely in use, generally verifiable:	Seamless, highly verifiable:
		Workstation policies and protocols not adequate to support organizational IT security goals.	Workstation policies and protocols at the user level assist organizational security with appropriate hardware and software controls.	Workstation policies and protocols at the user level assist organizational security with appropriate hardware and software controls
Installation configuration repair	Client desktop computers: no remote management.	Client desktop computers: mixed local and central responsibilities.	Client desktop computers: strong central policy, distributed management.	Client desktop computers: strong central policy, distributed management. Efficient repairs are done using imaging software.
	No capacity to rebuild computers using imaging software.	Some computers can be rebuilt using imaging software.	Most computers can be rebuilt using imaging software.	
Standardization	No standardization plan exists. Any de facto standards for hardware and software result from episodic bulk purchasing or donations.	Legacy software and hardware hampers standardization efforts.	Legacy software and hardware are in the process of being phased out.	Standardization goals are achieved. 3 to 4 year replacement cycle established. The majority of all computers use one operating system.
	No cycle of hardware replacement exists.	Limited cycle of hardware replacement exists.	5 to 6 year replacement cycle established.	
		Typically two to four generations of PCs/Macs/Servers may be online.	Number of operating systems supported has been reduced to Mac and PC systems.	
Patch management and application updates	Servers, other network devices: sporadic.	Servers, other network devices: routine updates.	Servers, other network devices: automated updates.	Servers, desktops, laptops, remote devices, cellphones, tablets, and other network devices: fully automated updates.

Patch management and application updates	Staff and administrator computers: virus data and system updates (patch management) are the responsibility of end users.	Staff and administrator computers: IT unit provides instructions and reminders for virus data file and system updates (patch management) to end users whose computers are not automatically updated.	Most virus data and system updates (patch management) are managed remotely for many assets.	All virus data and system updates (patch management) are managed remotely.
Patch management and application updates	Limited desktop management software may be in use for updates.	Central IT staff use desktop management software for updates in some locations.	Have established effective updates and routines controlled by central IT staff.	Staff and lab computers: central IT staff has established efficient protocols to refresh operating systems and deploy software in all locations.
Software Licensing	Software licensing managed at the building level.	Software licensing for operating systems, virus protection, and office productivity software is site-licensed by central IT group; other software, purchased without central guidance or controlling policy, is controlled at the building level.	Software licensing for operating systems, virus protection, and office productivity software is site-licensed by central IT group; other software is purchased with central guidance.	Software licensing for operating systems, virus protection, and office productivity software is site-licensed by central IT group; other software is purchased with central guidance or controlling policy to coordinate training and encourage shareable knowledge.
Passwords	Password protection is end users' responsibility; periodic password changes are not required.	Password policies exist but are not centrally enforced nor routinely used in all locations.	Password policy is monitored by LAN or WAN managers.	A centrally managed and strong password policy is monitored and enforced by WAN managers.
Advanced End User Security	No password requirements are in place for at-risk locations, databases, or systems.	Limited password requirements are in place for at-risk locations, databases, or systems.	Strong password requirements are in place for all at-risk locations, databases, or systems.	Biometric security devices, smartcards, or strong password requirements are in place on all computers.

Environmental and Physical Security

Environmental Security

Indicator\Status	Basic	Developing	Adequate	Advanced
Anticipation of natural disasters	Environmental hazards given cursory attention: Flood or water damage: network devices may be in basements or sitting on floors.	Environmental hazards partly addressed: Flood or water damage: network devices may be in basements or sitting on floors.	Most environmental hazards addressed. Flood or water damage: critical infrastructure not at risk.	Environmental hazards recognized and addressed. Flood or water damage: critical infrastructure not at risk. Redundant equipment and warning systems are in place to guard against other disasters.

Fire Protection	Fire: no dedicated alarms. Network equipment may be located in unlocked, multi-use spaces (offices, classrooms, etc.).	Fire: no dedicated alarms. Network equipment may be located in space also used for storage or custodial purposes.	Fire: alarms installed. Network equipment in clean, dedicated space.	Fire: alarms and suppression equipment installed. Network equipment in clean, dedicated space.
Climate Control	Temperature and humidity: no dedicated HVAC for network devices.	Temperature and humidity: network devices may lack protection from extreme heat, dampness.	Temperature and humidity: network devices properly ventilated.	Temperature and humidity: network devices properly ventilated, automated monitoring controls are in place.
Power Supply	Power: minimal UPS support for servers.	Power: most servers and network devices on UPS.	Power: all servers and network devices protected by uninterruptible power supply units or generators	Generator power is in place for all devices.
Inspection and review	No special environmental inspections are made.	Facilities are inspected occasionally for hazards.	Facilities are inspected periodically for most hazards	Facilities and emergency equipment are inspected on regular basis by external experts.

Physical Security				
Indicator\Status	**Basic**	**Developing**	**Adequate**	**Advanced**
Physical Security: Overview	IT facilities and infrastructure: not secure.	IT facilities and infrastructure: partially secure.	IT facilities and infrastructure: mostly secure.	IT facilities and infrastructure: secure.
Facilities	Many network devices are in shared or uncontrolled locations, e.g., book cupboards, custodial closets. Network cabling may be exposed, within reach, or subject to damage during routine building cleaning and maintenance.	Most network devices are in dedicated, secure locations.	All network devices are in dedicated, secure locations.	All network devices are in dedicated, secure spaces.
End User equipment security	Equipment is not physically secured where required.	Core equipment is physically secured where required.	Majority of all equipment is physically secured (locks, cables) where required.	All equipment physically secured (locks, cables) where required. Equipment monitoring is in place and automated wipe, scan, or asset locators are in place.
Access control	Control of Staff access to computers depends on direct supervision.	Staff access to computers is appropriately controlled in some locations.	Staff access to computers is appropriately monitored where required.	Staff access to computers is appropriately controlled and remotely monitored where required. Staff access to network devices is restricted where appropriate. All access is controlled

	Staff access to network devices is not restricted.	Staff access to network devices is restricted in some locations.	Staff access to network devices is restricted where appropriate.	and monitored with automated alerting.

End Users

Partners in Security

Indicator\Status	Basic	Developing	Adequate	Advanced
Awareness	Stakeholders generally lack expertise on and awareness of security issues.	Expertise: leaders often less capable than many Staffs in the use of productivity tools.	Expertise: Leaders demonstrate use of productivity tools.	Expertise: leaders demonstrate competency with productivity tools and knowledge of strategic and managerial IT topics, including security. Awareness: Users integrate essential security practices into everyday use of technology.
		Leaders may lack experience on strategic technology planning, including security issues.	Those charged with oversight of IT attend some trainings on strategic and managerial topics.	
		Awareness: Users are generally aware of organizational security concerns but lack specific knowledge on what to do.	Awareness: Users are generally aware of essential security guidelines and follow some security procedures.	
Training	Limited training opportunities do not include security topics.	Security is mentioned in IT training and professional development but training is not consistently tied to security policy.	Security integrated into IT training and professional development.	Security integrated into IT training and professional development. Leaders: receive regular user training plus training on strategic IT topics. End Users: Professional development, 0including security training, is tied to mission and security requirements. Community: Security is integrated into all outreach.
	End Users: training not required.	End Users: Not all are trained.	End Users: Most are trained.	
Communication	IT unit communicates to stakeholders only sporadically.	IT unit communicates to stakeholders a few times per year.	IT unit updates stakeholders on organizational security concerns on a monthly basis, or more frequently if significant vulnerabilities arise.	IT unit updates stake holders on organizational security concerns on a monthly basis, or more frequently if significant vulnerabilities arise. Leadership: receives regular updates on IT and security issues. End users: frequent messages issued on security concerns are disseminated using a variety of media. Community: receives regular publicity on IT or security issues.
	Leadership: receives periodic updates on IT and security issues.	Leadership: receives regular updates on IT and security issues.	Leadership: receives regular updates on IT and security issues.	
	End Users: receive only sporadic messages issued on security concerns.	End Users: receive occasional messages issued on security concerns.	End Users: frequent messages issued on security concerns are disseminated using a variety of media.	

Feedback	No organized feedback mechanisms exist.	Limited effort made to track stakeholder opinion and satisfaction. IT Unit relies on stakeholders to bring complaints and suggestions forward.	Help desk tracks problems and suggestions. Survey of user opinions may be performed every other year. All new IT initiatives including changes in security policy are reviewed by user groups.	Help desk tracks problems and suggestions and reports findings to management regularly. Survey of user opinions performed and published at established intervals. Users provide input to IT initiatives through organized means such as special interest groups or regularly scheduled meetings.
Summary: Community of Trust	IT unit has almost no capacity to monitor security. IT systems are extremely vulnerable to internal damage.	Increasing likelihood for security failures without clear policy or secure infrastructure may result in a climate of suspicion or confusion. Early adopters of new technology may be frustrated by apparent unresponsiveness of IT unit to meet their needs.	Decreasing likelihood for security failures the result of clear policy and significantly improved infrastructure reduces lingering suspicion and confusion. Early adopters of new technology learn to collaborate with IT unit to ensure security.	A secure network, with reliable infrastructure and transparent security policies, provides effective, mission-driven learning opportunities without the weight of surveillance.

Recommendation

Management needs to continue to move processes and procedures towards the right in almost every classification.

Appendix 2: NIST Cybersecurity Gap Assessment

The Framework focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization's risk management processes.

Framework Implementation Tiers ("Tiers") provide context on how an organization views cybersecurity risk and the processes in place to manage that risk. The Tiers range from Partial (Tier 1) to Adaptive (Tier 4) and describe an increasing degree of rigor and sophistication in cybersecurity risk management practices and the extent to which cybersecurity risk management is informed by business needs and is integrated into an organization's overall risk management practices.

Risk management considerations include many aspects of cybersecurity, including the degree to which privacy and civil liberties considerations are integrated into an organization's management of cybersecurity risk and potential risk responses. While organizations identified as Tier 1 (Partial) are encouraged to consider moving toward Tier 2 or greater, Tiers do not represent maturity levels. Progression to higher Tiers is encouraged when such a change would reduce cybersecurity risk and be cost effective.

Function	Category	Subcategory	Implementation Tier
IDENTIFY (ID) Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities. The activities in the Identify Function are foundational for effective use of the Framework. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs.	**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 business objectives and the organization's risk strategy.	**ID.AM-1**: Physical devices and systems within the organization are inventoried	**TIER 3: REPEATABLE**
		ID.AM-2: Software platforms and applications within the organization are inventoried	**TIER 3: REPEATABLE**

		ID.AM-3: Organizational communication and data flows are mapped	**TIER 2: RISK INFORMED**
		ID.AM-4: External information systems are catalogued	**TIER 1: PARTIAL**
		ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	**TIER 1: PARTIAL**
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	**TIER 1: PARTIAL**
	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	**TIER 3: REPEATABLE**

		ID.BE-2: The organization’s place in critical infrastructure and its industry sector is identified and communicated	**TIER 2: RISK INFORMED**
		ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	**TIER 3: REPEATABLE**
		ID.BE-4: Dependencies and critical functions for delivery of critical services are established	**TIER 2: RISK INFORMED**
		ID.BE-5: Resilience requirements to support delivery of critical services are established	**TIER 2: RISK INFORMED**
	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 information security policy is established	**TIER 2: RISK INFORMED**
		ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners	**TIER 2: RISK INFORMED**
		ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	**TIER 1: PARTIAL**

		ID.GV-4: Governance and risk management processes address cybersecurity risks	**TIER 1: PARTIAL**
	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	**TIER 1: PARTIAL**
		ID.RA-2: Threat and vulnerability information is received from information sharing forums and sources	**TIER 1: PARTIAL**
		ID.RA-3: Threats, both internal and external, are identified and documented	**TIER 1: PARTIAL**
		ID.RA-4: Potential business impacts and likelihoods are identified	**TIER 1: PARTIAL**

		ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	**TIER 1: PARTIAL**
		ID.RA-6: Risk responses are identified and prioritized	**TIER 1: PARTIAL**
	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	**TIER 1: PARTIAL**
		ID.RM-2: Organizational risk tolerance is determined and clearly expressed	**TIER 1: PARTIAL**
		ID.RM-3: The organization’s determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	**TIER 1: PARTIAL**
PROTECT (PR) Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services. The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event. Examples of outcome Categories within this Function include: Access Control; Awareness and Training; Data Security; Information Protection Processes and	**Access Control (PR.AC):** Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	**PR.AC-1:** Identities and credentials are managed for authorized devices and users	**TIER 3: REPEATABLE**
		PR.AC-2: Physical access to assets is managed and protected	**TIER 3: REPEATABLE**

Procedures; Maintenance; and Protective Technology.			
		PR.AC-3: Remote access is managed	**TIER 3: REPEATABLE**
		PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties	**TIER 3: REPEATABLE**
		PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate	**TIER 3: REPEATABLE**
	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.	**PR.AT-1:** All users are informed and trained	**TIER 2: RISK INFORMED**

		PR.AT-2: Privileged users understand roles & responsibilities	**TIER 3: REPEATABLE**
		PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities	**TIER 2: RISK INFORMED**
		PR.AT-4: Senior executives understand roles & responsibilities	**TIER 2: RISK INFORMED**
		PR.AT-5: Physical and information security personnel understand roles & responsibilities	**TIER 3: REPEATABLE**

	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	**TIER 3: REPEATABLE**
		PR.DS-2: Data-in-transit is protected	**TIER 2: RISK INFORMED**
		PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	**TIER 3: REPEATABLE**
		PR.DS-4: Adequate capacity to ensure availability is maintained	**TIER 4: ADAPTIVE**

		PR.DS-5: Protections against data leaks are implemented	**TIER 3: REPEATABLE**
		PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	**TIER 3: REPEATABLE**
		PR.DS-7: The development and testing environment(s) are separate from the production environment	**TIER 2: RISK INFORMED**
	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	**TIER 3: REPEATABLE**
		PR.IP-2: A System Development Life Cycle to manage systems is implemented	**TIER 3: REPEATABLE**

		PR.IP-3: Configuration change control processes are in place	**TIER 3: REPEATABLE**
		PR.IP-4: Backups of information are conducted, maintained, and tested periodically	**TIER 3: REPEATABLE**
		PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met	**TIER 3: REPEATABLE**
		PR.IP-6: Data is destroyed according to policy	**TIER 3: REPEATABLE**

		PR.IP-7: Protection processes are continuously improved	**TIER 3: REPEATABLE**
		PR.IP-8: Effectiveness of protection technologies is shared with appropriate parties	**TIER 2: RISK INFORMED**
		PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	**TIER 1: PARTIAL**
		PR.IP-10: Response and recovery plans are tested	**TIER 1: PARTIAL**
		PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	**TIER 2: RISK INFORMED**
		PR.IP-12: A vulnerability management plan is developed and implemented	**TIER 1: PARTIAL**
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.	**PR.MA-1:** Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools	**TIER 3: REPEATABLE**

		PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	**TIER 3: REPEATABLE**
	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	**TIER 2: RISK INFORMED**
		PR.PT-2: Removable media is protected and its use restricted according to policy	**TIER 1: PARTIAL**
		PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality	**TIER 3: REPEATABLE**

		PR.PT-4: Communications and control networks are protected	**TIER 3: REPEATABLE**
DETECT (DE) **Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event. The Detect Function enables timely discovery of cybersecurity events. Examples of outcome Categories within this Function include: Anomalies and Events; Security Continuous Monitoring; and Detection Processes.**	**Anomalies and Events (DE.AE):** Anomalous activity is detected in a timely manner 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	**TIER 1: PARTIAL**
		DE.AE-2: Detected events are analyzed to understand attack targets and methods	**TIER 2: RISK INFORMED**
		DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors	**TIER 1: PARTIAL**
		DE.AE-4: Impact of events is determined	**TIER 2: RISK INFORMED**
		DE.AE-5: Incident alert thresholds are established	**TIER 1: PARTIAL**

	Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	**DE.CM-1:** The network is monitored to detect potential cybersecurity events	**TIER 2: RISK INFORMED**
		DE.CM-2: The physical environment is monitored to detect potential cybersecurity events	**TIER 2: RISK INFORMED**
		DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	**TIER 1: PARTIAL**
		DE.CM-4: Malicious code is detected	**TIER 3: REPEATABLE**
		DE.CM-5: Unauthorized mobile code is detected	**N/A**
		DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	**TIER 2: RISK INFORMED**

		DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	**TIER 2: RISK INFORMED**
		DE.CM-8: Vulnerability scans are performed	**TIER 2: RISK INFORMED**
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.	**DE.DP-1:** Roles and responsibilities for detection are well defined to ensure accountability	**TIER 1: PARTIAL**
		DE.DP-2: Detection activities comply with all applicable requirements	**TIER 1: PARTIAL**
		DE.DP-3: Detection processes are tested	**TIER 1: PARTIAL**

		DE.DP-4: Event detection information is communicated to appropriate parties	**TIER 1: PARTIAL**
		DE.DP-5: Detection processes are continuously improved	**TIER 1: PARTIAL**
RESPOND (RS) **Develop and implement the appropriate activities to take action regarding a detected cybersecurity event. The Respond Function supports the ability to contain the impact of a potential cybersecurity event. Examples of outcome Categories within this Function include: Response Planning; Communications; Analysis; Mitigation; and Improvements.**	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.	**RS.RP-1:** Response plan is executed during or after an event	**TIER 2: RISK INFORMED**
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.	**RS.CO-1:** Personnel know their roles and order of operations when a response is needed	**TIER 2: RISK INFORMED**
		RS.CO-2: Events are reported consistent with established criteria	**TIER 2: RISK INFORMED**

		RS.CO-3: Information is shared consistent with response plans	**TIER 2: RISK INFORMED**
		RS.CO-4: Coordination with stakeholders occurs consistent with response plans	**TIER 2: RISK INFORMED**
		RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	**TIER 2: RISK INFORMED**
	Analysis (RS.AN): Analysis is conducted to ensure adequate response and support recovery activities.	**RS.AN-1:** Notifications from detection systems are investigated	**TIER 2: RISK INFORMED**
		RS.AN-2: The impact of the incident is understood	**TIER 2: RISK INFORMED**
		RS.AN-3: Forensics are performed	**TIER 2: RISK INFORMED**
		RS.AN-4: Incidents are categorized consistent with response plans	**TIER 2: RISK INFORMED**

	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.	**RS.MI-1:** Incidents are contained	**TIER 2: RISK INFORMED**
		RS.MI-2: Incidents are mitigated	**TIER 2: RISK INFORMED**
		RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks	**TIER 2: RISK INFORMED**
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	**RS.IM-1:** Response plans incorporate lessons learned	**TIER 2: RISK INFORMED**
		RS.IM-2: Response strategies are updated	**TIER 2: RISK INFORMED**
RECOVER (RC) **Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event. The Recover Function**	**Recovery Planning (RC.RP):** Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.	**RC.RP-1:** Recovery plan is executed during or after an event	**TIER 2: RISK INFORMED**

supports timely recovery to normal operations to reduce the impact from a cybersecurity event. Examples of outcome Categories within this Function include: Recovery Planning; Improvements; and Communications.	**Improvements (RC.IM):** Recovery planning and processes are improved by incorporating lessons learned into future activities.	**RC.IM-1:** Recovery plans incorporate lessons learned	**TIER 1: PARTIAL**
		RC.IM-2: Recovery strategies are updated	**TIER 1: PARTIAL**
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.	**RC.CO-1:** Public relations are managed	**TIER 3: REPEATABLE**
		RC.CO-2: Reputation after an event is repaired	**TIER 3: REPEATABLE**
		RC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teams	**TIER 3: REPEATABLE**