CYBER ALBERTA

Governance, Risk and Compliance

CONTROL FRAMEWORK

Executive Summary

The control framework described in this document is designed to establish a robust, sustainable, risk and security control framework that reduces risk, defines the security stance, and supports the organizational policy and directives.

Executive Support and authority (Governance) is required for the creation of all controls and control activities in the control framework. Governance is initially established through policy. The Control Policies establish Governance, define Executive intent, and provide Control Owners with direction for evaluation and monitoring of controls and the delegation of roles and responsibilities.

The controls in this framework are logically designed to address areas of IT risk that require secure, auditable, and sustainable control activities. These controls, and associated control activities, are required for IT operations that can introduce risk or increase risk potential due to either the complexity of the task, or the risk associated with the introduction of changes. For example, change management and patch management are areas that can introduce risk of a security breach, or result in unscheduled downtime if changes are unauthorized, untested, or unplanned.

The control framework achieves the following objectives:

1. Reduces IT risk through the integration of risk management practices with IT operations and Services.
2. Protects organizational information and data assets by integrating cybersecurity with all IT activities.
3. Establishes Governance over controls through:
    a. Executive support and authorization of Control policies that define controls and control activities.
    b. Executive authorization of IT standards that support controls and control activities.
    c. Identification and assignment of Control Owners for each Control, and Custodians for all control activities.
4. Continuous improvement through sustainability requiring regular reviews and reporting on effectiveness of control activities to Control Owners.

The framework will focus on the following controls: Risk Management, Security Management, Application Access, Change Management, Security Incident Handling and Response, Solution Acquisition and Development (DevSecOps), IT Disaster Recovery, Vulnerability Management, and Cybersecurity Awareness.

The controls are not developed in a silo. Each control will require involvement of Subject Matter Experts (SMEs) from across IT including the Custodians, Service Owners, and Cybersecurity experts. This ensures that policy, standards, process and procedures are developed by experienced individuals, iteratively, and with consensus. The Control Framework is also designed so that new controls can be inserted into the framework as required and new control activities can be added to individual controls with minimal impact.

Table of Contents

List of Figures

1. Introduction

The Cybersecurity Control Framework integrates Policy, Standards, Risk and Procedures into a single structure and provides the building blocks for establishing a risk and security management program across all organizational IT operations. This document introduces general computing controls and a comprehensive set of risk based controls designed to support the implementation of a cost-effective risk and security management program. The Control framework provides the structure for achieving compliance in a logical manner and documents appropriate levels of governance for all control activities.

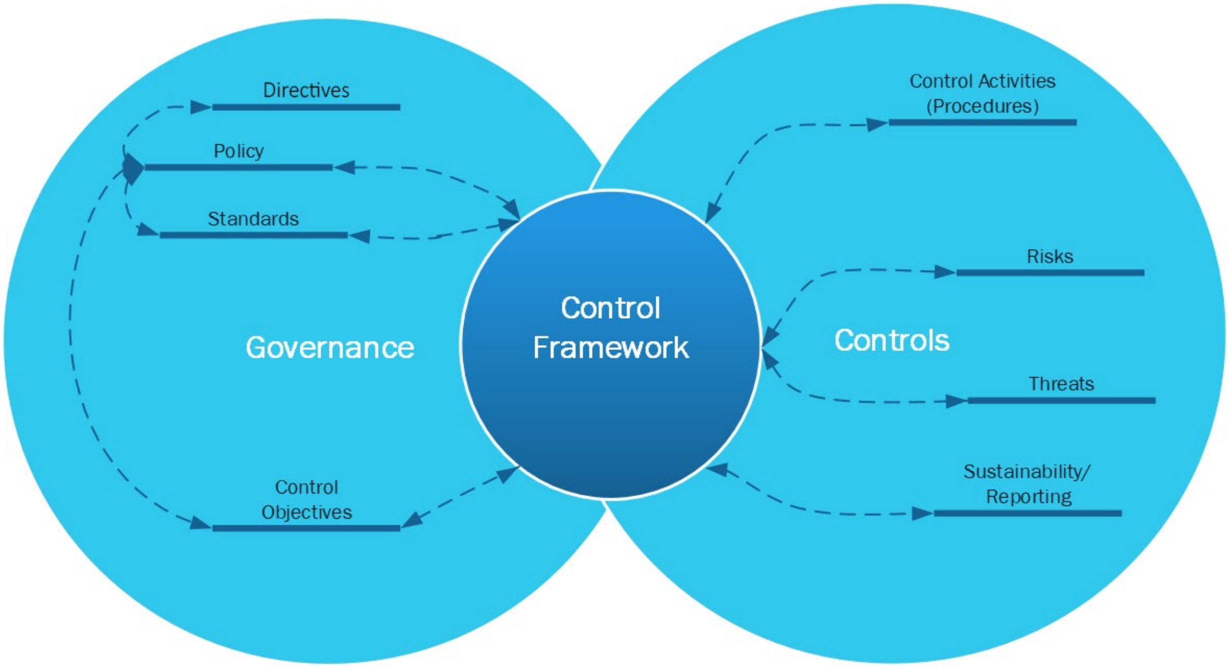

Figure 1 Control Framework

Policy provides the high level statements of management intent that are intended to provide direction and achieve desired outcomes of the business and executive. A set of directives should be created to establish the IT risk and security stance of an organization. Directives are what drive the need for, and creation of a control framework.

The *Control Policies* reinforce directives, establish governance, and ensure that risk and security is built into all IT controls. The policies are high level and define control objectives that address risk and security concerns associated with IT activities. Proactively addressing risk is the main reason for the control framework and to do this effectively means that governance, executive support and authorization for the controls must be established.

Control objectives are the statements describing the purpose of the control and ultimately the risk that is being addressed. It is the control objectives that define the requirements for specific technical standards, and the process and procedures to implement the standards.

This *Control Framework* aligns with the National Institute of Standards and Technology, Cybersecurity Framework (NIST CSF), which has five key functions; Identify, Protect, Detect, Respond and Recover. These five functions provide a comprehensive view of the lifecycle for managing cybersecurity, over time.

There are two or more of these NIST functions identified for each control activity. NIST defines the five key functions as:

- **Identify** – Develop an organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.
- **Protect** – Develop and implement appropriate safeguards to ensure delivery of services.
- **Detect** – Develop and implement the appropriate activities to identify the occurrence of a Cybersecurity event.
- **Respond** – Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.
- **Recover** – 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.

All controls must have the NIST identify function which establishes the following:

1. Governance for control activities.
2. Assessing and Managing Risk.
3. Understanding of organizational assets.
4. Cybersecurity roles and responsibilities.

RECOVER
IDENTIFY
FRAMEWORK
RESPOND
PROTECT
DETECT

Figure 2 NIST CSF Framework Functions

All controls require one or more of the *Protect, Detect, Respond and Recover* functions, depending on the control focus.

The controls are logically designed to address areas of risk requiring secure, repeatable, and sustainable control activities. These controls and associated control activities are needed for IT operations; Especially IT operational activities that introduce risk or increase risk potential due to either the complexity of the task, or the risk associated with the introduction of changes. For example, change management, patch management, and application access are all areas that introduce risk of a security breach, or downtime through unauthorized or unplanned change activities and therefore these are areas focused on by Risk and Security professionals, and Auditors.

2. Control Framework

The Control Framework is the hierarchical structure used to categorize and organize controls by areas of risk in IT Operations, Services, and tasks. The framework establishes due diligence and provides evidence of due care in addressing IT Risk and Cybersecurity.

1. The Control framework defines areas of risk and logically assigns controls that are designed to treat risk through documented control objectives, control activities, roles and responsibilities.
2. The Control Framework establishes governance[1] for control activities through executive authorized policy instruments. These documents provide executive support and authority for all control activities.
3. The Control Policy instruments provide the Executive with the mechanism used to establish intent and to direct[2] activities associated with IT operations.
4. Controls in the framework are designed to achieve cybersecurity compliance across all IT operations.
5. The Control framework helps to integrate security into all IT operations.
6. All controls are sustainable and provide the executive (Control Owners and Executive) a mechanism to monitor and evaluate control activity.

The Control Framework is described using the following column headings.

Control Title	Risk Statement	Control Identifier	Control #	Control Activities	IDENTIFY (ID)	PROTECT (PR)	DETECT (DE)	RESPOND(RE)	RECOVER (RC)

1. The Control title column provides the title for the control in the framework. For example, Change Management, Application Access, and Disaster Recovery.
2. The Risk statement defines the risk associated with the lack of policy, standards, process and procedures, and is what establishes the need for the control.
3. The Control number is for easy reference, which should identify the control and control activity.

[1] IT Governance helps an organization achieve desired behaviors and outcomes and stakeholder value.

[2] CoBIT clearly separates Governance and Management. Evaluate, Direct and Monitor (EDM) are the governance activities associated with Controls. Governance is not management.

4. Control activities provides a brief description of each of the control activities that will achieve control objectives.
5. The final 5 columns establish the relation between controls and the NIST Cybersecurity Framework (CSF). There are five NIST CSF functions and each control activity aligns with one or more of these functions.

3. IT Controls

An effective and auditable IT control consists of more than a policy or standard statement or a process and procedure. It requires that roles and responsibilities, as well as accountability, be defined at all levels of control activity. The control is designed to be sustainable by the people that implement it through process and procedures.

The control therefore has, and requires, governance and sustainability to be built into each control. This is accomplished by establishing roles and responsibilities for each control activity. The Owner is accountable for the control and regularly reports on control effectiveness. The Controller is responsible for process, and ensuring that the control process and procedures are effective and function as designed. The Custodian is responsible for creation and maintenance of procedures that implement the control and for performing reviews of their control activities.

Each Control in the framework consists of the following elements, read from left to right:

Risk	Control Objective	Control #	Control Activity	Control Description	Areas in Scope	Owner	Controller	Custodian

1. Risk - A Risk statement that describes what can go wrong if the control is not implemented.
2. One or more Control objectives that describe how risk will be treated.
3. Control number for easy reference.
4. Control activities are the individual control statements designed to address control requirements as defined in Policy. A control activity is ultimately, a procedure.
5. Control descriptions that elaborate on control objectives and activities and provide the Custodians with additional direction on control requirements.
6. Areas in Scope [3]are used for those controls that are applied with specific boundaries, such as a Department.
7. Responsibilities for Control Activities:
    a. Controller [4]

[3] For example, application access controls are built around Department applications and data that require authorization from the Information Controller for the application before access is implemented. Therefore the Department is provided as an area in scope so that the business owners are part of the control.

[4] Note that the Information Controller role is only required when business approval of access, or changes to access (or accessibility) to application and data is required.

b. Custodian [5]
c. Control Owner [6]

3.1 Control Activities

Control activities are the procedures used to accomplish control objectives. The procedures ensure that there are step by step instructions associated with the activity. These procedures, and adherence to them, is what implements the control.

The control activities are not created in a void but require Subject Matter Experts to be involved and provide input to the creation of the Controls. The policy, standards, process and procedures must all be in alignment and this requires SMEs to provide input on the tools and procedures currently in use, or are required, to implement control activities. The SMEs are also the ones that perform the activities on a day-to-day basis.

Control activities are developed, managed and maintained by the assigned Custodians for a particular IT task or service. Some examples of these activities are:

New user access provisioning - New user access requests for business applications must be approved by the business. The permissions associated with the requested account must meet business requirements, and are role based. The level of permissions assigned to each account must adhere to the principle of least privilege and need to know.

Change authorization - Changes to production networks, servers, applications, hardware and software are authorized prior to migration to production and must use documented change control process and procedures.

DR Testing - The networks, systems and applications that process store, transmit and receive Department information and data, require regular testing to ensure that the technology, programs, and services they rely on can be restored in the event of a disaster.

Cybersecurity awareness compliance - Provide regular and consistent reporting on Department compliance with cybersecurity awareness training.

4. Governance

Governance is an integral part of the Control framework and is built into all control activities. Governance, within this context, is demonstrated formal executive involvement and support for Controls and Control activities. The control policies assist in establishing governance and these policy instruments are further qualified by internal factors such as Policy, Directives and mandates.

[5] Information Custodians (Custodians) are the stewards for the IT applications, information/data, and the supporting IT infrastructure utilized by the business. Custodians provide IT operational support and administrative functions for the users and are responsible for their areas procedures.

[6] The Control Owner is accountable for the Control or a control activity within the control. The Control Owner ensures that reviews are done and issues resolved.

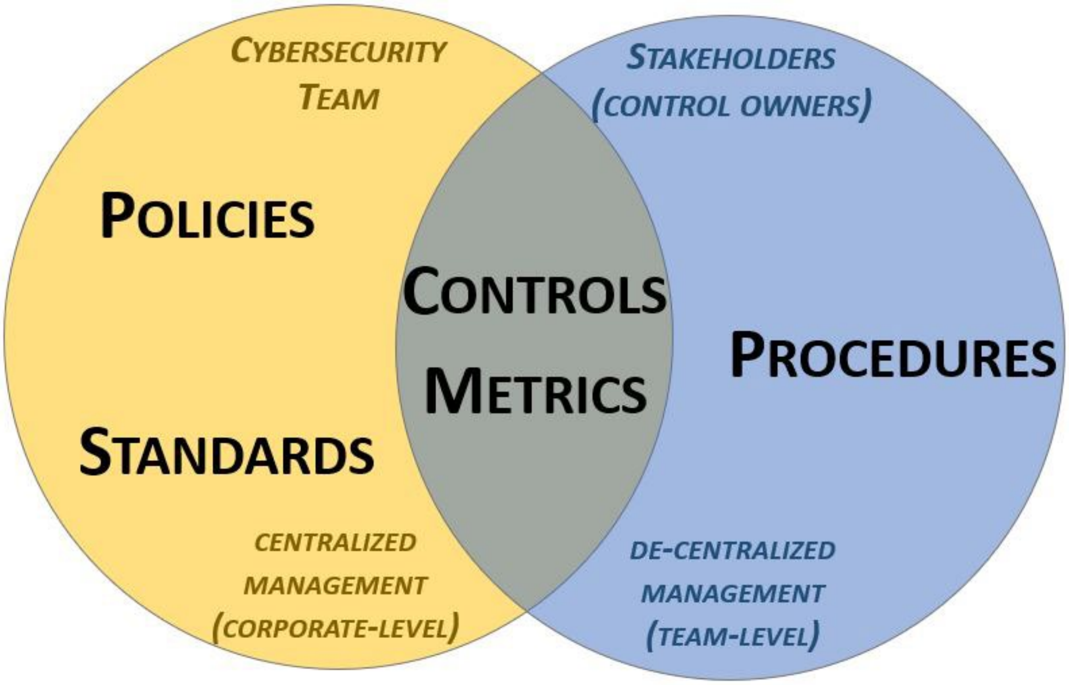
CYBERSECURITY TEAM
POLICIES
STANDARDS
CENTRALIZED MANAGEMENT (CORPORATE-LEVEL)
CONTROLS
METRICS
STAKEHOLDERS (CONTROL OWNERS)
PROCEDURES
DE-CENTRALIZED MANAGEMENT (TEAM-LEVEL)

Figure 3 Policy Standards Controls and Procedures (ref: Compliance Forge)

The diagram in figure 3 describes governance as it relates to Policy, standards, controls and procedures. Policies are documents that describe the expectations and the intent of Executive. Standards provide quantifiable requirements for cybersecurity and data protection, are responsibility of Cybersecurity, and are managed at a corporate level.

The procedures (also known as Control Activities) establish defined practices or steps that are performed to implement standards and satisfy control objectives. These are documented control activities, are de-centralized, and are therefore managed at the team level. Management at the procedural level is part of the governance structure and ensures that responsibility and accountability is migrated across the control framework. This is done by introduction of the Control Owner role. The control owner is accountable for the effectiveness of the process and procedures for their assigned control activities.

The metrics for measuring compliance sit at the intersection of the two Governance domains.

At the team level, the process and procedures are designed to address corporate mandates as defined in policy and standards. The effectiveness of the procedures and how well they address the requirements set forth in policy is reported to the Control Owner on a regular basis. Those reports provide control metrics that are used to show compliance and to address observations uncovered during periodic review of control activities.

The level of accountability established in the control depends on the assets, and the relation of the individuals involved with that asset. For example, those who do not own Department applications and data cannot be the risk owners for these Department information assets. However, a specific Department's staff may be the stewards[7] for the applications, the data, and the supporting infrastructure. That Department is therefore accountable for the supporting infrastructure and risks resulting from how that is managed, monitored and maintained.

Control Governance: Demonstrated formal executive involvement and support for Controls and Control activities.

1. Demonstrates executive awareness and support for the Control Framework and activities.
2. Authorizes policy instruments that establish intent and expectations for control activities.
3. Provides direction to IT management and staff on Executive's intent to address risk, and to enhance the security and safety of information and data.
4. Establishes responsibility and accountability for control activities at all levels of the organization.

[7] Stewardship is the careful and responsible management of something entrusted to one's care. (Merriam-Webster Dictionary)

5. Compliance

The metrics for measuring compliance are at the intersection of the two governance domains shown in Figure 3 Policy Standards Controls and Procedures. The intersection is where the responsible teams report on the effectiveness of their controls to the control owners.

Compliance can not be addressed tactically; one audit observation finding or recommendation at a time. The intent of the control framework is to define, document and communicate the organization's risk and security stance across all IT operations. Each control in the framework will address regulatory compliance, reduce risk to organizational assets, and ensure that risk and security management are built into all IT tasks. Past audit recommendations, findings, and observations should be included/considered in the control creation as part of a strategic response.

5.1 Sustainability

To achieve compliance with organizational directives requires a sustainability element to be built into each control. Sustainability is accomplished through periodic reviews. The periodic reviews ensures that the department and teams responsible for a control or control activity regularly reviews the effectiveness of the process and procedures that define the tasks associated with their control activities.

Periodic reviews will also ensure compliance with established policies, standards and provide sustainability for control activities. The purpose of the sustainability process is to establish a standard practice for conducting regularly scheduled reviews that evaluate the effectiveness of organizational controls and identify the changes or improvements required for existing policies, standards, or procedures. Each time the review is performed, progress on resolution of previously identified issues is updated and new issues are documented.

Each Control will require specific procedures for performing the review and a template. A sample template used for application access review is located here. The review process should be automated whenever possible so that reports required for the review are generated and sent for initiation of the review.

Controls should require regular reviews to be performed. This ensures that continuous improvement can be achieved and that accountable parties are informed of the status of issues before they become incidents or audit findings. Longer review cycles, such as an annual review, result in control problems being unreported and unaddressed for a year or more; achieving control maturity is hampered by the lack of reporting, tracking and treatment.

5.2 Control Automation

Control automation is important for control sustainability and achieving higher control maturity levels. Automation ensures that activity is time stamped and auditable. It takes the onus off organizational staff to initiate and develop reports and offloads some of the busy work required to manage, monitor and maintain controls and control activities.

Manual report generation and reviews are time consuming, especially when the control's maturity is low. Low maturity controls, at first implementation, require continuous review and improvement. The control effectiveness cannot wait on an annual audit cycle to be measured and addressed. This would be no different than tactically responding to audit observations. Most controls must be reviewed regularly.

Automation assists in compliance, and sustainability through:

1. Workflows that are designed for processes and procedures that were created for control activities.
2. Automation is used to request periodic reviews.
3. Automation includes generation of reports and templates required for reviews and ad hoc reporting requests.
4. Communication to Control Owners, Controllers and Custodians.

6. Control List

The following section provides the list of IT Controls. Each of these controls requires, a risk description, control objectives, and control activities that address risk with consideration for operational necessity, business needs, and directive. Each of the controls identified could apply to the organization's networks, servers, applications and services both on premise and in the cloud.

These particular controls were chosen because they are fundamental to achieving a baseline level of cybersecurity and IT risk management and each of these introduces the highest risk probability and impact, if they are not addressed.

1. **Risk Management** – Includes requirements for completion of risk instruments. This requires risk instruments that assess and classify information assets and assess security threats and risk. Risk reduction is the common thread throughout the control framework; if there is IT risk, then a control is required. Managing risk is central to all IT services and Operations.
2. **Security Management** – Integrates security management with all IT operations, standards, process, and procedures. The Security Management Control ensures that countermeasures are proactively implemented to protect the confidentiality, integrity and availability of business program applications and not just as a reaction to a security incident or privacy breach.
3. **Application Access Control** – Application access requests, including new user provisioning, user access changes, are authorized by the Information Controller and consistently managed across the organization. Terminations are performed in a timely manner. Regular reviews are mandatory.
4. **Change Management** – All changes to IT networks, systems, and applications are assessed for impact, tested for functionality, security tested, and authorized prior to migration to production.
5. **Security Incident Handling and Response** – Includes the requirements for monitoring, alerting, forensic investigation, intrusion analysis, log analysis, log retention, and incident response process and procedures. The detection and reaction times to incidents must be rapid. The response process and procedures must be predefined to ensure that roles and responsibilities, communication, and escalation fan-outs are defined, and documented.
6. **Solution Acquisition and Development** – Project Management for solution development use milestones/gates that include mandatory requirements for information security classification, vulnerability assessment, risk assessment, and treatment. Software development requirements for secure coding, compliance with architectural standards, portfolio and investment management, cloud and vendor procurement are defined. The control must consider the full Solution Delivery lifecycle (SDLC) of development and deployment of a solution on premise of in the cloud.
7. **Vulnerability Management** – Vulnerability assessment and remediation searches for weaknesses in technology, policy process and procedures with a combination of technical tools and activity reviews.
8. **IT Disaster Recovery** – Ensures that IT networks, systems, applications and the operations that support business critical and vital programs can be restored in a timely manner.

IT DR requires disaster recovery plans, technical recovery plans, communication fan-outs, and alignment with business continuity plans for the business.

9. **Cybersecurity Awareness** – Consists of online awareness training, formal training courses and certifications, and Cybersecurity Awareness month.

6.1 Potential controls

The following is a list of potential controls and/or supporting standards. These additional controls, in most cases, will only require a policy instrument (e.g standard) to ensure that IT operations, architects and developers have effective guidance. The determination on whether these will be standards or a full control will depend on how tightly coupled these potential controls can be made with the initial list and how easy it is to establish ownership.

For example, Solution Acquisition and Development relies on architecture and design standards, logging standards, cryptographic standards, SW development standards, software release management, patch management, DB and web application security etc. The standards provide consistent mandates for the secure development and implementation of networks, servers, and operating systems, on premise and in the cloud.

Another example, is system hardening standards that require process and procedures to ensure that server hardware is configured and implemented securely and consistently across the organization. The standard is also used to support other controls identified in the control list. It does this by providing additional mandates related to cybersecurity and risk management for server operating systems and this has impacts on vulnerability management, incident handling, change and patch management.

a. Network Security – Firewalls and perimeter security
b. System hardening UNIX/LINUX servers
c. System hardening Windows Servers
d. Physical and Environmental Security
e. DB security
f. Desktop security
g. Cloud security
h. Architecture and design standards
i. Cryptographic controls
j. Logging, alerting and Intrusion Analysis
k. Patch Management – N-1 revisions or N + 30
l. SW development – solution architecture on premise and cloud.
m. SW Deployment – Release Management
n. Password standard – Identity and Access Management standard.
o. DevSecOps standard.

6.2 Control Risks

The following table defines the risks associated with the controls selected in Section 6. The Risk identified below, is the risk assessed against a lack of controls. The risk level will tend to go from good to bad based on cycles. So the risk established in the table below is the risk associated with control failure.

In most of these control areas, the controls in place vary across departments. Some control activities will be well defined, documented and repeatable, while others will be ad hoc and based entirely on the knowledge and experience of individuals in the department.

Once the baseline controls are established the residual risk can be measured and Continuous improvement through sustainment activities achieved.

Control	Description	Risk
Risk Management	The Risk Management Control addresses the integration of risk management practices throughout the IT life cycle. This includes asset identification and Information security classification, Risk Governance, Threat Intelligence, and Vulnerability management – tracking and remediation. Risk is integrated throughout the control framework. If there is no risk a control/control activity is not required.	VH All IT activities have risks that arise from the introduction of changes; largely through maintenance activities. If these risks are not addressed they will result in the increased probability for a breach of confidentiality, data corruption, and/or loss of availability. Risk management is critical. The goal of the risk management control is to ensure that risk management practices are integrated across all IT activities, operations and services. Each control in the framework must therefore account for the risks associated with IT operations and services and ensure that a department's risk capacity is not exceeded.
Security Management	Integration of security management into all IT services, projects, and tasks and the control framework. Includes vulnerability management, incident handling and response, security standards, system and network hardening etc.	VH Cybersecurity is fundamental to the survival of any organization. The costs in time, effort, money, reputation, trust, and the publicity associated with breaches can have severe consequences and exceed the organization's risk capacity.

Control	Description	Risk
		Security management is critical. The intent of the Security Management control is to ensure that proactive cybersecurity practices and countermeasures are integral to all IT operations. Cybersecurity should not be an afterthought.
Application Access	Establishes control activities ensuring that access requests to applications and data are approved by the business and that the level of access provisioned is appropriate. Changes to access are similarly treated and require that previous levels of access are removed so that new access permissions can be applied without compromising the least privilege principle or need to know. Application access must also handle user access terminations in a timely manner.	H Increased risk of a breach of confidentiality or loss of integrity due to inconsistent provisioning of user access and permissions. Applications may provide processing and storage of Personally Identifiable Information (PII) and other sensitive data. Access to this information and data must be controlled or the risk of a breach of confidentiality or data corruption is increased. The identity and access management associated with that access is the first line of defense designed to protect organizational data.
Change Management	Change Management reviews, tests, and authorizes all significant and major changes prior to implementation/migration to production. This should include HW, FW, and SW changes. All changes must be tested (SIT, UAT & security), authorized, approved and have a back-out plan. Change management must also account for emergency changes.	H The introduction of untested and unauthorized Information technology, networks, systems, and software can result in unscheduled downtime and increase the risk of a breach of confidentiality, and data corruption. The probability of an impact to business systems is high and there are instances where changes made in production caused downtime to occur. This was usually due to inadequate testing or unauthorized activity.

Control	Description	Risk
Solution Acquisition and Development	A PM Framework is used as part of the software/solution acquisition and Development control. The framework ensures that milestones for advancing a solution's development to its next phase, whether on premise or in the cloud and regardless of the methodology used, is in place, authorized and includes cybersecurity, vulnerability testing (including penetration testing), and risk assessment. Security requirements must be defined at the earliest stages of the project (Non-Functional Requirements) so that the architecture and design accounts for the confidentiality, integrity, and availability (CIA) needs of the business.	VH Without a defined and documented Project Management framework that actively integrates security and risk requirements through architecture, design and development, IT projects will continue to introduce risk. The risks are associated with the architecture, design, development and introduction of new technology and solutions, as well as updates to existing solutions. This risk applies to applications and supporting infrastructure both on premise and in the cloud, where risk and cybersecurity were not an integral part of the Solution Development Lifecycle. The IT risks associated with solution acquisition and development increase the potential for a breach of confidentiality, data corruption, and loss of availability.
Security Incident Handling and Response	To ensure all security events and incidents are detected and responded to in a timely manner. All security incidents are high priority. The objective is to contain and eradicate the threat and restore business operations as soon as possible.	H Without the ability to effectively detect and react to security incidents unauthorized access to or corruption/loss of sensitive organizational data may not be detected and reaction to incidents may be slow. The severity of an incident should be established at the outset, in a consistent manner, using a single formula by all security practitioners. The level of protection provided by the incident response capability is equal to the detection and reaction time. Monitoring and alerting are critical components of the organization's response. Having a complete set of predefined responses to incident types speeds up reaction time.

Control	Description	Risk
Vulnerability Management	Reduce the risk of a breach of department applications and information assets through implementation of a complete vulnerability management program that focuses on risk reduction in the organization.	H Without a Vulnerability Management program, weaknesses in hardware, software, operating systems, architecture, design, policy, standards, processes, procedures will result in the increased probability of a security breach. The vulnerability management program must be expanded to include desktops, DBs, and cloud based infrastructure and include the need for static and dynamic code analysis during SW development and vulnerability assessment including penetration testing prior to deployment in production environments. The frequency of scanning will need to be increased. Remediation time frames are required to be defined for vulnerabilities. The frequency is to be based on the potential risk associated with the weakness.
IT Disaster Recovery	To ensure that IT networks, systems, applications and the operations that support business critical and vital programs can be restored in a timely manner.	H Without adequate disaster recovery policy, process, procedures, and plans it may not be possible to restore business operations to required levels in a timely manner. Require DR Plans, technical recovery plans, communication planning, DR exercises, and governance to be in place.
Cybersecurity Awareness	To ensure that employees, consultants, and contractors are informed and aware of the security stance of the organization and understand the importance of cyber security in their day to day activities.	H Without cyber security awareness training, employees, contractors and consultants can inadvertently increase risk to the organization through mishandling of information assets, and insecure usage of networks, systems and services. Requires development of training and mechanisms to ensure that training is kept current as technology, risk landscape and security threats change.

Note: VH = Very High, H = High. The initial controls are all Very High or High risk areas.

7. Control Framework Summary

The Control Framework is designed to integrate risk and security management into Information Technology (IT) operations. IT must take a risk based approach to operational activities, initiatives, projects and services. Information and data that is not secured is subject to increasing levels of risk that can exceed the risk appetite and capacity of the organization.

IT staff are the stewards for electronic information and data that the business collects, processes, stores, transmits and receives. Cybersecurity and IT personnel must therefore ensure that the information they work with is protected at all times in accordance with business requirements.

The Control Framework, including the elements that define it (directives, policy, and standards), do not, in and of themselves, implement the controls. The Controls are defined and documented in the framework however the control is not enacted until governance is established over all control activities. Governance establishes executive support and authority for the controls and defines control ownership, accountability and responsibility for each control activity.

The Control framework establishes requirements for documentary evidence that goes beyond written policy, standards, process and procedures. Policy instruments and the control framework could be considered as evidence of due care, because the controls provide direction related to IT operations. However, the framework does not show due diligence; that requires evidence that the controls are working as designed. Gathering evidence of control effectiveness is required to show both compliance, and due diligence.

The control framework includes reviews of control effectiveness and regular reporting of results. This ensures the controls are sustainable. Sustainability is the most important requirement for all controls; once they are implemented. When controls are implemented they will fail, usually within a year or two, if due diligence [8]is not followed. To avoid control failures, each control has a built in sustainability element that consists of periodic review process and procedures. The periodic review is a template used to review all control activities.

[8] Note that due diligence and due care must both be demonstrated for the control to be effective.

Appendix A – Control description

The following is a sample control for application access.

Application Access Control

Risk

1. Without documented user access process and procedures for new employees, there is an increased risk that staff will be provisioned with inappropriate access/permissions to Department applications and information assets.
2. Without user access change processes and procedures employees could retain access and permissions to application data that increase the potential for, and severity of, a breach.
3. Without a process in place to remove a terminated user's access in a timely manner, former staff and third parties could continue to have access to department applications including material financial systems.
4. Without an access review process in place, there is no effective way to verify that provisioning procedures are effective or to ensure sustainability of the control.

Objective

To ensure that all users are provisioned with appropriate levels of access based on their position and roles and that every access request is authorized by the Department. The permissions associated with access must be commensurate with job responsibilities and adhere to the principle of least privilege.

Application Access Control Activities and Descriptions

C-01.a The Application Access Control Policy, process and procedures must be formally documented. The Policy must align with organizational directives and reinforce Identity and Access Management Standards. Process and Procedures will be created by the Information Controllers and Custodians that enact the application access policy, and reinforce standards through step by step directions on how application users are provisioned, user access and permissions are changed, and when and how terminated users access is removed.

C-01.b New user access requests for business applications must be approved by the business. The permissions associated with the requested account must meet business requirements, and must be role based. The level of permissions assigned to each account should adhere to the principle of least privilege and need to know.

C-01.c The user change process for applications ensures that the user’s access to Department Applications and data is commensurate with their job requirements even after a change in employee responsibilities. Old access permissions are removed and new access permissions are applied.

C-01.d The application access termination process and procedures ensure that access to department applications is disabled in a timely manner.

C-01.e Authorized personnel (Controllers, and Custodians) must regularly monitor who has access to departmental information assets and determine if the level of access is appropriate and reasonable. Special attention is paid to accounts with elevated access and permissions or admin level access.

Governance

Control Ownership

Owner - The Control Owner is accountable for the effectiveness of the Control and all Control activities.

Information controller – The Information Controller is responsible for:

- Security of the application and information asset.
- User Access Control policy updates and the effectiveness of processes and procedures implemented for each control activity.
- All reviews are initiated by the Information Controller and the results are reported to the Control Owner. Different controls may require different levels of business involvement.

Custodian - is responsible for creation and maintenance of procedures that implement the control and for performing reviews of their control activities.

Appendix B – Barriers to Compliance

Compliance when looked at through a Governance lens makes clear that without executive awareness and support, any control framework will fail over time[9]. Time to failure will be approximately one to two years from control implementation. The failures usually result from lack of focus on control activities, in particular maintenance of the controls.

A control is not just a policy document, standard, process or procedure. It is not a checkbox in an audit column. Compliance requires control governance; executive awareness, and support for the Controls and Evaluation, Direction and Monitoring (EDM) which demonstrates effective Governance. If EDM is not established at the outset, the directives, policy and standards supporting them become pieces of paper and control activities are ad hoc.

A control is only enacted through assignment of roles, responsibilities for control activities and establishing accountability for achievement of control objectives. Governance is therefore critical to the success of the control program. Policy is the mechanism that leadership within the organization can provide direction to staff and clearly define requirements for compliance.

1. Unauthorized policy results in controls with no ownership, accountability, or enforcement ability.
2. Lack of standards results in multiple interpretations of what the organization's authorized technology, architecture, design, and operations entails.
3. Undocumented process and procedures that do not align with Control requirements, result in audit observations and findings and noncompliance with standards and policy.
4. Scope limitations where risk and cybersecurity management policy and standards are not integrated in all IT operations.
    i. Each of the controls, listed in the control list in Section 6.0, requires defined Control Owners, and Custodian(s). These key roles must be determined and each has responsibility for the effectiveness of their activities.
    ii. Creating policy and standards for these groups can result in governance failures if IT operations (e.g. change management, patch management, release management, solution acquisition and delivery), are considered to be outside the domain of cybersecurity.
5. Sustainability failures
    i. No control sustainability mechanism will result in control failures.
    ii. Lack of commitment to performance of self-reviews (time and effort).
    iii. Reporting of issues (fear of reprisal).
    iv. Lack of automation to assist with performance of reviews.

6. Policy documents, standards, process and procedures, when created in a silo, will result in control failures over time. Controls must integrate with each other to create a system. This requires a consistent approach using a common lexicon.

[9] Time to fail is based on controls

7. A steering committee for oversight of control creation and implementation, including Evaluation, Direction and Monitoring of control development is required. The steering committee ensures that expectations are met and escalations are managed.

Appendix C – Control Maturity

Compliance can be measured in a number of ways, including the use of various capability maturity models. These models vary and can have a different number of maturity levels, usually 4 or 5.

The NIST controls use four maturity levels based on industry expertise and experience:

Tier 1 – Partial – ineffective risk management methods. Unsystematic risk management processes, unreliable risk management programs, and unresponsive risk management participation.

Tier 2 – Risk informed – informal risk management methods. Unfinished risk management processes, underdeveloped risk management programs and incomplete risk management participation.

Tier 3 – Repeatable – structured risk management methods. Orderly risk management processes, robust task management programs and routine risk management participation.

Tier 4 – Adaptive – dynamic risk management processes, responsive risk management programs and interactive risk management participation.

Appendix D – Policy, Control Objective, Standard, Procedure and Guidelines

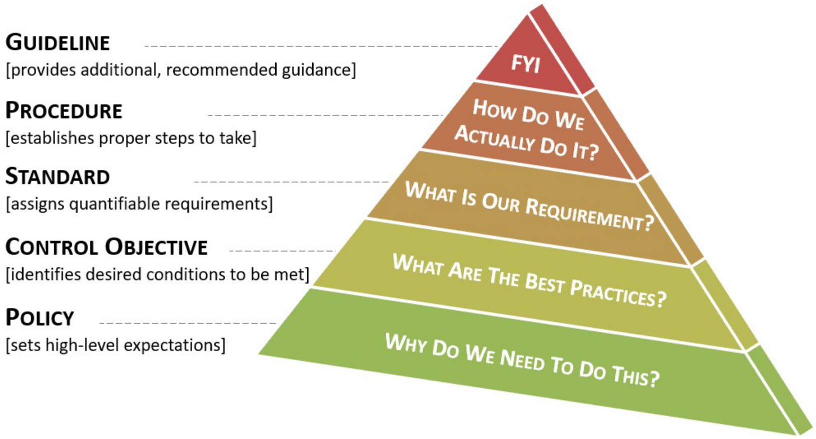
GUIDELINE
[provides additional, recommended guidance]
PROCEDURE
[establishes proper steps to take]
STANDARD
[assigns quantifiable requirements]
CONTROL OBJECTIVE
[identifies desired conditions to be met]
POLICY
[sets high-level expectations]
FYI
HOW DO WE ACTUALLY DO IT?
WHAT IS OUR REQUIREMENT?
WHAT ARE THE BEST PRACTICES?
WHY DO WE NEED TO DO THIS?

Figure 4 Policy to Guideline Pyramid (ref: Compliance Forge)

1. Policies are established by the organization’s corporate leadership which establishes “management’s intent” for cybersecurity and data protection requirements that are necessary to support the organization’s overall strategy;
2. Controls / Control Objectives identify the technical, administrative and physical protections that are generally tied to legislation, acts, regulation, and industry frameworks;
3. Standards provide organization-specific, quantifiable requirements for cybersecurity and data protection;
4. Procedures (also known as Control Activities) establish the defined practices or steps that are performed to meet to implement standards and satisfy controls / control objectives; and
5. Guidelines provide additional guidance and are considered for your Information (FYI).

Appendix E - Control Prioritization

Control development and implementation requires prioritization because we are treating risk and have finite resources for accomplishing the tasks associated with control creation. The creation and implementation of IT controls provides the means by which the organization will achieve compliance with directives. The controls are also the primary mechanism used to reduce risk associated with IT activities and services. Each control identifies associated risks, defines control objectives, and assigns control activities that effectively treat the risk. The control activities[10] provide guidance which must be implemented within process and procedures.

There are various activities within IT Operations that are major sources of risk to business programs and can result in downtime, data corruption or breach of confidentiality. These IT operations and services require documented, effective, consistent process and procedures to ensure that risk is addressed and Information security is a primary consideration.

A risk based approach to establishing priority will ensure that risk reduction occurs where it is most needed at the outset and that risk treatment is not based on a tactical response to an audit observation. An audit observation is addressed during control development, not because of it.

[10] Control activities and procedures are synonymous except in the context of the control framework a Custodian must be assigned and accountable for the procedures and ensure they are sustained.

Appendix F – Periodic Review Template - Application[11]

SECTION A		
Application Name:		
Information Owner:		
Information Controller:		
Information Custodian:		
Date of Review *(d/m/y)*:	d/m/y	
Review Period *(d/m/y)*:	d/m/y – d/m/y	
Application Access Self Review Results	**Issues?** **Y/N**	**Substantive/ Material?** **Y/N**
	□	□

Instructions for Self Review Completion

1. In Section A, fill in each line with the appropriate names, review dates, and whether or not an issue was identified.
2. In Section B, identify whether or not the specified report was reviewed. For those reports that were not reviewed, you must explain why it was not reviewed in the Comments section. For each report that was reviewed, you must indicate whether any issues were identified (*NB:* More Issue details can and should be detailed in Section C). The Reviewer must sign off (initial) each line item for verification. ***Note that the Controller and Custodian are encouraged to modify this section of the review log so that it aligns with their documented processes and procedures for performing the review.***
3. In Section C, for those reports that had an issue or issues identified, you must complete one line item for each issue. Issues should be numbered using the format of 1.1, 1.2, 2.1, 2.2, etc., where the first digit represents the report number from Section B and the decimal digit represents the issue number identified in that report. Fill in the details completely, providing a reasonable description of the issue and identifying when it occurred and whether it should be considered as serious. Assign the issue to the appropriate group and continue to monitor its status through to final resolution. Status should be tracked on this log, so that for each review, you are able to provide a reasonable update. Once the issue has been fully resolved, change the status to Completed (in some cases, it may be changed to Deferred or Cancelled; however a reasonable explanation must be provided in the Comments section should either of these statuses be used). Fill in the Date Closed section if the issue has been Completed or Cancelled (but not if it is Deferred) and have the Control Owner sign off on the log. Add more rows to the table if required. Return the completed form to the Controller who will have it reviewed and signed off by the Control Owner. The Information Controller retains a copy for audit purposes. ***Note that for the purpose of executive awareness, additional signatures can be added to section C as required by the business, however it must be signed by the Information Controller.***
4. Section D is filled out by the Information Owner. Comments are optional. ***Signatures in this section signifies that the Information Owner is aware of the status of this review and has initiated/authorized required remediation activities.***

SECTION B							
		Reviewed?		**Issue(s) Identified**			**Initials**
Report #	**Review Item**	**Yes**	**No**	**Yes**	**No**	**Comments**	**Custodian**
1	New User Report	□	□	□	□	<Review list of new users over the last quarter to ensure they were provisioned with appropriate access>	
2	Roles Granted to Users Report	□	□	□	□	<Review permissions applied to roles and whether they are appropriate. Ensure that separation of duties is maintained.	
3	Terminated Users Report	□	□	□	□	<Terminated users were removed in a timely manner. Users that retained access should be identified and disabled/removed>	
4	Application Changes Report	□	□	□	□	<Ensure access changes involve removal of previous level of access>	
5	Dormant Accounts Report	□	□	□	□	<Investigate accounts that have not been used over the last quarter>	
6	Role Based Access Control Matrix Review	□	□	□	□	<Review RBAC matrix – exists, is current, requires updates?>	

[11] Note that this template will be replaced in the future with a form that is standardized for all controls and allows for the reporting section to be easily modified.

SECTION C						
Item # *(ie 1.1, 2.1)*	**Finding Description**	**Event Date** *(d/m/y)*	**Material Event?** *(Y/N)*	**Assigned To**	**Status** *(In Progress, Deferred, Cancelled, Completed)*	**Comments**
		d/m/y				
		d/m/y				
		d/m/y				
		d/m/y				
		d/m/y				

SECTION C Signatures		
Title (Must include Information Controller Signature)	**Date** **(d/m/y)**	**Signature**

SECTION D			
Information Owner	**Date** **(d/m/y)**	**Comments**	**Signature**

Terms

Information Custodian – is the steward for the application and information assets that they support. The Custodian will only provision access when authorized by the business.

Information Controller – is responsible for the overall health and effectiveness of the controls used to secure the Application on behalf of the Information Owner.

Information Owner – The Information owner is an ADM or E-Team level executive responsible for the business area that is utilizing the application. The owner must be someone within the organization that is authorized to accept risk.

Control Deficiency – is a weakness, or failure of a control sometimes as a result of poor design, or execution, or failures of processes in support of the control. Control deficiencies may be discovered within control environments, risk assessment, control activities, information and communication, and monitoring.

Significant deficiency – is a control deficiency where a) the magnitude of misstatement that occurred or could occur is high, b) the likelihood of misstatement is high, c) size and complexity of the organization, organizational structure, and characteristics of ownership increase the likelihood or probability. A significant deficiency therefore could be related to lack of proper segregation of duties and responsibilities (design within the internal control) or lack of timely preparation of bank reconciliations, (execution within the internal control).

Material weakness - A material weakness is a significant deficiency, or combination of significant deficiencies, that results in more than a remote likelihood that a material misstatement of the financial statements will not be prevented or detected.