Thromde IT Controls
Dzongkhag Thromdes (TT, PT, GT and SJT)

Municipal Finance and Management Component
Bhutan Second Urban Development Project (BUDP-2)

Table of Contents

Conventions Used

Following terms are used in certain sections of this document. The terms should be interpreted as follows:

Mandatory – Those controls categorized as mandatory should be enforced within one year of adoption of this IT controls. These are the controls that are derived from existing practices and those that do not require substantial investment to have required solution to comply.

Recommended – These controls should be enforced within three years of the adoption of this control document. Deployment of solutions to ensure compliance would require investments to be made.

1. Executive Summary

Organizations should have internal controls in effect which provide reasonable assurance regarding the reliability of information and records, effectiveness and efficiency of operations, proper execution of managements' objectives and compliance with laws and regulations. Segregation of duties and safeguarding controls over resources and assets and all forms of information processing are necessary for proper internal control.

Segregation of duties is the concept of have different stakeholders do different task within the organization. It provides the foundation of good internal control by assuring that no one individual has the capability to perpetuate and conceal errors or irregularities in the normal course of their authorized duties.

Segregation of duties is achieved within information technology equipment, components, networks, information systems and database systems by appropriate assignment of security profiles that define the data the users can access and the functions that they can perform. Access must be restricted to the minimum required for the user to perform their job function. Access right must be periodically reviewed and approved by management.

COSO defines internal controls as: "A process, effected by an organization's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

- Effectiveness and efficiency of operations
- Reliability of financial reporting
- Compliance with applicable laws and regulations"

IT controls encompass those processes that provide assurances for information and information services and help mitigate the risks associated with an organization's use of technology.

Thromde Information Technology Controls describe the knowledge needed by users of IT systems, executives, IT professionals, and internal auditors to address technology control issues and their impact on business. Other professionals may find the guidance useful and relevant.

Information is a key resource for all organizations, and from the time that information is created to the moment that it is destroyed, technology plays a significant role. Information technology is increasingly advanced and has become pervasive in organizations and in social, public and business environment. As a result, organizations and executives strive to:

- Maintain high quality information to support decision making
- Generate business value from IT-enabled investments, i.e. achieve strategic goals and realize business benefits through effective and innovative use of IT
- Achieve operational excellence through the reliable and efficient use of technology
- Maintain IT related risk at an acceptable level
- Optimize the cost of IT services and technology
- Comply with relevant laws, regulations, contractual agreements and policies

Organizations have recognized that the board and executive need to embrace IT like any other significant activities. It is important that IT is included within the governance and management approach.

IT is an integral part of all processes that enable businesses and government agencies to accomplish their missions and objectives. IT facilitates local and global communications and fosters external cooperation. IT controls have two significant components: automation of business controls and control of IT. They support business management and governance, and they provide general and technical controls over the policies, processes, systems and people that comprise IT infrastructure. IT controls support the concept of "defense in depth" so a single weakness does not always result in a single point of failure.

IT control assurance addresses the ability of controls to protect the organization against the most important threats and provides evidence that remaining risks are unlikely to harm the organization and its stakeholders significantly.

2. Understanding IT Controls

IT controls provide for assurance related to reliability of information and information services. IT controls help mitigate the risk associated with an organization's use of technology. The range from organization policies to their physical implementation within coded instructions; from physical access protection through the ability to trance action and transactions to responsible individuals; and from automatic edits to reasonability analysis for data.

To adequately understand IT controls, it is essential to remember the following key concepts:

a. Assurance must be provided by the IT controls within the system of internal controls. This assurance must be continuous and provide a reliable and continuous trail of evidence.
b. The auditor's assurance is an independent and objective assessment of the first assurance. Auditor assurance is based on understanding, examining, and assessing the key controls related to the risks they manage, and performing sufficient testing to ensure the controls are designed appropriately and functioning effectively and continuously.

3. Importance of IT Controls

Many issues drive the need for IT controls, ranging from the need to control costs and remain competitive through the need for compliance with internal and external governance. IT controls promote reliability and efficiency and allow the organization to adapt changing risk environment. Any control that mitigates or detects fraud or cyber attacks enhances the organization's resiliency because it helps the organization uncover the risk and manage its impact. Resiliency is a result of a strong system of internal controls because a well-controlled organization has the ability to manage challenges or disruptions seamlessly.

Key indicators of effective IT controls include:

a. The ability to execute and plan new work such as IT infrastructure upgrades required to support new products and services
b. Development projects that are delivered on time and within budget, resulting on cost-effective and better product and service offerings
c. Ability to allocate resources predictability
d. Consistent availability and reliability of information and IT services across the organization and for customers, business partners, and other external interfaces
e. Clear communication to management of key indicators of effective controls
f. The ability to protect against new vulnerability and threats and to recover from any disruption of IT services quickly and effectively
g. Heightened security awareness on the part of the users and a security-conscious culture throughout the organization.

4. Control Classification

General Controls – General controls, also referred to as Infrastructure Controls, apply to all system components, processes, and data for a given organization or systems environment. General controls include, but not limited to: information security policy, administration, access, and authentication; separation of key IT functions; management of systems acquisition and implementation; change management; backup, recovery; and business continuity.

Application Controls – Application controls pertain to the scope of individual business processes or application systems. They include such controls as data edits, separation of business functions (e.g. transaction initiation versus authorization), balancing of processing totals, transaction logging and error reporting. The function of a control is highly relevant to the assessment of its design and effectiveness.

Preventive Controls – Preventive controls prevent errors, omissions, or security incidents from occurring. Examples include simple data-entry edits that block alphabetic characters from being entered into numeric fields, access controls that protect sensitive data or system resources from unauthorized people, and complex and dynamic technical controls such as antivirus software, firewalls, and intrusion prevention systems.

Detective Controls – Detective controls detect errors or incidents that elude preventive controls. For example, a detective control may identify account numbers of inactive accounts or accounts that have been flagged for monitoring of suspicious activities. Detective controls can also include monitoring and analysis to uncover activities or events that exceed authorization limits or violate known patterns in data that may indicate improper manipulation. For sensitive electronic communications, detective controls can indicate that a message has been corrupted or the sender's secure identification cannot be authenticated.

Corrective Controls – Corrective controls correct errors, omissions, or incidents once they have been detected. The corrections vary from simple correction if data entry errors, to identifying and removing unauthorized users or software from systems or networks, to recovery from incidents,

disruptions or disasters. The corrective processes are also subject to preventive and detective controls because they represent another opportunity for errors, omissions or falsification.

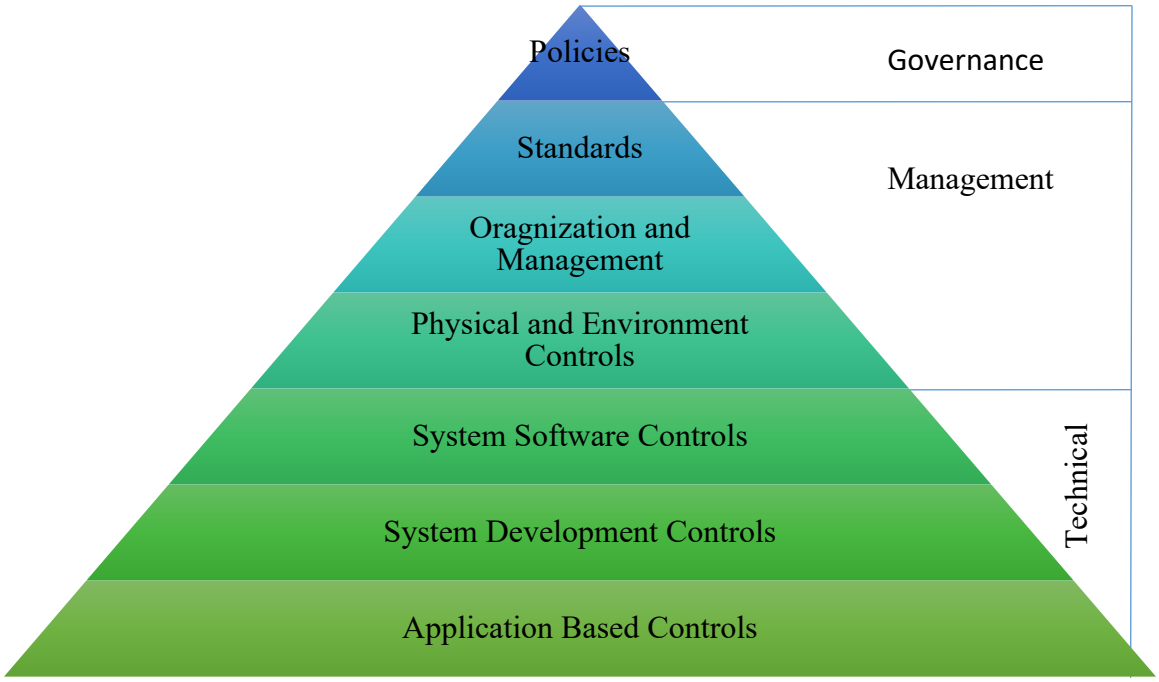
Governance Controls – IT controls at governance level involves ensuring that effective information management and security principles, policies, and processes are in place and performance and compliance metrics demonstrate ongoing support for the framework. Governance Controls are those mandated by, and controlled by the organization's executive management.

Management Controls – Management responsibility for internal controls typically involves reaching into all areas of the organization with special attention to critical assets, sensitive information and operational functions. Management must ensure the IT controls needed to achieve the organization's established objectives are applied and ensure reliable and continuous processing. These controls are deployed as a result of deliberate actions by management to:

- Recognize risks to the organization, its processes, and assets
- Enact mechanisms and processes to mitigate and manage risks (protect, monitor, and measure results)

Technical Control – Technical controls form the foundation that ensure the reliability of virtually every other control in the organization. For instance, by protecting against unauthorized access and intrusion, the controls provide the basis for reliance on the integrity of information – including evidence of all changes and their authenticity. These controls are specific to the technologies in use within the organization's IT infrastructures.

5. Coverage of IT Controls



5.1. Policies

Thromde is required to define aims and objectives through strategic plans and policy statements. Without clear statements of policy and standards for direction, Thromde can become disoriented and perform ineffectively. Because technology is vital to the operations of Thromde, clear policy statements regarding all aspects of IT should be devised and approved by management and endorsed by the Thromde Tshogdu, and communicated to all staff. Considering the size of Thromdes, a single IT policy statement will suffice.

Typically, IT policy statement should include, but not limited to, the following:

a. A general policy in the level of security and privacy throughout the Thromde. The policy should be consistent with all relevant national legislation and should specify the level of control and security required depending on the sensitivity of the system and data processed
b. A statement on the classification of information and the rights of access at each level. The policy should also define any limitations on the use of the information by those approved for access
c. A definition of the concepts of data and systems ownership, as well as the authority necessary to originate / enter, modify, or delete information.
d. A general policy statement that defines the extent to which users can use available technologies to create user specific applications
e. Personnel policies that define and enforce conditions for staff in sensitive areas. This includes the positive vetting of new staff prior to joining Thromde, and having employees sign agreements accepting responsibility for the required levels of control, security, and confidentiality. The policy would also detail related disciplinary procedures.
f. Definitions of overall business continuity planning requirements. These policies should ensure that all aspects of the business are considered in the event of a disruption or disaster

5.2. Standards

Standards exist to support the requirements of policies. They are intended to define ways of working that achieve the required objectives of Thromde. Adopting and enforcing standards also promotes efficiency because staff are not required to reinvent the wheel every time a new technology solution is purchased and deployed. Standards also enable the organization to maintain the whole IT operating environment more efficiently. Set of standards expected in the Thromdes include, but not limited to, the following:

a. System Development Processes – When Thromde develop applications internally, standards apply to the processes for design, development, testing, implementation, and maintenance of the systems. When Thromde outsource development and implementation of systems, the project management team from Thromde should ensure that technology partners / vendors apply standards consistent with the Standards adopted by the Thromde.

b. Systems Software Configuration – Because systems software provides a large element of control in the IT environment, standards related to secure systems configuration needs to be in place. The way system software like Operating System, networking software, and database management systems are configured can either enhance security or introduce weakness that can be exploited.
c. Application Controls – All applications which support operational activities need to comply with controls that enhance the information security. Standards are necessary for all applications Thromde use (developed in-house or procured through external vendor) that define the types of controls that must be present across the whole range of operational activities, as well as specific controls that should apply to sensitive processes and information.
d. Data Structures – Having consistent data definitions across the full range of software applications ensures disparate system can access data seamlessly and security controls for private and other sensitive data can be applied uniformly.
e. Documentation – Standards should specify the minimum level of documentation required for each IT component or class of IT asset, processes, and data.

Standards should be written in clear and understandable language. After approval from the management the standards should be made available to all who are supposed to implement / comply / assess the compliance with standards.

5.3. Organization and Management

Organization and management play major role in the whole systems of IT controls, as it does with every aspect of an organization's operations. An appropriate organization structure allows lines of reporting and responsibility to be defined and effective controls systems to be implemented.

6. Separation of Duties

Separation of duties is a vital element of any control framework. Thromde should not allow responsibility for all aspect of data to rest upon one individual or division. The functions of initiating, authorizing, inputting, processing, and checking data should be separated to ensure no individual can both create and error, omission, or irregularity and authorize it and/ or obscure the evidence. Separation of duties controls for application systems are provided by getting access privileges only in accordance with job requirements for processing functions and accessing sensitive information.

The separation of duties should be at users' level through implementation of roles and permission to access the systems as well as from system implementation aspects as development duties and operational duties.

System access level duties are segregated as system administrators, transaction initiators, transaction approvers, collection, executive report viewers. Duties in management information systems are implemented by having provisions to manage system access control by the system administrator. Permission on workflow level and data manipulation level (entry, edit, view provisions).

System Implementation level separation of duties as system development and operations where operations duties include responsibilities to ensure production systems are available to users as expected and the development duties include activities in the system development lifecycle. The system operation team members are restricted from accessing or modifying production programs, systems or data. The system development team will have very little dealing with the production system.

7. Financial Controls

Because Thromde is making considerable investment in IT, budgetary and other financial controls are necessary to ensure the technology yields the protected return on investment or proposed savings or expected benefits. Management process should be in place to collect, analyze and report related information.

8. IT Roles and Responsibilities

Many different roles have emerged for positions with the organization with management of IT responsibilities and ownership. Each position within the governance, management, operations and technical levels should have a clear description of its roles, responsibilities, and ownership for IT resources to ensure accountability for specific issues.

9. IT Control Implementation

IT controls are selected and implemented in the basis of the risks they are designed to manage. As risks are identified, suitable risk responses are determined ranging from doing nothing and accepting the risk as cost of doing business to applying a wide range of specific controls, including insurance.

10. Monitoring and Techniques

The implementation of a formal control framework facilitates the process of identifying and assessing the IT controls necessary to address specific risks. A control framework is a structured way of categorizing controls to ensure the whole spectrum of control is covered adequately. The control framework should apply to, and be used by, the whole organization – not just IT Office or internal auditing.

11. IT Control Assessment

Assessing IT controls is a continuous process. Business processes are changing constantly as technology continues to evolve. Threats emerge as new vulnerabilities are discovered. Audit methods improve as auditors adopt an approach where IT control issues in support of the business objectives are one of the top agendas.

Management provides IT control metrics and reporting. Auditors attest to their validity and opine on their value. The auditors should liaise with management at all levels to agree on the validity and effectiveness of the metrics and assurances for reporting.

12. Control Guidelines

12.1. Disaster Recovery

A well written Business Continuity Plan is required to ensure that critical data will be processed in the event of interruption of computer processing capability. The plan must be updated and tested annually or when significant modifications to computer hardware, software or application systems occur. One copy of the Business Continuity Plan should be retained offsite.

12.2. Backup Processing

All computer application programs and operating system software must be backed up on a periodic basis after modification. Applications system data and configuration files must be backed up on a periodic basis with adequate testing and verification for easy restoration of the data during failures of systems. The backup media must be periodically tested to ensure restoration will occur accurately. A copy of the backup data must be retained offsite.

12.3. Physical Security

The ICT systems and the associated telecommunications equipment must be adequately protected from environmental damage including, but not limited to, fire, water and physical damage by individuals. In additional, the ICT components must be protected from unauthorized access, terminals must be inoperable when not used by authorized employees, and the terminals used to enter sensitive commands / data must not be kept where unauthorized individuals may view the contents of the video display terminals.

a. Access to server rooms and IT equipment rooms should be restricted to only those whose job responsibilities require they maintain the equipment or infrastructure of room
b. Signs should be placed at the entrance to server rooms and IT equipment rooms, warning that access is restricted to authorized personnel and prohibiting food, drink and smoking
c. Server rooms and IT equipment rooms should not double as office space or storage space or any other shared purpose
d. Doors to server rooms and IT equipment rooms should be fireproof and secured with deadbolt type locks that cannot be easily picked
e. Access to server rooms and IT equipment rooms should be controlled by a strong authentication method, such as an electronic combination lock, a badge reader, a fingerprint reader or other biometric scanning device. Lock combinations should be changed on regular basis

f. Keys to server room doors – both electronic and traditional – should be numbered and the whereabouts of each copy logged. Traditional keys should be marked "Do not duplicate" and electronic keys should be copy protected
g. Server rooms and IT equipment rooms should not have windows through which a person could gain access. If there are windows, they should be shatterproof, and / or protected by metal grates to prevent access if broken
h. Server rooms and IT equipment rooms should be monitored by CCTV or IP cameras 24x7
i. Server rooms and IT equipment rooms should have redundant power sources, such as a generator, to power electronic locks and authentication system in case of power failure or outage
j. A system for securely disposing of unwanted discs, tapes, cards, hard drives, printed paper, and anything else they could contain confidential information should be implemented.

12.4. Logical Security

Effective Logical Security prohibits unauthorized access and restricts the ICT resources each authorized user may utilize. Access to organizational data, ICT resources and processes must be controlled through implementation of access control privileges (ACP) and user identification using user IDs and password. User IDs must be unique identifiers assigned to each authorized user. The user ID of a user should remain constant. Passwords are confidential keywords associated with the user ID to provide verification of the user's identity. Each user must have a unique user ID and password which must not be shared. Passwords must meet the following criteria:

a. Passwords should be changed frequently to prevent misuse
b. Passwords should be a minimum of eight (8) characters in length
c. Passwords should be a combination of alphabetic, numeric and special character. Minimum of one alphabetic character should be in upper case, minimum of one numeric character and minimum of one special character.
d. Password may not be the same for a user ID as the last three (3) passwords used used by the user ID
e. Individuals should assign their own passwords
f. Passwords should be encrypted while stored in database / any other storage
g. Reporting of user access rights to system functional capabilities and information, as well as reporting of security definitions such as configuration parameters, workflow approval hierarchy, thresholds, and override capabilities should be available to, and easily understood by, Thromde management and auditors during the course of a regular audit. These security definitions and user access right must enforce adequate segregation of duties for any IT component used in the Thromde.
h. Users other than System Administrators and Security Administrators should be prevented from accessing sensitive commands of the IT components
i. Developers of any system should not have update access to production instance of the Thromde information management systems
j. Users should not be allowed to be active on multiple terminals at the same time with the same user ID

k. User ID should be deactivating after three unsuccessful attempts to sign on to the systems. Same should be applied to other IT components that require login for operations
l. For inactive terminals, the user must be automatically prevented from access the computer after 15 minutes of no activity until the user's password is entered
m. Users should be prevented from modifying or deleting operating system and computer program files. Administrative right should be provided to users other than administrators of the system
n. Users should be prevented from updating data except through authorized transactions and processes within the information systems
o. User access rights must be eliminated or revised upon termination of employment and transfers of employee responsibility
p. Systems should be hosted on Secure Socket Layer (SSL) or Transport Layer Security (TLS) enabled hosting infrastructure
q. Hosting premise should have proper deployment DMZ and related data center security implementation

12.5. Audit trails

All the MIS application systems should maintain electronic audit trails sufficient to trace all transactions from the original source of entry into the system, through all system processing, though various levels of summarizations, and to the results produced by the system. The audit trails should also maintain sufficient information to trace all transactions from the final results produced by the system, through all system processing and summarizations and to the original source of entry into the system. Audit trails should be protected from modification and deletion

12.6. Input controls

All MIS applications should provide input edits and controls to ensure that information entered into the system is accurate, that all appropriate information is entered into the system, and that information is entered into the systems only once. All information entered into the systems should be authorized through effective manual or system-based workflow.

Transaction dates should be based upon system generated dates which cannot ne modified by the user. If necessary, the system may provide an additional effective date / actual activity date of the transaction that is user controlled. However, controls must exist to ensure effective dating does not result in data integrity, reporting, and reconcilement problems.

12.7. Output Controls

All Thromde MIS Systems should incorporate features that ensure all of enterprise data is reported accurately and completely. Procedures must also exist to ensure that only authorized individuals have access to output information.

All receipts or payment generated by the systems should include unique document identification numbers either pre-printed on the form or printed on the form by the application system. If the

numbers are printed on the forms by the application system, adequate security should be implemented to prevent unauthorized modification of the number sequence.

Preprinted receipt and check stock should not include pre-printed signatures, should be securely stored, and usage must be logged and reconciled.

If reports can be generated through selection of various criteria such as organizational units, account codes, transaction codes, status codes, date, etc. the report generation interface should contain sufficient information regarding the selection criteria to allow users to understand what information is being reported and recreate the report. All output reports should clearly indicate the effective dates of the information in addition to the report generation date. Output reports should have appropriate subtotals (wherever applicable) to allow reconcilement to other reports and to external documentation.

12.8. Interface Controls

Information generated in one MIS application system and transferred to another MIS application system should be accurate and complete.

12.9. Inventory of Authorized and Unauthorized Devices

Attackers, who can be located anywhere in the world, are continuously scanning the address space of target organizations, waiting for new and unprotected systems to be attached to the network. Attackers also look for devices which are plugged in and out of the Thromde's network, and those that are not adequately synched with patches or security updates. Attacks can take advantage of new hardware that is installed on the network but not configured not patched with appropriate security updates. Even devices that are not visible from internet are susceptible to be exploited once attackers gain internal access. Any device can be victim of such attacks. Additional systems that connect to Thromde's network (e.g. demonstration systems, temporary systems for installed for testing, guest access networks, etc.) should be managed carefully and isolated in order to prevent adversarial access from affecting the security of Thromde operations.

As new technology continues to be used by the employees, bring our own devices (BYOD) approaches gaining traction where employees bring personal devices into work and connect the BYOD devices to Thromde network. Such devices could already be compromised and can be used to infect internal IT resources.

Managed control of all devices also plays a critical role in planning and executing system backup and recovery.

This control set requires both technical and procedural actions united in a process that accounts for and manages the inventory of hardware and all associated information throughout its life cycle. The controls ensure business governance by establishing information / asset owners who are responsible for each component of a business process that includes information, data, software and hardware.

Actively manage (inventory, track and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.

Sl. No.	Control	Requirement
1	Prepare and deploy an asset inventory management and discovery system which is connected to Thromde's private and public network.	Mandatory
2	Any new device should be adequately verified before connecting to the Thromde network. Once connected the traffic flowing through the device should be monitored.	Mandatory
3	Use a mix od active and passive tools, and apply as part of a continuous monitoring of IT environment. It is recommended that active tool that can scan through IT infrastructure components and passive tools that can identify host based on analyzing traffic is deployed	Recommended
4	Adequate logging should be enabled in the dynamic host configuration protocol (DHCP) server and the logged information should be used to improve the IT asset inventory and help detect unknown systems	Recommended
5	Ensure that all component / device acquisitions are updated in the inventory system, and only approved components / devices are connected to the Thromde network	Mandatory
6	Maintain an asset inventory of all systems and equipment connected to the network, recording at least the network address, machine names(s), purpose of each system / device, and owner of the asset / device. The inventory should include every system that has an internet protocol (IP) address, including but not limited to desktops, laptops, servers, network equipment (routers, switches, firewalls, etc.), printers, storage area networks, Voice Over-IP telephones, virtual machines and virtual addresses, platform software, business applications, and communication suites. The asset inventory created must also include data on whether the device is a portable and / or personal device. Devices such as mobile phones, tablets, laptops, and other portable electronic devices that store or process data must be identified, regardless of whether they are attached to the Thromde network.	Mandatory
7	Deployment of network level authentication via 802.1x to limit and control which devices can be connected to the Thromde network is recommended. The 802.1x must be tied into the inventory data to determine authorized versus unauthorized systems	Mandatory
8	Use of client certificates to validate and authenticate systems prior to connecting to the private network is recommended.	Mandatory

9	Any devices that shows suspicious activities should be immediately blocked from being connected in Thromde network	Mandatory
10	Any device with unusual traffic should be immediately removed from Thromde network either by the user or forcefully by the Administrator.	Mandatory

12.10. Inventory of Authorized and Unauthorized Software

These controls are designed to actively manage (inventory, track and correct) all software on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.

These controls are critical as attackers would continuously scan target organizations looking for vulnerable versions of software that can be remotely exploited. Attackers may use software programs, web pages, document files, or media files to exploit computing resources when the users install / access those files giving attackers long term control of the computing resources. Sophisticated attacks like zero-day exploits taking advantage of previously unknown vulnerabilities for which no patches exist. Hence, adequate knowledge or control of software deployed in Thromde is essential to secure the IT resources. Poorly controlled machines can also be used as launch point for movement of compromising programs throughout the Thromde network and network of agencies within the cluster network.

Controls in this section include the following:

Sl. No.	Control	Requirement
1	Maintain a list of authorized software and version that is required in Thromde	Mandatory
2	The list should be monitored by file integrity checking tools to ensure that the file is not altered	Recommended
3	Deploy application white listing that allows systems to run software only if it is included on the whitelist and prevents execution of all other software. Whitelist application libraries (DLLs) in addition to executable binaries.	Recommended
4	Proper inventory system should be used to maintain and manage the software list with ability to track the version of the applications.	Mandatory
5	Software downloads will have to be verified using the verification approaches provided by the developers of the software using checksum, signature used to sign the codes	
6	The inventory should include platform software like Operating Systems, database packages, etc.	Mandatory
7	The software inventory should be in the same inventory system that of hardware inventory	Mandatory
8	Inventory of pirated / cracked software should be maintained with justification for using such versions of the software	Mandatory

9	Deploy solutions that are bundled with IDS, IPS, firewall, anti-virus, and anti-spyware	Mandatory
10	Any software instances detected with unwanted activities should be blocked from being used (moved to blacklist)	Mandatory
11	Any software instance with unusual traffic should be terminated immediately either by the user or the Administrator	Mandatory

Modern endpoint security suites provide tools for management of application whitelists. Such solutions should be a bundle of anti-virus, anti-spyware, personal firewall, and host intrusion detection systems (IDS) and intrusion prevention system (IPS). Typically used approach for whitelisting is verification of cryptographic has of the executable file.

12.11. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers

It is very important to establish, implement and actively manage (track, report on, correct) the security configuration of laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

Manufacturers and resellers deliver hardware and software geared to ease-of-deployment and ease of use. Thromde is required to implement security configurations. Basic controls, open services and ports, default accounts or passwords, older (vulnerable) protocols, pre-installation of unneeded software can be used to exploit.

Sl. No.	Control	Requirement
1	Standard secure configurations of operating systems and software applications should be established.	Mandatory
2	Standardized images should be used for installation of operating systems. Standardized images should be the hardened versions of the underlying operating systems and the applications installed in the system.	Recommended
3	The standardized images should be validated and tested on regular basis to update their security configuration in light of recent vulnerabilities and attack vectors.	Recommended
4	Strict configuration manage process should be followed, building a secure image that should be used to build systems that are deployed in Thromde	Mandatory
5	Any existing system that becomes compromised should be re-imaged with the secure build	Mandatory
6	Updates (Regular and ad-hoc) or new exceptions to the stored secure image of any system should be processed as per the change management process	Mandatory
7	Always store the master images on securely configured infrastructure validated with integrity checking tools capable of	Mandatory

	continuous inspection and change management to ensure only authorized images as per change management process is possible	
8	While transferring the images between storage and production network always use secure media or secure channel like SSH	Mandatory
9	Perform all remote administration activities on servers, workstations, network devices, and similar requirement over secure channels like SSH, TLS or IPSEC. Avoid use of telnet, VNC, RDP and any other channel that do not support strong encryption.	Mandatory
10	File integrity checking tools should be used to ensure that the critical system files (including sensitive system and application executables, libraries, and configurations) have not been altered.	Mandatory
11	Appropriate reporting system should be implemented that has the ability to account for routine and unexpected alterations, capable of showing history of configuration changes over time and identify who made the changes. The history should provide information on the accounts used to make changes and the account switch details.	Mandatory
12	The integrity checks should adequately identify suspicious system alterations like owner and permission changes to files or directories, use of alternate data streams, addition of new files to system files, etc.	Mandatory
13	File integrity of critical system files are verified as part of a continuous monitoring program	Recommended
14	Automated test and automated configuration monitoring system to be implemented that can verify all configuration elements, and alerts are generated when unauthorized changes occur.	Recommended
15	Use tools compliant with the Security Content Automation Protocol (SCAP) to streamline reporting and integration	Recommended
16	System configuration management tools (e.g. Active Directory Group Policy Objects for Microsoft Windows system, Puppet for UNIX Systems) that will automatically enforce and redeploy configuration settings to systems as per schedule.	Recommended

12.12. Continuous Vulnerability Assessment and Remediation

It is very important to continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers. Thromde IT managers must operate in a constant stream of new information like software updates, patches, security advisories, threat bulletins, etc. Understanding and managing vulnerabilities should be continuous activity.

Sl. No.	Control	Requirement
1	A SCAP validated vulnerability scanner that is capable of checking both code-based vulnerabilities and configuration-based vulnerabilities should used for vulnerability assessment of all systems	Recommended

2	Automated vulnerability scanning tools should be run against all systems and remediate the vulnerabilities	Recommended
3	Fix all the vulnerabilities identified by BtCIRT	Mandatory
4	Audit trail of the vulnerability scanning is maintained	Recommended
5	System administrators should always establish correlation between any attacks and the vulnerability scanning results and determine if any exploit was used against reported vulnerability	Recommended
6	Vulnerability scanning should be performed in authenticated mode irrespective of whether agents are running locally or remote scanners with administrator accounts.	Recommended
7	Always use dedicated account for authenticated vulnerability scans, which should not be used for any other administrative activities.	Recommended
8	Only authorized employee should have access to the vulnerability management tools and each user should be assigned roles	Recommended
9	Relevant IT officer should subscribe to vulnerability intelligence services in order to stay aware of emerging exposure and use the information gained to update Thromde's vulnerability scanning activities	Mandatory
10	Vulnerability scanning activities should be conducted atleast once a month	Mandatory
11	Ensure that the vulnerability scanning tools are regularly updated with all relevant important security vulnerabilities	Mandatory
12	Deploy automated patch management tools and software update tools for operating system and software / applications on all systems for which such tools are available and safe.	Mandatory
13	Scanning activities log should be monitored to ensure the scanning activities are based on the schedules	Mandatory
14	Address all the vulnerabilities either by patching, implementing a compensating control or documenting and accepting reasonable business risk. Adequate information about the business risks should be provided to all stakeholders in the Thromde.	Mandatory
15	Accepted business risks for existing vulnerabilities should be periodically reviewed to determine if newer compensating controls or a patch can address previously accepted vulnerability.	Mandatory
16	Patch management should not impact the normal operation of the systems	Mandatory

12.13. Controlled Use of Administrative Privileges

This controls set describes the processes and tools used to track / control / prevent / correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.

Misuse of administrative privileges is a primary method for attackers to spread inside a target organization. Any workstation running on privileged account can be fooled into opening a malicious program through which attacker can take control of the victim's machine and completely to execute several other programs.

Sl. No.	Control	Requirement
1	Use of administrative privileges should be minimized and used only when required.	Mandatory
2	Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior	Mandatory
3	Use automated tools to inventory all administrative accounts and validate that each person with administrative privileges and validate that each person with administrative privileges on desktops, laptops, and servers	Mandatory
4	Default passwords and other authentication details for applications, operating systems, routers, firewalls, wireless access points should be changed before deploying any new devices in Thromde network	Mandatory
5	All systems should be configured to record log entries and alert when an account is added or removed from a domain administrators' group or when a new local administrator account is added on a system	Recommended
6	Systems should be configured to log unsuccessful login attempts	Mandatory
7	Multi-factor authentication should be implemented for all administrative access.	Mandatory
8	Where multi-factor authentication is not supported, strong passwords should be used. Strong password should be alpha numeric of more than 8 characters with atleast one uppercase and one special character.	Mandatory
9	Administrators should be required to access any system using a fully logged and non-administrative account. Then, once successfully logged in user should transition to administrative privileges using tools like Sudo (in Linux), RunAs (in Windows).	Mandatory
10	Administrators should use a dedicated machine for all administrative tasks or tasks that require elevated access.	Mandatory
11	The machine used for administrative activities should be isolated from primary network of Thromde and should avoid accessing internet from designated machine.	Mandatory
12	Do not use the dedicated machine for administrative activities for accessing emails, composing documents, or surfing internet	Mandatory

12.14. Maintenance, Monitoring and Analysis of Audit Logs

Systems event audit logs are to be regularly collected and analyzed. Analysis of audit logs is important source of information to help detect, understand or recover from an attack. Attackers can hide their access events, malicious software and activities on victim machines and such events

are recorded in audit logs. The logs also provide details of unauthorized access. In absence of solid logs, an attack may go unnoticed indefinitely and damages can be irreversible.

Sl. No.	Control	Requirement
1	Time in the servers and other network equipment should be synchronized with time sources that can be trusted so that the timestamps in logs are consistent.	Mandatory
2	Validate and ensure that audit log settings for each hardware device and software installed in it is adequate to record date, timestamp, source address, destination address and other relevant information of each packet and / or transaction	Mandatory
3	Ensure that systems record logs in a standardized format such as syslog entries or those outlines by the Common Event Expression initiative.	Mandatory
4	If systems are not capable of generating logs in a standardized format, log normalization tools should be deployed to convert logs into standardized formats.	Recommended
5	Ensure that all systems that store logs have adequate storage space for the logs generated so that log files will not fill up the allocated space.	Mandatory
6	The logs must be archive and digitally signed on a periodic basis	Archival is mandatory, digitally signed recommended
7	Thromde IT security personnel / IT administrator should monthly reports that identify anomalies in logs. The identified anomalies should be reviewed and findings documented.	Mandatory
8	The network boundary devices (firewalls, network based IPS) should be configured to verbosely log all traffic (both allowed and blocked) arriving at the devices.	Mandatory
9	A Security Information and Event Management (SIEM) or log analytic tools should be deployed for log aggregation and consolidation from multiple machines and for log correlation and analysis	Recommended
10	The SIEM / log analytic tools should be used to configure profiles of common events to allow detection of such events / unusual activities, to identify anomalies and notify system administrators as per the configuration	Recommended

12.15. Email and Web Browser Protections

This controls set aims at minimizing attack surface and the opportunities for attackers to manipulate human behavior though their interaction with web browsers and email systems. Web browsers and email clients are very common points of entry and attack because of their high

technical complexity and flexibility, and their interaction with users and with the other systems and websites.

Sl. No.	Control	Requirement
1	Only fully supported web browsers and email clients should be allowed to execute in the Thromde. Ideally, only the latest version of stable release should be used in order to take advantage of latest security functions and fixes.	Mandatory
2	Any unnecessary or unauthorized browser or email client plugins or add-on applications should be uninstalled or disabled.	Mandatory
3	All authorized plugins should be based on application / URL whitelisting and use of such applications should be used for pre-approved domain	Recommended
4	Unnecessary scripting languages in web browsers and email clients should be avoided. Use such languages only if it is absolutely necessary.	Mandatory
5	All URLs used for accessing any systems (hosting in all devices) should be logged in order to identify potentially malicious activity and potentially compromised systems	Mandatory
6	Consider deploying two browser configurations in each device. Once configuration with all plugins disabled, unnecessary scripting languages. This configuration should be used for general web browsing. The other configuration with all the required plugins and scripting languages to be used for specific systems.	Recommended
7	Thromde should maintain and enforce network based URL filters that limit devices' ability to access websites and systems	Mandatory
8	Thromde should subscribe to URL categorization services to ensure that the URL categorization is up-to-date with the most recent website category definitions available	Recommended
9	Uncategorized websites should be blocked by default.	Recommended
10	Sender Policy Framework (SPF) should be implemented by deploying SPF records in DNS to lower the chances of spoofed email messages. Receiver side verification should also be enabled in the mail server.	Recommended
11	Make sure that all email attachments entering Thromde email gateway are scanned. Any attachment detected with malicious code or file types that are not necessary for Thromde operations should be blocked.	Mandatory
12	Email scanning should be done before the email is placed in the user's inbox. Scanning should also enable content filtering and we content filtering	Recommended

12.16. Malware Defenses

It is very important to control the installation, spread and execution of malicious code at multiple points in the Thromde, while optimizing the use of automation to enable rapid updating of defense, data gathering and corrective actions. Malicious software is an integral and dangerous aspect of internet threats and can be designed to attack systems, devices and data. Malware defenses must be able to operate in dynamic environment through deployment at multiple possible points of attach to detect, stop the movement of, or controls the execution of malicious software.

Sl. No.	Control	Requirement
1	Employ automated tools to continuously monitor workstations, servers, and mobile devices with anti-virus, anti-spyware, personal firewalls and host based IPS functionality.	Mandatory
2	The tools should be configured to post the malware detection events in Thromde anti-malware administration tool and event log storage	Mandatory
3	The anti-malware software should provide a centralized interface that compiles information and provision to push updates to all machines.	Recommended
4	Once the updates are applied it should be verified that each system has received its signature update	Mandatory
5	Limit the uses of external devices except during situation where there is no alternative.	Mandatory
6	Monitor the use and attempted use of external devices	Mandatory
7	Configure laptops, workstations and servers so that these devices do not auto-run the content from removable media like USB drives, CDs/ DVDs, FireWire Devices, external serial advanced technology attachment devices, and mounted network shares	Mandatory
8	Systems should be configured for automatic anti-malware scan of removable media when inserted	Mandatory
9	Anti-exploitation features such as Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR), virtualization / containerization, etc. should be enabled in the servers and other terminal devices.	Recommended
10	Network based anti-malware tools should be used to identify executables in all network traffic and use techniques other than signature-based detection to identify and filter out malicious content before it arrives at the endpoint.	Recommended
11	Domain Name system (DNS) query logging should be enabled to detect hostname lookup for known malicious domains	Mandatory

12.17. Limitation and Control of Network Ports, Protocols, and Services

It is very important to manage (track / control / correct) the ongoing operational use of ports, protocols, and services on networked devices on order to minimize channels of vulnerability available to attackers. Attackers search for remotely accessible network services that are vulnerable to exploitation.

Sl. No.	Control	Requirement
1	It is to be ensured that only ports, protocols, and services with validated business needs are running in each system	Mandatory
2	Apply host-based firewalls or port filtering tools on end systems, with a default-deny rile that drops all traffic except those services and ports that are explicitly allowed	Mandatory
3	Perform automated port scans on a regular basis on all key devices (servers, routers, managed switches) and compare to a known effective baseline	Mandatory
4	During port scan if a change not listed in the approved baseline is detected then alerts needs to be generated by the scanning tool. Such changes should be reviewed.	Mandatory
5	Ensure that any server that is visible from the internet or an untrusted network, and it is not required for business purpose, then move such servers to an internal VLAN with private address	Mandatory
6	Use Network Address Translation (NAT) to configure systems that are to be accessed from external networks	Mandatory
7	Whenever possible use port forwarding to hide default ports	Mandatory
8	Operate critical services on spate physical or dedicated virtual machines or logical host machines such as DNS, File Server, web server, database server, application server	Mandatory
9	Ensure that application firewalls are placed in front of any critical servers to verify and validate the traffic going to the server. Any unauthorized services or traffic should be blocked and an alert should be generated.	Recommended

12.18. Data Recoverability

This controls set describes the requirements with regard to the processes and tools to be used to properly back up critical information with a proven methodology for timely recovery of it. Sometime attackers make subtle alterations of data stored on compromised machines potentially jeopardizing organizational effectiveness with polluted information.

Sl. No.	Control	Requirement
1	Critical systems (systems storing sensitive information) should be automatically backed up on at least a weekly basis.	Mandatory
2	As and when system updates / upgrades are carried out (e.g. installation of updates, new application systems deployed, etc.), recover point should be created and backed up in secure location.	Mandatory
3	The restore point should comprise of all platform software including operating system, database system, configurations, application system and data on the machine.	Mandatory

4	There should be multiple back ups over time, so that in the event of compromise / malware infection, restoration can be from a version that is taken prior to the compromise.	Mandatory
5	All the back ups should be adequately tested on a regular basis performing a data restoration process to ensure that the back up is properly working.	Mandatory
6	All the back ups (on premise, remote or cloud) should be properly protected via physical security or encryption when stored as well as when moved across network.	Mandatory
7	Key systems should backups in multiple locations – same network but not continuously addressable through operating system call, in detachable storage devices (external drive) and in remote location.	Mandatory
8	All the documents and files generated by the employees should be backed up in storage apart from the local storage of the machines used by the employees.	Mandatory
9	The document storage should be accessible through local domain after adequate authentication to access the files	Mandatory
10	Users should be able to access the files from different machines after successfully logging into the domain irrespective of the machines.	Mandatory

12.19. Secure Configuration for Network Devices

It is essential to establish, implement, and manage (track, report on, correct) the security configuration of network infrastructure devices using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings. Attackers take advantage of network devices becoming less securely configured over time as users demand exceptions for specific business needs. At times the exceptions are deployed and left unreversed once the business need is achieved. Sometimes the exceptions are deployed without proper analysis of associated risks. Typically, attackers search for vulnerable default settings, electronic holes in network devices like open ports and protocols to penetrate into the ICT infrastructure.

Sl. No.	Control	Requirement
1	Define and document Thromde wide standard configuration for network equipment (UTM, firewall, routers and switches). This standard configuration should be approved by Thromde change control team	Mandatory
2	Actual configuration implemented in the network equipment should be properly documented for review, approval and reference	Mandatory
3	Periodically compare configuration with the standard secure configuration defined	Mandatory
4	Any deviations from the standard configuration or updates to the standard configuration should be documented and approved in a change control system	Mandatory

5	Any new configuration rules that deviate from a baseline-hardened configuration that allow traffic to flow through network security devices, such as firewalls and network based IPS should be documented and recorded in a configuration management system. Each deviation should be justified with reason, employee who requested the deviation, and expected duration of the deviation to be implemented	Mandatory
6	All the deviations from the baseline-hardened configuration should be revoked once the business is met	Mandatory
7	Automated tools should be used to verify standard device configurations and detect changes.	Recommended
8	Any alteration to standard device configuration should be logged and reported to the system administrator / security personnel	Recommended
9	Management of network devices should follow two-factor authentication and encrypted sessions	Recommended
10	All network devices should have latest stable version of security related updates	Mandatory
11	The network administrator should use dedicated machine for all administrative tasks or tasks requiring elevated access	Mandatory
12	The dedicated machine used for network administration should be isolated from the Thromde primary network and should not have internet connection	Mandatory
13	The machine used for administrative tasks should not be used for accessing emails, composing documents or surfing internet	Mandatory
14	Management of network infrastructure should be handled from separate VLAN than that of network that has Thromde operations users	Mandatory
15	The critical systems should be hosted through deployment of DMZ	Mandatory
16	Access Control List should be always updated based on the need to access the ICT resources	Mandatory

12.20. Boundary Defense

As the Thromde network is connected to other networks of different trust level, it is important to detect / prevent / correct the flow of information transferring networks of different trust levels with focus on security and data compromise. The boundary lines between internal network and external networks are diminishing as a result of increased interconnectivity within and between organizations. Rapid rise in deployment of wireless technologies largely contributing to it. Boundary defense should be multi-layered, relying on firewalls, proxies, DMZ perimeter networks, and network-based IPS and IDS.

Sl. No.	Control	Requirement
1	Communications from / to known malicious IP addresses (black lists) should be denied or limited or limit access only to trusted sites (whitelists).	Mandatory

2	Periodically carry out test by sending packets from bogon source IP addresses (non-routable or unused IP addresses) into the Thromde network to verify that such communications are not transmitted through network perimeter	Mandatory
3	Subscribe to bogon addresses list. List of such addresses are publicly available from various sources, and indicate a series of IP addresses that should not be used for legitimate traffic traversing the internet	Mandatory
4	On DMZ network, monitoring system should be configured to record at least packet header information but preferably full packet header and payloads of the traffic destined for or passing through the Thromde network border	Recommended
5	The incoming traffic (destined for Thromde network or passing through Thromde network) should be sent to a properly configured Security Information Event Management (SEIM) of log analytics system so that events can be correlated from all devices on the Thromde network.	Recommended
6	Network based IDS sensors should be deployed in Internet and extranet DMZ systems and network that look for unusual attack mechanism and detect compromising activities through the use of signatures, network behavior, etc.	Recommended
7	Network based IPS should be deployed to complement IDS by blocking known bad signatures or the behavior that could be construed as potential attack.	Recommended
8	The network perimeter should be designed and implemented in such a way that all outgoing network traffic to the internet must pass through at least one application layer filtering proxy server.	Mandatory
9	The proxy should be capable of decrypting network traffic, logging individual TCP sessions, blocking individual URL, domain names, and IP addresses. This will allow management of black list and whitelist	Mandatory
10	All the remote login access should use two-factor authentication.	Mandatory
11	All Thromde enterprise level devices should be managed using remote login for configuration, software installation / upgrade, and patch management.	Mandatory
12	A minimum-security standard for accessing Thromde devices should be developed and enforced if third party devices are to be used to access devices in Thromde ICT infrastructure.	Mandatory
13	The third-party devices should be scanned to verify compliance with the security standards before allowing access. Third party device includes any device that is not issued by Thromde even if the device is owned by Thromde employee.	Mandatory
14	Periodic scan mechanism for back-end channel connections to the internet that bypass the DMZ, including unauthorized VPN connection and duel homed hosts connected to Thromde network and other networks via wireless, mobile internet, or other mechanisms is required	Mandatory

15	Firewall session tracking should be configured to identify TCP sessions that last an unusually long-time alerting personnel about the source and destination addresses associated with these long sessions.	Mandatory
16	Ensure that internal network protection is deployed to defend against an internal attacker through network segmentation.	Mandatory
17	Packet sniffers should be deployed on DMZ to look for Hypertext Transfer Protocol (HTTP) traffic that bypasses HTTP proxies.	Mandatory

12.21. Data Protection

These controls define the processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information. Data resides in many places. Protection of data residing in many places can be best achieved through the application of a combination of encryption, integrity protection and data loss prevention techniques.

Sl. No.	Control	Requirement
1	Have proper documentation on how classifying data as sensitive data and normal data. The classification will allow IT professionals to decide on encryption requirement.	Mandatory
2	All storage devices used to move data should have encryption software so that sensitive data can be encrypted while moving from one system to another.	Mandatory
3	Tools to monitor movement of sensitive data to discover unauthorized attempts to exfiltrate data across Thromde network and block such transfers while alerting system administrators	Mandatory
4	Periodic scanning of servers should be configured (or manual scans) to determine whether sensitive data is present in the system in clear text form.	Recommended
5	Identification of devices that are required for movement of data and configure the system to allow data writing process in those identified devices.	Recommended
6	Any sensitive data that is written to the should be encrypted and would require username and password to access the data	Recommended
7	Up to date inventory of authorized devices should be maintained every time	Recommended
8	Network based DLP solutions to monitor and control the flow of data within Thromde network. Any anomalies that exceed the normal traffic patterns should be identified and appropriate actions should be taken to address them.	Recommended
9	Always monitor all traffic leaving Thromde and detect any authorized use of encryption.	Mandatory
10	Thromde ICT infrastructure should be robust enough to detect rogue connections, terminate the connections, and remediate the infected systems.	Recommended

11	Access to known file transfer and email exfiltration websites should be blocked except for those authorized in Thromde	Mandatory
12	Host based data loss prevention (DLP) should be used to enforce ACLs even when data is copied off a machine.	Mandatory

12.22. Controlled Access Based on the Need to Know

This section provides the controls describing the processes and tools used to track / control / prevent / correct secure access to critical assets (e.g. information, resources, systems) according to the formal determination of which person, machine, and applications have a need and right to access these critical assets based on an approved classification.

Sl. No.	Control	Requirement
1	Use concept of network segmentation to create VLANs or otherwise based on classification level of information stored in devices.	Mandatory
2	Sensitive information should be stored in network segment that has adequate filtering to ensure that only authorized individuals are able to access the machines connected to this segment.	Mandatory
3	All communication of sensitive information over less trusted networks should be encrypted.	Mandatory
4	All network switches should enable VLANs for segmented workstations / devices to limit the ability of devices on a network to directly communicate with other devices on the subnet.	Recommended
5	Only authorized individuals should have access / manage to the information based on their need to access the information as part of their responsibilities	Mandatory
6	All information stored in systems shall be protected with file systems, network share, claims, applications, or database specific access control lists.	Mandatory
7	Sensitive information stored on systems should be encrypted at rest and require a secondary authentication mechanism, not integrated into the operating system, in order to access the information	Recommended
8	Detailed audit logging for access to non public data and special authentication for sensitive data. Logging will be turned on for all systems in order to track access and examine situations where someone is accessing data that they are not supposed to be accessing	Mandatory
9	Archived data sets or systems not regularly accessed by Thromde should be removed from the active network devices. Such data can be stored in virtual machines that are powered on on need basis.	Recommended
10	Archived data should be made available to business users / units needing to occasionally use the data or systems.	Mandatory

12.23. Wireless Access Control

This control sets define processes and tools used to track / control / correct secure use of wireless local area networks (LANs), access points, and wireless client systems. Major thefts of data have been initiated by attackers who have gained wireless access to Thromde ICT infrastructure from outside the Thromde premises bypassing Thromde's security perimeters using wireless connection. Wireless clients accompanying traveling officials are infected through remote exploitation during travel or in public access networks (e.g. cyber café). Such exploited systems can be then used as back doors when the devices are connected to Thromde network.

Sl. No.	Control	Requirement
1	Thromde should create and deploy authorized configuration and security profile for wireless devices with type of device owner and business need	Mandatory
2	Each wireless device connecting to Thromde network should match the authorized configuration and the security profile	Mandatory
3	Thromde should deny access to those devices that do not match required configuration and security profile	Mandatory
4	Network vulnerability scanning tools should be used to detect wireless access points connected to Thromde network. The tool should compare the identified devices with authorized device list.	Recommended
5	Identified devices that are not authorized should be deactivated	Recommended
6	Deploy wireless intrusion detection system (WIDS) to identify rogue wireless devices and detect attack attempts and successful compromises.	Mandatory
7	Wireless traffic should be monitored by WIDS tool as traffic passes from wireless to wired network	Recommended
8	Any new devices to be connected to Thromde should be linked to business need. If business need does not exist then connection should be denied	Mandatory
9	When there is a specific business need for wireless access the configure wireless on client machines to allow access only to authorized wireless networks	Mandatory
10	For devices that do not have an essential wireless business purpose, disable wireless access in the hardware configuration	Mandatory
11	All wireless traffic should at least leverage Advanced Encryption Standard (AES) encryption and at least Wi-Fi Protected Access 2 (WPA2) protection	Mandatory
12	The wireless networks should use authentication protocols such as Extensible Authentication Protocol – Transport Layer Security (EAP-TLS), which provide credential protection and mutual authentication	Recommended
13	Peer – to – peer wireless capabilities should be disabled on wireless clients	Recommended
14	Unless required for a documented business need, disable wireless peripheral access of devices (like Bluetooth, NFC)	Recommended

15	Separate virtual local area networks should be used for devices under BYOD scheme or for untrusted devices / devices brought by guests.	Mandatory

12.24. Account Monitoring and Control

Actively manage the life cycle of system and application accounts – their creation, use, dormancy, deletion – in order to minimize opportunities for attackers to leverage them. Attackers frequently discover and exploit legitimate but inactive user accounts to impersonate legitimate users making discovery of attackers' behavior difficult for network watchers.

Sl. No.	Control	Requirement
1	Review all system accounts and disable any account that cannot be associated with a business process and owner	Mandatory
2	All the system access accounts should have provision to activate and deactivate	Mandatory
3	Establish and follow a process for revoking system access by disabling accounts immediately upon termination of an employee.	Mandatory
4	System access accounts should be disabled to preserve audit trails. Reasons for disabling the accounts should be provided.	Mandatory
5	Regularly monitor the use if all accounts, automatically logging off user after a standard period of inactivity.	Mandatory
6	Configure screen locks on systems to limit access to unattended workstations	Mandatory
7	Monitor account usage to determine formant accounts, notifying the user or supervisor.	Recommended
8	Disable accounts that are dormant and are not required anymore	Mandatory
9	Establish process that requires managers match active employees with each account belonging to staff members	Mandatory
10	System administrator should disable accounts that are not assigned to valid staff members	Mandatory
11	Use and configure account lockouts such that after a set number of failed login attempts the account is locked for a standard period of time	Mandatory
12	Monitor attempts to access deactivated accounts through audit logging	Mandatory
13	Configure access for all accounts through a centralized point of authentication like Active Directory or LDAP	Recommended
14	Configure network and security devices for centralized authentication	Recommended
15	Profile each user's typical account usage by determining normal time-of-day access and access duration	Mandatory

16	Reports should be generated that indicate users who have logged in during unusual hours or have exceeded their normal login duration	Mandatory
17	Record when user access system from machine other than machine on which the user generally works	Mandatory
18	Ensure that multi-factor authentication for all user accounts that have access to sensitive data or systems using OTP or similar technology	Mandatory
19	Where multi-factor authentication is not supported, user accounts should be required to use strong passwords on the systems	Mandatory
20	All the accounts usernames and authentication credentials should be transmitted across networks using encrypted channels	Mandatory
21	Verify and ensure that all authentication files are encrypted or hashed and that the files cannot be accessed without privileged accounts	Mandatory
22	Maintain audit log of all access to password files in the systems	Mandatory
23	Do not share system access credentials (username, authentication details) to others	Mandatory
24	If responsibilities is delegated to other users temporarily, new system access credentials should be created and provided to the new staff	Mandatory
25	If system access credentials is shared / leaked and data manipulation is done using shared / leaked access details then accountability rests on the owner of the system access account	Mandatory
26	If account information lost / leaked to unauthorized individuals, owner user should report to the administrator for changing the password	Mandatory
27	If existing users are out of office traveling then administrator should temporarily disable system access credentials and can be activated when the user resume responsibilities.	Mandatory

12.25. Security Skills Assessment and Appropriate Training to Fill Gaps

For all functional roles in Thromde identify the specific knowledge, skills and abilities needed to support defense of Thromde; develop and execute an integrated plan to assess, identify gaps, and remediate through policy, organizational planning, training, and awareness programs. People fulfill important functions at every stage of system design, implementation, operation, use and oversight.

Sl. No.	Control	Requirement
1	Perform gap analysis to see which skills employees need to implement the controls, and which behaviors employees are not adhering. Use the gap analysis information to build a baseline training and awareness roadmap for all employees	Mandatory
2	Organize training to fill the skill and awareness gap	Mandatory

3	Implement a security awareness program that • Focuses on the methods of commonly used intrusions that can be blocked through individual actions • Is delivered as short modules convenient for employees • Is updated frequently • Is mandated for completion by all employees at least annually • Is reliably monitored for completion by employees • Includes the senior leadership team	Mandatory
4	Validate and improve awareness levels through periodic tests to see whether employees will click on a link from suspicious email or provide sensitive information on the telephone without following appropriate procedures for authenticating a caller.	Mandatory
5	Targeted training should be provided to those who fall victim to attacks	Mandatory
6	Use security assessment for each of the mission critical roles to identify skills gaps. Online assessment options can be used to assess.	Mandatory

12.26. Application Software Security

Attacks often take advantage of vulnerabilities found in web-based and other application software. It is important to manage the security life cycle of all in-house developed and acquired software in order to prevent, detect and correct security weaknesses.

Sl. No.	Control	Requirement
1	For all acquired application software, check that the version being used is under comprehensive support from the vendor or Thromde possess capacity to manage and maintain the system.	Mandatory
2	If the existing software is not supported by vendor, upgrade to the supported version or install all recommended relevant patches and security recommendations	Mandatory
3	Web applications should be protected using web application firewalls (WAF) that inspect all traffic flowing to the web application for common web application attacks like cross site scripting, SQL injection, command injection, etc.	Recommended
4	For applications that are not web based specific application firewalls should be deployed if such tools are available for the given application type.	Mandatory
5	If application specific firewalls are not available then host-based application firewall should be deployed.	Mandatory
6	For in-house developed application, explicit error checking should be performed and documented for all input, including for size, data type, and acceptable ranges or formats	Mandatory

7	In-house developed and third party procured web applications should be tested for common security weaknesses using web application scanners prior to deployment.	Mandatory
8	Input validation and outputs should be reviewed and tested thoroughly	Mandatory
9	Error messages should not be displayed to end-users or ensure output sanitization	Mandatory
10	Always maintain separate environments for production and non-production systems	Mandatory
11	Developers should not be allowed to access production environment unless absolutely necessary. Production system access by developers should be monitored	Mandatory
12	Development artifacts (sample data and scripts, unused libraries, components, debug code, or tools) should not be included in deployed system or accessible in the production environment	Mandatory

12.27. Incident Response and Management

Cyber incidents are now just part of our way of life. It is very important to be prepared. Protect Thromde's information as well as its reputation, by developing and implementing an incident response infrastructure (plans, defined roles, training, communications, management oversight) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and the systems.

Sl. No.	Control	Requirement
1	Well documented incident response procedures the include a definition of personnel roles for handing incidents should be developed. The procedures should define the phases of incident handling.	Mandatory
2	Assign job titles and duties for handling computer and network incidents to specific individuals	Recommended
3	Define management personnel who is supposed to support the incident handling process by acting as key decision-making personnel in incident response team	Recommended
4	Devise Thromde wide standards for the time required system administrators and other personnel to report anomalous events to the incident handling team, the mechanism for such reporting, and the kind of information that should be included in the incident notification.	Mandatory
5	The reporting should also include process of notifying BtCIRT as per the standards developed by BtCIRT	Mandatory
6	Publish information for all employees of Thromde regarding the computer anomalies and incidents.	Mandatory

7	Regular employee awareness activities should have incident information to be shared	Mandatory

12.28. Penetration Tests

It is essential to test the overall strength of Thromde's defenses (the technology, the processes and the people) by simulating the objectives and actions of an attackers.

Sl. No.	Control	Requirement
1	Regular external and internal penetration test to identify vulnerabilities and attack vectors that can be used to exploit Thromde systems successfully needs to be executed.	Mandatory
2	Both outsider and insider attacks should be simulated	Mandatory
3	Accounts used for penetration testing should not be used for any other activities. Strict monitoring of such accounts is required.	Recommended
4	Perform periodic red team exercise to test Thromde's readiness to identify and stop attacks or to respond quickly and effectively	Recommended
5	Include tests for the presence of unprotected system information and artifacts that are useful to the attackers like network diagrams, configuration files, emails or documents containing passwords, etc.	Recommended
6	Use vulnerability scanning and penetration testing tools. The results of vulnerability testing can be used as starting point for penetration testing	Recommended
7	Red team exercise reports should be well documented and archived	Recommended

12.29. System Development

The systems development controls provide several controllable activities that distinguish an effective systems development process.

Sl. No.	Control	Requirement
1	A preliminary feasibility study should show that the system development project is feasible	Mandatory
2	All systems should be properly authorized to ensure their economic justification and feasibility	Mandatory
3	System development plan should be prepared and endorsed by the Thromde management. The plan should include activities covering standard system development life cycle. Activities should cover: • Planning • Systems Analysis and Requirement • System Design • System Development & Testing • Implementation	Mandatory

	• Operation and maintenance Roles and responsibilities of all stakeholders should be clearly specified in the project plan.	
4	A formal process should be established where business users submit request and the request is reviewed in a forum where the requesting user is provided opportunity to justify the need	Mandatory
5	Users should be actively involved in the system development process.	Mandatory
6	Technical complexity should not stifle user involvement. Regardless of technology involved, detailed written description of needs should be generated, reviewed and vetted by the users	Mandatory
7	System professionals / consultants should provide required support to user for validation of needs / business requirement documents	Mandatory
8	The requirement should provide sufficient details to the technical professionals (in-house team, external consultants)	Mandatory
9	System development team should comprise of business / process owners, end users, technical professionals, quality assurance professionals, trainers and post implementation support professionals	Mandatory
10	If system development needs to be outsourced, Thromde procurement process should be followed to select development partner and should be in compliance with the Thromde Internal Control guidelines	Mandatory
11	All deliverables and milestones should be finalized and enforced for timely delivery of the system	Mandatory
12	Minimum set of documentation that are required to be generated are: 1. User needs specification 2. Business process and workflow documentation AS-IS and TO-BE 3. System Functional Requirement Specification 4. System Requirement Specification 5. Test Cases with test plan 6. Detailed design document (application, database and other interfaces) include class diagrams and database schema 7. Test execution reports 8. System user manual 9. System Administration manual 10. System operations manual	Mandatory
13	If consultants are hired to develop and implement the systems, then relevant team members in the Thromde should review and vet the documentations submitted by the consultants	Mandatory
14	Agile approach to system development should be adopted to ensure early discovery of issues, errors and mismatch with the requirement. Agile approach requires frequent verification by the user group	Mandatory
15	All program modules should be thoroughly tested by the users of the system before implementation	Mandatory

16	The results of the tests should be compared with predetermined results in the test cases to identify programming and logic errors	Mandatory
17	Testing should be extensive and involve several transactions that test all aspects of the system	Mandatory
18	The test team should be composed of user personnel, system professionals and internal auditors	Mandatory
19	The details of the tests and the results should be formally documented and analyzed.	Mandatory
20	Testing of systems should include the following: • Authenticity tests that verify that and individual, a programmed procedure, or a message attempting to access a system is authentic • Accuracy test which ensure that the system processes only data that conform to specified tolerances • Completeness test which identify data within a single record and entire records missing from the batch • Redundancy test which determine that an application processes each record only once • Access test which ensure that the application prevents unauthorized users to access the data in the system • Audit trail test which ensures that the application creates an adequate audit trail	Mandatory
21	Test data should have complete set of valid and invalid transactions	Mandatory
22	Source version management should be followed where version number automatically assigned by the version management systems	Mandatory

12.30. System Change Management

Change may be needed for many reasons like application modifications and enhancements, vendor recommendations / requirements, periodic maintenance, changes in regulations, application failures, addition of modules / applications, etc. There are generally two types of changes viz. incident reports and functional modifications. Incident reports are changes as a result of system failure or an error preventing a user from completing a task. Functional modifications are changes requested that are not part of the initial scope of system.

Change management should be as per the following procedure:

a. Document Change Request -- A functional business owner must first make a request to the change control team in Thromde. The request should include the following information:

- Incident report or function modification desired
- Description of the requested change
- The system(s) involved
- The functional business unit affected

- Date by which the change is needed

b. Requirement Analysis – The requirement analysis should be done by the change control team working in conjunction with the requesting functional business unit. Technical staff should be included in the change control team. Analysis should include:

- Develop specification requirement
- Determining impact of change to all functional business units
- Determining the impact to system performance
- Determining the impact of integration (if applicable)
- Plan of ensuring sustainability
- Consider best practices
- Technical design and review based on approved requirements
- Communicate the proposed change and obtain sign off from all affected functional business units
- Obtain written sign off for specification requirement

c. Code and validation - The development team should make the changes to code as specified in analysis phase. The code changes should be performed in the development environment only. Code changes should meet the following

- Appropriate development kit should be used
- Code reviews performed
- Unit testing with documented results
- Develop version and custom impact controls
- Communicate with functional business user

Once complete the development team should deploy the changes in test environment and inform the business unit to commence testing of changes.

d. User acceptance Testing and Approval – the functional users should perform functionality testing of the changes incorporated in the system. The testing should include:

- Functionality testing
- Assess impact on operations and security
- Verify that only intended and approved changes were made
- Communicate testing results and / or needed modification to developer
- Provide sign off

Approval of changes should be based on formal acceptance criteria. Functional user should give written approval of changes made to the developer.

e. Documentation – Documentation is required for all changes made by the developer. It should be developed and maintained throughout all phases of the change management process. Documentation should include:

- Change specification / requirement
- Approval / acceptance of change specification / requirement
- Code changes documentation
- Communication of changes to functional business units
- End user documentation
- Documented fall back plan

f. Release Planning and Implementation - Upon notification by the developer the changes should be deployed in the production environment as per the change implementation schedule. Release planning and implementation should include the following:

- Verification that all appropriate approvals have been obtained
- Validate custom change package
- Migrate custom change to production environment during next available change implementation schedule time slot
- Version control
- Communicate completion to change to change control team and the business users
- Close change ticket

Annex – I: Access Control Matrix - Roles

System Name	System Description	Role Name	Authority Description	Access Control				Remarks
				System Function	View	Edit	Add	

Annex – II: Access Control Matrix – Users

Employee Name	Employee Designation	Job Role Brief	System Access Username	Role Assigned	Date of Creation	Status	Remarks

Annex – III: Access Control Suspension / Deactivation

Sl. No.	Employee Name	System Access User Name	Role Assigned	Suspension Date	Suspension Reason	Remarks

Annex – IV: Access Control Activation

Sl. No.	Employee Name	System Access User Name	Role Assigned	Activation Date	Activation Reason	Remarks

Annex – V: Hardware Component Inventory

Component ID	Serial No.	Device Type	Model	Manufacturer	Installation Date	Owner	Location	Status (Authorized or Unauthorized)

Annex – VI: Software Component Inventory

System Name	System Description	System Type	Technology Platform	Application Tier Type	Implementation Date	Vendor	License Type	Maintenance Contract (Yes / No)

Annex – VII: Maintenance Log

Component Name	Maintenance Type	Date of Maintenance	Maintenance Service Executed By	Spare Parts Used	Remarks

Annex – VIII: System Update Schedule

System Name	Update Type (Manual / Automatic Update)	Scheduled Date	Actual Update Date	Update Cost	Update Executed By	Remarks

Annex – IX: Change Management

System Name	Change Description	Request Submission Date	Date of Finalization	Change Deployment Date	Test Completion Date	Production Date	Document Reference

Annex – X: Support Ticket Management

System Name	Issues / Bug Description	Responsible User	Submission Date	Solution Deployment Date	Test Completion Date	Production Date	Document Reference

Annex – XI: Service Contract Management

System Name / Component Name	Service Provider	Contract Date	Start Date	End Date	Contact Information	Remarks

Annex – XII: Open Port Log

Device Name	Open Port / Protocol / Service	Port Use	Opened Port	Opened on	Remarks