Business & Computing Examinations (BCE)
LONDON (UK)

BCE Information Technology (IT) Strategy

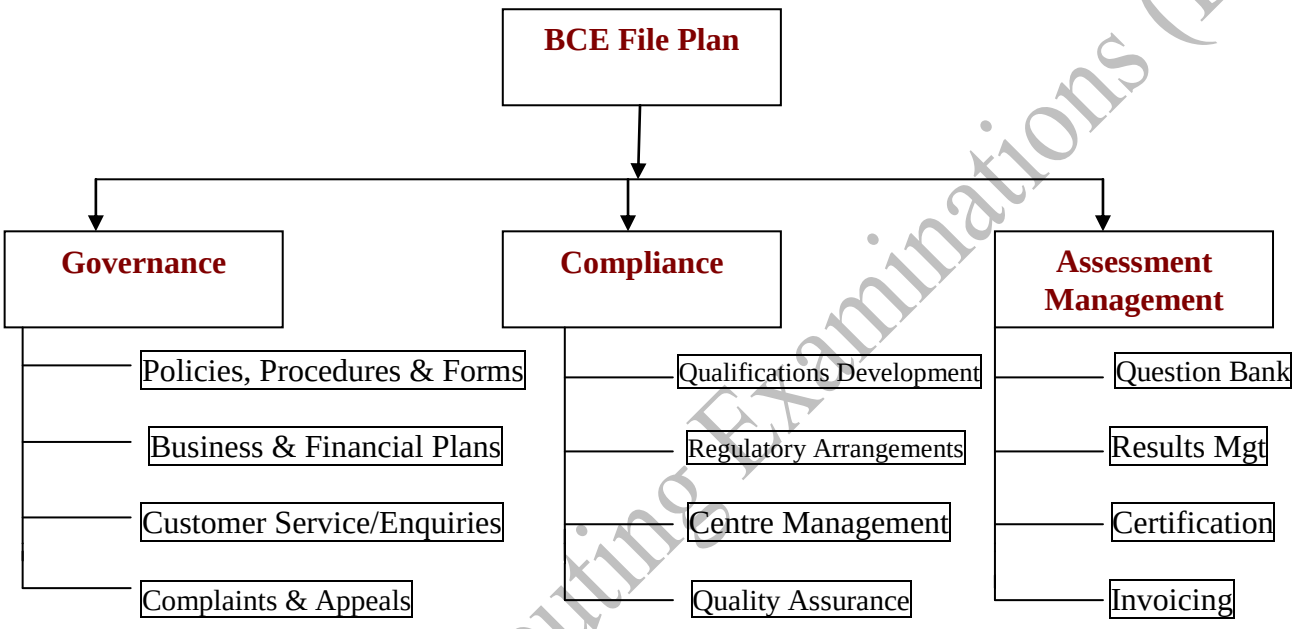
Information Technology (IT) Strategy Framework

1. Management	2. Audit	3. E-Commerce	4. Security	5. Operations	6. Business Continuity	7. Systems Development	8. Third Party / Contracting
• Policies & Procedures • IT Plan • Data Integrity • Data Classification • Job Descriptions • Personnel Screening • Confidentiality Agreements • Segregation of Duties	• Risk Assessment • Audit Plan • Audit Resources • Reporting	• E-Commerce Policy • E-Commerce Business Planning • E-Commerce Controls • Electronic Record Retention • Internet Domain Names • Authentication of Customers • Insurance Coverage • Weblinking • Electronic Mail • Web Site Content • Web site Compliance	• General Security • Physical Security • Logical Security • Firewalls • Event Protection	• General Operations • Network Operations	• Risk Assessment (Business Impact Analysis) • Business Continuity Plan • Defined Recovery Process • Training • Testing • Backup and offsite storage • Insurance	• Systems Development Life Cycle (SDLC) Standards and Procedures • SDLC Management and Controls • SDLC Documentation • Testing Standards • Change Control Approval • Change Control Documentation • Emergency Change Control Procedures	• Risk Assessment • Due Diligence • Contract

BCE Corporate File Plan

BCE will continue to use Excel as the main portal for Centre and Management of Assessment Results. Due to limitations of Access in having a maximum number of records and also now that Access 2010 works more like Excel, BCE has transferred all management of assessment results into Excel. Only Centre address details are stored in Access.

The CEO, Programme Development Manager and Office Manager are fully conversant in IT and networking skills. They ensure BCE network and data security compliance.



Top Level Navigation

The top level navigation comprises of three folders: ***Governance***, ***Compliance*** and ***Assessment Management***.

Underneath each top level folder are 4 subfolders respectively.

(i) Governance top folder and subsequent subfolders

The Governance subfolders contain Code of Practice and Regulations (policies, procedures and workpapers) to establish clear and explicit expectations to minimise risks and problems; Business Plan (Operational and Strategic Plans) to ensure our goals and objectives are achieved; Customer Service charter, complaints database enquiry analysis and appeals.

Policies, Procedures and Forms

These include organisational chart, Terms of Reference/Responsibilities for Board of Advisors, CEO and all functional units (Programme Design & Review Panel, Appeals Panel, Programme Development & Services and Administration).

Business & Financial Plans

The Action Plans, Marketing Plans, Financial Plans and other parts of the Management Handbook naturally belong here. The Management Handbook is an internal document distributed to all staff.

This area also contain completed CEO Action Plans, Management Logs, Management Handbooks and Complaints Management Tracking sheet.

Customer Service/Enquiries
Customer charter compliance and administrative information on enquiries received through web, telephone etc.

Complaints & Appeals
Complaints management investigations/resolutions. This section also include information relating to BCE statistics on enquiries received. In this part of the file plan we have tracking sheets supporting the live management of areas of activity. It also contains the master copy FAQs.

(ii) Compliance top folder and subsequent subfolders

The Compliance subfolders contain information which demonstrates compliance with regulatory rules and regulations by describing;

- Compliance Testing Process
- Compliance Testing Frequency
- Compliance Testing Approach
- Compliance Testing Documentation
- Compliance Reviews and follow-up actions

Qualification Development
This tracks the output of qualification develop activity and include draft and final versions of qualification specifications (and in particular assessment criteria), the outputs of level mapping activity and other sector specific information supporting qualification development. Qualification Development matrixes and currency review checklist are also stored here.

Regulatory Arrangements
This include the documentations developed for Recognition Bodies application and on going forwarding documentations supporting qualification accreditation and the annual statements as required.

Centre Management
This include the Accreditation Handbook, list of Approved Centres, Learner Registers, Centre incidents etc. There are also subfolder structures grouped by centre containing returned forms and evaluations of centre training. The outputs of on-going centre monitoring are also saved here.

Quality Assurance
This contain Centre visit reports, supervision and enforcement guidance, malpractice/maladministration allegations, sanctions and record of specific action taken in support of this.

(iii) Assessment Management top folder and subsequent subfolders

The Management of Assessment subfolders contain information on BCE Assessment, Centre Invoices and Certification. All supporting activities to the development of examination scripts, verification and standardisation activities are saved here.

Question Bank
Contain all BCE Examination Question papers for each year's three assessments. Another highly secure part of our file plan, it contains final examination questions and coursework assignments

structured by examination series. This is our ‘Assessment Question Bank’. It also contains dummy scripts and records of standardisation and verification activities conducted under the oversight of the assessment panel.

Assessment Results Management
This is a highly secure part of our corporate file plan where only responsible personnel manage and track candidate data and results. It contains candidate examination numbers, examination marks, Centre Exam Reports and also Chief Examination Officer and External Verifier reports.

Certification
This contains the certification tracking sheet and master templates for both original and replacement certificates. Also, information about Associate, Member and Fellow membership schemes.

Invoicing
This contains current BCE fee charges, invoices issued to Centres for each year's three assessment windows and Candidate Exam Number Requests.

Introduction to Information Technology Strategy

The BCE Information Technology (IT) Strategy contains the baseline expectations used by BCE Responsible Persons to investigate information systems and technology operations. It provides the basis for a consistent approach to the investigation and supervision of and services. It also provides all functional units with the baseline expectations for general controls.

The IT Strategy is divided into eight sections representing broad categories of IT functions. Each section includes the following subheadings:

- The **Introduction** provides background information and guidance.

- The **Inspection Objectives** determine if the Board of Advisors and CEO have established and maintained effective processes for the IT function as part of BCE's overall internal control environment.

- The **Inspection Procedures** employed by BCE Responsible Persons are based on the criticality and complexity of the business functions.

- The **Essential Practice Statement(s)** describe the baseline expectations for BCE involvement in specific IT functions. The statements are written for the use of all users and Responsible Persons, and are based on regulatory guidance and industry best practices.

The IT Strategy will be updated as BCE and the technology industry change, as the involvement in information technology increases in criticality and complexity, and as the investigation process evolve to address new risks and changes in laws and regulations. Some sections in the IT Strategy do not apply to BCE at the current time, but included for future considerations.

1. Management

Introduction:
The Board of Advisors and CEO actions and philosophy affect all functional units of BCE, including management of information technology. Therefore, executive management must create a framework for the use of Information Technology (IT) by integrating technology strategic planning into the overall corporate plan, developing applicable policies and procedures, and establishing an internal control system to safeguard data. As part of business planning, executive management should complete a risk assessment to identify potential risks to information and information systems, the probability that these risks will occur, and the expected loss if potential risk becomes reality. Then they can determine what guidelines are required to mitigate the known risks, formulate appropriate policies and procedures, and implement controls. The formality of the information technology plan and policies should be commensurate with organisation size, risk, and complexity.

Inspection Objective:
Determine if the Board of Advisors and CEO have established and maintained effective IT management. This is accomplished through the following inspection objectives:

- **Board of Advisors and CEO Oversight** – Evaluate Board of Advisors and CEO's planning and oversight of the IT environment. BCE remains ultimately accountable for managing its IT functions even if some services are being outsourced.

- **Internal Controls** – Assess the overall adequacy of BCE's internal control systems (e.g. IT policies and procedures, plans, segregation of duties, reporting structure, personnel qualifications).

Inspection Procedures:
Inspection activities should be based on the criticality and complexity of the business functions present at BCE. The inspection should begin with a review of audit activities and the risk assessment for IT management.

Essential Practice Statement:
At a minimum, the Essential Practices for IT Management should be clearly documented and functioning within the internal control environment.

Essential Practice Statements	Responsibility	BCE Reference Document
1.1 **Policies and Procedures** Adopt policies and procedures to ensure the organisation's safety and soundness and compliance with law and regulations. **Reason:** Policies provide the basis for establishing and maintaining proper information technology controls. Policies also translate the development, maintenance and use of management information systems into practical and usable user rules and aid in training new employees. As the operating environment changes, the organisation needs to keep pace through updates of policies, procedures, and other operating guidelines. The lack of policy and procedural direction has the potential to cause credit, financial, and other operational problems.	CEO Programme Development Manager Office Manager	Management Handbook *Sections:* ▪ Policies and Procedures ▪ Module 5 (Management) **Inspection Objective** Determine the adequacy of BCE's policy-making process. Determine the adequacy of BCE's policies and procedures.
1.2 **Information Technology Plan** Develop short-and long-range information technology plans, regulation management and budgets that support BCE's mission and goals. Incorporate the information technology plan into the overall corporate plan. **Reason:** Information technology is an integral part of BCE operations. Therefore, the successful development and maintenance of information technology requires Board of Advisors commitment and planning, as well as appropriate oversight. Because major investments in IT resources have long-term implications on both the delivery and performance of automated products and services, IT resources must be integrated into the overall business planning process. While the complexity of the technology plan will depend on the size and operations of the organisation, each technology plan should consider the following critical areas, at a minimum: hardware, software (commercial and in-house development), personnel, and budgets. Operational planning focuses on short-term actions (e.g., annual planning). The operational plans should flow logically from the strategic plan and be revised at least annually.	CEO	Management Handbook *Sections:* ▪ Business Planning ▪ Strategic Planning BCE Business Plan
1.3 **Data Integrity** Ensure data is complete, accurate, and has not been altered in an unauthorised manner (i.e., use appropriate controls such as: edit checks, reasonableness tests, limit tests, common definitions, etc.). **Reason:** Data integrity ensures that data remains complete, accurate, and valid during its input, update, and storage. It will also provide management with accurate information for decision-making. Measures taken to ensure integrity include controlling the physical environment of networked terminals and servers, restricting access to data, and maintaining rigorous authentication.	CEO Programme Development Manager Officer Manager	Management Handbook *Section:* Internal Control Review Internal Control Policy Record Management Policy

1.4 **Data Classification** Classify data and information according to the importance assigned during the risk assessment process. **Reason:** Data classification and the allocation of responsibility for its ownership are important to ensure that the value of information is properly recognised. It is the first step towards ensuring that the most valuable information assets have the highest level of protection. Classifying information can help ensure the correct level of protection will be defined and implemented. Information identification should be done at a high level and identify broad categories of information. For example: • **Public**—non-sensitive information available for external release • **Internal**—information generally available to employees and approved non-employees • **Confidential**—sensitive information intended for use only by specified groups of employees • **Restricted**—extremely sensitive information intended for use only by named individuals	CEO Programme Development Manager Officer Manager	IT Strategy Document *Section:* BCE Corporate File Plan Management Handbook *Sections:* ▪ BCE Policy Framework ▪ Paper Records Retention Policy Management Information System (MIS)
1.5 **Job Descriptions** General document and specific security roles and responsibilities for all employees within their job descriptions. **Reason:** All employees, officers, and contractors should comply with security and acceptable user policies as documented in BCE's code of practice. Describing the systems and processes that employees will protect and the control processes for which they are responsible increases accountability for security.	CEO	Management Handbook *Section:* Corporate Governance
1.6 **Personnel Screening** Verify job application information on all new employees and contractors. Confirm the applicant's: • Character references; • Prior experience, academic record, professional qualifications; and • Identity using government-issued identification. **Reason:** Due to their internal access levels and knowledge of the organisation's processes, authorised users can pose a threat to systems and data. Performing appropriate background checks should reduce the risks of theft, fraud, or misuse of facilities and information. The sensitivity of a particular job or access level may warrant additional criminal background and credit checks. Management should remain alert to changes in employees' personal circumstances that could increase incentives for system misuse or fraud.	CEO Programme Development Manager Officer Manager	Recruitment & Selection Policy

1.7 **Confidentiality and Non-disclosure Agreements** Obtain signed confidentiality agreements before granting new employees and contractors access to information technology systems. **Reason:** Confidentiality agreements put all parties on notice that BCE owns its information, expects strict confidentiality, and prohibits information sharing outside what is required for business needs. A breach in confidentiality could violate regulatory requirements, disregard customer privacy and associated rights, increase fraud risk, disclose competitive information, and damage the organisation's reputation.	CEO Programme Development Manager Officer Manager	Record Management Policy Individual contracts Management Handbook *Section:* ▪ Internal Control Review Internal Control Policy
1.8 **Segregation of Duties** Organise and segregate management and staff assignments to reduce opportunities for unauthorised modification of data, misuse of information, or fraud. **Reason:** Segregation of duties is a basic internal control procedure and is the best deterrent against employee dishonesty or external harm to equipment, documentation or records. For instance, the duties associated with the requisition, approval, execution, and recording of a particular transaction should not be assigned to the same person. Failure to implement and maintain such a system with respect to business activities and information security administration, including maintenance of individual security profiles, constitutes a potentially dangerous practice that may lead to a compromise of system integrity.	CEO Programme Development Manager Officer Manager	Management Handbook *Section:* ▪ BCE Organisational Structure

2. Audit

Introduction:
The Board of Advisors and CEO are responsible for ensuring adequate management practices are in place for effective oversight and management of BCE's IT environment. All functional units should adopt an effective audit and review programme regardless of the number of employees or whether the technology services are provided internally or externally. BCE regulation requires the adoption of internal audit and control procedures that evidence responsibility for review and maintenance of comprehensive and effective internal controls. Standard audit processes should be followed including developing an audit plan and establishing reporting requirements.

Inspection Objectives:
Determine if the Board of Advisors and CEO have established and maintained an effective audit program. This is accomplished through the following inspection objectives:

- **Board of Advisors Direction and Oversight** – Evaluate the Board of Advisors' involvement in establishing IT audit scope and reporting requirements and ensuring the availability of competent IT audit resources.
- **Audit Program** – Assess the quality and effectiveness of the IT audit program. This will assist the Responsible Person in evaluating the adequacy of IT audit coverage and to what extent, if any, the Responsible Person may rely upon the results of the audit program in determining the scope of the IT inspection.

Inspection Procedures:
Inspection activities should be based on the criticality and complexity of the business functions present at BCE. The inspection should begin with a review of audit results and the adequacy of corrective actions.

Essential Practice Statement:
At a minimum, the Essential Practices for IT Audit should be clearly documented and functioning within the internal control environment.

Essential Practice Statements	Responsibility	BCE Reference Document
2.1 **Risk Assessment** Conduct a risk assessment and identify risk exposures (e.g., that threaten data integrity, financial condition, financial performance, continuity of operations, regulatory compliance, and customer service). **Reason:** A risk assessment provides the internal auditor and the Board of Advisors with objective information to prioritise the allocation of audit resources properly. In assessing risk, consider the nature of the specific operation and related assets and liabilities, the existence of appropriate policies, the effectiveness of operating procedures and internal controls, and the potential materiality of errors and irregularities associated with the specific operation. A risk assessment: • Provides a foundation for the audit plan; • Promotes timely audit reporting on high-risk conditions; • Ensures that relevant information has been obtained from all management levels, including Board of Advisors, IT auditors, and functional unit management; • Establishes a basis for managing the audit department effectively; and • Provides a summary of how the individual audit subject is related to the overall organisation as well as to the business plans.	CEO	Risk Management / Contingency Plan Policies Risk Management Log Contingency Plan Report
2.2 **Audit Plan** Develop an IT audit plan based on the results of the risk assessment. **Reason:** The IT audit plan defines the IT scope, objectives and strategies. It establishes a balance between scope, timeframes, and staff days to ensure optimum use of resources.	CEO	
2.3 **Audit Resources** Ensure audit resources are independent, competent, and have the necessary experience to accomplish the IT audit objectives. **Reason:** The ability of the internal audit function to achieve desired objectives depends largely on the independence of audit personnel. The auditor should report and be accountable to the Board of Advisors. This accountability precludes the auditor from certain relationships that may compromise audit independence. The overall competence level required for an internal audit function depends upon the size and complexity of its operations and the responsibility delegated to the auditor. External sources can be used to supplement or perform the IT audit function if internal resources or expertise are not adequate.	External Consultants/Auditors External Verifier Chief Examinations Officer Quality Assurance Manager	Accreditation Handbook Assessment Policy Examination Regulation Policy Health and Safety Evaluation Workpaper
2.4 **Reporting**	CEO	Report of Evaluation (ROE)

Prepare written reports for the Board of Advisors which outline the results of each audit or review. Such reports include: • Description of scope and findings, • Underlying causes of weaknesses, • Conclusions, and • Recommendations for corrective action. **Reason:** Reports communicate audit findings to the board. They also assist management in evaluating the quality of its IT department and identifying methods for correcting or improving adverse conditions.	Programme Development Manager Officer Manager Quality Assurance Manager	

3. E-commerce

Introduction:
The qualifications and assessment services industry's use of Electronic Commerce (E-commerce) to promote its services, disperse information, take online applications, and assist in their own internal operations has increased substantially. Because technology has tended to change rapidly, the array of services and products offered will most likely expand, thereby offering additional income opportunities. While these activities may provide new business opportunities, they will also create new business risks and challenges that must be managed actively. BCE Board of Advisors and CEO must understand the risks associated with E-commerce if they are to make informed decisions regarding the development of a particular product or service. BCE may be conducting these services either in-house or through a vendor relationship with other firms, or may be providing such services to other organisations. Regardless of the method used, executive management is responsible for ensuring that it understands the related business risks, implements the necessary internal controls, and complies with applicable regulatory requirements.

Inspection Objective:
Determine if the Board of Advisors and CEO have established and maintained effective controls over E-commerce activities. This is accomplished through the following inspection objectives:

- **Board of Advisors and CEO Oversight** – Determine the adequacy of Board of Advisors and CEO oversight of E-commerce activities with respect to policies and procedures, planning, management reporting, and audit.
- **Internal Controls** – Determine if BCE has implemented appropriate controls to ensure the availability and integrity of processes supporting E-commerce services.
- **Legal and Regulatory Compliance** – Assess Board of Advisors and CEO's understanding of and adherence to legal and regulatory compliance requirements associated with E-commerce activities.

Inspection Procedures:
Inspection scope should be based on the level of E-commerce activity. The inspection should begin with a review of audit activities and a risk assessment for E-commerce.

Essential Practice Statement:
At a minimum, the Essential Practices for E-commerce should be clearly documented and functioning within the internal control environment.

Essential Practice Statements	Responsibility	BCE Reference Document
3.1 **E-commerce Policy** Adopt E-commerce policies and procedures to ensure safety and soundness and compliance with laws and regulations. Among other concerns, the policies and procedures must address, when applicable: • Security and integrity of Approved Centre and Candidate data; • Privacy of web site customers and visitors; • Notices of web site customers or visitors when linking to an affiliate or third party web site; • Capability of vendor or application providers; • Business resumption after disruption; • Intrusion detection and management; • Liability insurance; and • Prompt reporting of known or suspected criminal violations associated with E-commerce to law enforcement authorities. **Reason:** Establishing applicable policies and procedures is required to comply with laws and regulations, and also contributes to appropriate internal controls for ensuring safety and soundness.	CEO Programme Development Manager Officer Manager	BCE Marketing Strategy Risk Management Log Record Management Policy Operational Management and Evaluation Workpapers
3.2 **E-commerce Business Planning** Describe BCE's business plan, the existing and planned E-commerce initiatives, including intended objectives, business risks, security issues, relevant markets, and legal compliance. **Reason:** Placing this information in the business plan is required to comply with regulations. It will also aid the Board of Advisors and CEO in appropriately preparing for future activities and major investments to provide quality, cost-effective initiatives.	CEO	Management Handbook *Section:* Strategic Plan
3.3 **E-commerce Controls** When applicable, internal systems and controls must provide reasonable assurances that functional units will: • Follow and achieve business plan objectives and policies and procedures requirements regarding E-commerce; and • Prevent and detect material deficiencies on a timely basis. **Reason:** A strong internal control system provides the framework for the accomplishment of management objectives, safeguarding of assets, accurate financial reporting, and compliance with laws and regulations. Effective internal controls serve as checks and balances against undesired actions and, as such, provide reasonable assurance that BCE operates in a safe and sound manner. The lack of internal controls puts BCE at risk of mismanagement, waste, fraud, and abuse.	CEO	Management Handbook *Section:* Internal Control Environment

3.4 **Electronic Record Retention** Records stored electronically must be accurate, accessible, and reproducible for later reference. **Reason:** BCE management might maintain all records electronically, including those recorded originally on paper. The stored electronic record must accurately reflect the information in the original record. The electronic record must be accessible and capable of being reproduced by all persons entitled by law or regulations to review the original record.		
3.5 **Electronic Signatures / Online Inspections** Electronic Signatures: • Develop policies and procedures to comply with the E-Sign Act. • Obtain the customer's agreement to provide electronic disclosures. • Confirm the customer's technological capacity to receive required disclosures prior to providing electronic disclosures. • Continue paper notification on notices of default, acceleration, repossession, foreclosure, or eviction when secured by the primary residence. **Reason:** E-Sign pre-empts provisions in most government statutes or regulations that require contracts or other records to be written, signed, or in non-electronic form. With the parties' agreement, organisations nowadays can engage in E-commerce in many situations. E-Sign pre-empts only those statutes and regulations that relate to business, customer, or commercial transactions. Customers who use electronic signatures should be afforded transparent and effective customer protection that is not less than the level of protection afforded in other forms of commerce.		
3.6 **Internet Domain Names** Protect the organisation's internet domain name(s) by: • Registering and renewing domain names in a timely manner ; • Conducting periodic Internet searches for the organisation's legal or trade names. **Reason:** Timely registration and renewal of domain names are important to ensure that BCE acquires and retains ownership of the Internet address(es) that it desires. Any lapses in registration could result in the loss of a domain name to another party and create customer confusion, reputation harm, fraud, etc. Internet searches of organisation names may identify other parties attempting to confuse or misdirect customers. Additionally, some web sites have been created to publish harmful information about an organisation or to redirect customers by using a domain name similar to that of the original organisation.		

3.7 **Authentication of Customers** Use reliable authentication methods for on-line customer transactions. These methods include the use of passwords, PINs, digital certificates and Public Key Infrastructure, physical devices such as tokens, and biometrics. **Reason:** As most businesses migrate from paper-based, person-to-person transactions to remote electronic access and transaction initiation, the risk of doing business with unauthorised or incorrectly identified people must be evaluated. Failure to control this risk by implementing an authentication program could result in both financial loss and reputation damage to BCE. Additionally, effective authentication can help reduce fraud and promote the legal enforceability of electronic agreements and transactions.		
3.8 **Insurance Coverage** Ensure insurance coverage is commensurate with the level of BCE's E-commerce activities and risk appetite. **Reason:** BCE should have a risk management programme in place to manage the risks inherent in its operations. Insurance can play a role in mitigating risks to an acceptable level so the strategic objectives can be achieved. The availability and extent of insurance coverage varies by carrier. Examples of the kinds of risk for which coverage now exists in the marketplace include: • Vandalism of organisation web sites • Attacks against organisation systems with the intent to slow or deny service • Loss of related income • Computer extortion • Theft of confidential information • Violation of privacy • Litigation (breach of contract) • Destruction or manipulation of data (including a virus) • Fraudulent electronic signatures on Centre agreements • Fraudulent instructions via e-mail • Certain events impacting systems not under the organisation's control (e.g., service provider) • Insiders who exceed system authorisation • Actual or threatened situations requiring the use of negotiators, public relation consultants, security consultants, programmers, substitute systems, etc. The risks noted above are primarily addressed in optional coverage. It is important for BCE to understand what is specifically covered in existing and prospective insurance policies. Exclusions in coverage may apply in a variety of circumstances.		

3.9 **Weblinking** Plan, implement, and supervise weblinking arrangements. **Reason:** Customers and visitors to the web site may become confused about BCE's relationship with a third party and its products. Disclosures to customers and visitors to the web site, including privacy policy, must be clear and concise to avoid confusion. The disclosures must also ensure that customers and visitors to the web site understand that the organisation does not endorse or guarantee a third party's products or services. To avoid potential legal risks, BCE must define the rights and responsibilities of a weblinked third party in formal contracts or agreements.		
3.10 **Electronic Mail (E-mail) Policy** Establish a clear policy regarding the use of e-mail that addresses: • Attacks on e-mail; • Protection of e-mail attachments; • Guidelines on when not to use e-mail; • Expectations that employees will not compromise the company; • Use of encryption to protect the confidentiality and integrity of electronic messages; • Retention of messages which, if stored, could be discovered in cases of litigation; and • Additional controls for examining messages that cannot be authenticated. **Reason:** E-mail differs from traditional forms of business communications by its speed, message structure, degree of informality, and vulnerability to unauthorised actions. Risks include unauthorised access to data, modification of messages, inaccurate addressing or misdirection, and legal considerations (such as the potential need for proof of origin, delivery, etc.).		
3.11 **Web Site Content** Ensure only appropriate content is published on BCE's web site and protect this content from unauthorised alteration. **Reason:** Web sites are often one of the first places that malicious entities search for valuable information. Some generally accepted examples of what should not be published on a public web site, or at least should be reviewed carefully before publication, include: • Classified or proprietary information; • Information on the composition or preparation of hazardous materials or toxins; • Sensitive information relating to internal security; • An organisation's detailed physical and information security safeguards; • Details about an organisation's network and information system infrastructure (e.g., address ranges,		

naming conventions, access numbers); • Information that specifies or implies physical security vulnerabilities; and • Detailed plans, maps, diagrams, aerial photographs, and architectural drawings of organisational buildings, properties, or installations. While information on public web sites is intended to be public, assuming a credible review process and policy is in place, it is still important to ensure that information cannot be modified without authorisation. Users of this information rely upon the integrity of such information even if the information is not confidential.		
3.12 **Web Site Compliance** Ensure BCE's web site contains clear and conspicuous disclosures of the following: • A privacy statement that identifies the information the web site gathers automatically or collects from e-mails or web forms, how the information is used, how the intrusion detection process may help law enforcement identify harmful intrusions, and a statement on weblinking. • A specific statement identifying BCE as an equal opportunity Awarding Body. • A specific statement identifying BCE as an equal opportunity employer if the web site contains job announcements or online job applications. • BCE's official name including any parent/subsidiary relationship. • Have a privacy statement that tell visitors about the types of information the web site collects, how the site collects the information, how the site uses the information, and whether the site gives the information to anyone else. The privacy policy must be clearly written and understandable. **Reason:** BCE as an assessment organisation needs to adapt to a changing technological environment to maintain compliance with laws while using new technologies. BCE should comply with internal laws to provide appropriate disclosures to customers, protect customer information, and minimise financial liability and reputation risk. The privacy of customer personal information has become an increasing concern with the rapid growth in electronic commerce conducted over the Internet, emerging electronic payment systems, and new business affiliations. Organisations are increasingly deploying online systems to facilitate the convenient delivery of services. Some organisations use Internet web sites designed to collect information from customers via online forms, surveys or e-mail links. Information about customers is also collected through inconspicuous means such as hidden, undisclosed electronic information collection methods (e.g., "cookies"). Because of this, customers are increasingly concerned about the collection, use and dissemination of personal information, particularly in the online environment. While customer concerns about privacy are not uniform, studies have shown that the vast majority of customers want the ability to control their personal information and to feel comfortable with how it is used.		

4. Security

Introduction:
Information is an important business asset and, like other important assets, must be protected. To conduct ongoing operations, BCE must have accurate information (or data) available when needed. If this information is also sensitive, such as a candidate examination results record or an employee's personnel files, it must be protected to preserve the individual's privacy and to protect and safeguard the organisation's reputation and legal responsibilities.

Information security is the process by which an organisation protects and secures systems, media, and facilities to process and maintain information. Key elements of any security program must address:

- **Confidentiality**—the assurance that information is accessible only to those authorised to have access;
- **Integrity**—the assurance that information and processing methods are accurate and complete; and
- **Availability**—the assurance that authorised users have access to information and associated assets when needed.

These concepts are achieved by implementing controls, which include policies, procedures, practices, organisational structures, and software applications. These controls must be established to ensure security is commensurate with the organisation's size, risk, and operational complexity. The Essential Practice Statements below are baseline expectations. As the organisation evolves, additional security measures may be necessary.

Security is an ongoing process that is the responsibility of everyone within the organisation. This responsibility begins with the Board of Advisors and CEO who establishes necessary security policies, culture, and direction. Management must implement the CEO's direction through procedures, internal controls, and training. BCE policy and management processes must provide strong support and commitment to security programmes and practices because senior management's attitude towards security affects the entire organisation's commitment to security.

Inspection Objectives:
Determine if the Board of Advisors and CEO have established and maintained effective security over the organisation's facilities, systems, and media that process and store vital information for business operations. This is accomplished through the following inspection objectives:

- **Risk Assessment**—Evaluate the adequacy of BCE's risk assessment process for information security. Key elements of this process may include management's self-assessment of the IT environment (threats, vulnerabilities, and compensating controls).
- **Risk Management**—Evaluate the risk management process used to identify, control, and mitigate security risks.
- **Board of Advisors and CEO Oversight**—Assess the adequacy of information security oversight by examining security policies, procedures, plans, and controls. Oversight responsibilities also extend to all outsourced services and contractors.

- **Internal Controls**—Evaluate the effectiveness of preventive and detective controls designed to identify material deficiencies on a timely basis.

Inspection Procedures:
Inspection activities should be based on the operational complexity and use of information technology. The inspection should begin with a review of audit activities and the risk assessment for information security. If a service provider performs information processing for the organisation, then the organisation's management must perform sufficient due diligence to ensure appropriate internal controls and sound business practices are maintained.

Essential Practice Statement:
At a minimum, the Essential Practices for Security should be clearly documented and functioning within the internal control environment.

Essential Practice Statements	Responsibility	BCE Reference Document
4.1 **General Security** **Security Officer** Appoint a security officer to be responsible for implementing, monitoring, and enforcing the security rules that management has established and authorised (consistent with BCE policies). **Reason:** A designated security officer provides BCE with a central point to coordinate management's security administration, ensure consistency across the organisation, and assist in security-related decision making. **Security Plan** Based on a defined data classification system, document BCE-wide security plan which includes: • Physical security • Logical security • Backup processes and business continuity planning • Employee training and awareness programme **Reason:** BCE needs a comprehensive written security plan to minimise exposure to all threats and risks. Security is the responsibility of every employee within the organisation, not just those working in IT-related sections. Organisation-wide security awareness training puts emphasis on organisation-wide security responsibilities. **User Training** Implement a user education program to promote employees' awareness of information security threats and concerns and their obligation to challenge any person or procedure that may violate security systems. Ensure employees are aware of procedures for reporting observed or suspected security weaknesses and incidents. **Reason:** To minimise possible security risks, all users should be aware of the organisation's security policies and the repercussions of violating them. Security incidents should be reported through appropriate management channels as quickly as possible. Training materials would typically review the acceptable user policy and include issues like log-on requirements, password administration guidelines, etc. Training should also address social engineering, and the policies and procedures that protect against social engineering attacks. Many organisations implement a signed security awareness agreement along with periodic training and refresher courses.	Office Manager	
4.2 **Physical Security** Effective security at an organisation begins with strong physical security measures. Physical security refers to		

the various measures or controls that protect the confidentiality, integrity, and availability of information and systems from threats of theft, fire, flood, malicious destruction, mechanical failure, or power failure. Management can establish physical security by creating physical barriers around the business premises and information processing areas. Examples of physical barriers are walls, locked (electronic or conventional) entry gates, or staffed reception and guard desks. Adequate physical security is necessary to prevent, detect, minimise, and recover losses from damage or unauthorised use of equipment, software, or data. Security measures must protect against both intentional and accidental threats and should be commensurate with the identified risks. (i) **Building** Physically secure or monitor (i.e., security, reception) entrances to the building. **Reason:** Appropriate security barriers and entry controls (key pads, key card systems, biometrics, tokens, etc.) prevent unauthorised access, damage, theft, and interference to business premises and information. (ii) **Equipment** Physically protect equipment from security threats and environmental hazards. **Reason:** Protection of equipment (including that used offsite) is necessary to reduce the risk of unauthorised access to data and to protect against loss or damage. Such protection should also consider equipment sitting (location) and ultimate disposal or destruction. (iii) **Data Centre (i.e., the computer room, the server room)** Restrict access to the data centre and other critical devices (servers, terminals, etc.) to authorised personnel. Key controls include: • Locked data centre • Escorting unauthorised personnel • Unidentified location **Reason:** As noted previously, appropriate security barriers and entry controls prevent unauthorised access, damage, and interference to business premises and information. Restricting physical access to authorised personnel ensures that only those staff members whose job functions require the use of the information or equipment have access to it. Removing or limiting signage on doors to sensitive areas reduces the chance that an intruder or an unauthorised staff member could locate the equipment and damage it.		

(iv) **Location** Strategically locate the data centre in an area of the building that is safe from exposure to fire, flood, explosion, or similar hazards. **Reason:** The data centre houses the organisation's most important information systems components (hardware, software, and data); therefore, it must be as safe as possible from hazards. (v) **Environmental Controls** Establish environmental controls for the data centre, including: • Sufficient air conditioning and humidity control systems to maintain temperatures within manufacturers' specifications. • Adequate fire detection and suppression systems or equipment (i.e., dry chemical, gas, or sprinklers). • Strategically located fire extinguishers. This equipment should be located throughout the building—not just the data centre—and inspected at least annually. • An uninterruptible power supply (UPS) to continue operations during minor power fluctuations or enable the safe shut down of equipment during a prolonged power outage. • Protection for equipment from the effects of static electricity and electrical surges. **Reason:** It is necessary to protect equipment to enable it to function properly and to safeguard it from loss or damage. (vi) **Cabling and Wireless Access Points** Physically secure the building's network wiring infrastructure to prevent unauthorised access. This infrastructure may include wiring closet(s), cabling, and wireless access points. **Reason:** Power and telecommunications connections that carry data or support information services must be protected from interception or damage. **Data** Protect data from fire, theft, destruction, alteration, and other physical hazards. **Reason:** Data security controls are necessary to protect data and software resources from accidental or intentional disclosure to unauthorised persons or from unauthorised modification or destruction.		
4.3 **Logical Security** Effective security controls often combine physical security and logical security by first governing physical		

access to computer facilities or equipment, and then governing logical access to the data stored within the physical system. Logical security refers to the standards and procedures designed to protect data against accidental or intentional unauthorised disclosure, modification, or destruction. Data, or information, is a business asset and is of no use to the organisation if it is incorrect or not available. Additionally, if the information were disclosed inappropriately, the organisation could lose business, damage its reputation, and face criminal or legal liabilities. Proper security over a user's logical access to systems and data is necessary to prevent unauthorised users from gaining access to application and system resources. Examples of logical access controls include user identification (user ID), passwords, and restricting user privileges. Biometrics and tokens can add another level of authentication control to bolster logical security. Again, the level of security must be commensurate with the organisation's size, risk, and complexity.

(i) **Authentication**

Assign unique user IDs to each user, review user accounts periodically to ensure access remains appropriate, adjust access rights when users change jobs, and immediately remove access rights when users leave the organisation.

Reason:

A unique user ID links an individual to actions on the network system and provides a mechanism to identify responsibility. Added authentication controls are necessary when user access to privileged or sensitive systems and information increases.

(ii) **Password Standards**

Establish and enforce appropriate password standards that require all users to:

- Select a unique password and keep it confidential.
- Choose a password that is easy for the user to remember, but difficult for an intruder to guess. Do not use words found in a dictionary (any language), the names of family members or sports teams, or other terms associated with the user or organisation.
- Ensure passwords are not displayed in any form (i.e., when entered on computer screen, printed within reports, or written on a piece of paper in the user's desk).
- Select a password with at least eight characters that include a combination of upper and lower case letters, numbers, and special characters.
- Use unique passwords for a minimum of twelve months before reusing passwords.
- Change the password regularly (i.e., at least every 90 days for general users and more frequently for administrators and privileged users).

Reason:

Passwords are the most common authentication mechanism for validating the user's identity and establishing access rights to information systems and facilities. The strength of an individual's password, and thus the

amount of security provided, relies on continued confidentiality, appropriate complexity, and adequate change frequency.

(iii) **Access Control**
Limit user access for any particular system resource to the minimum required to perform the job function.

Reason:
Access beyond the minimum required for work to be performed exposes the organisation's systems and information to a loss of confidentiality, integrity, and availability.

(iv) **Web Server Security**
Secure web servers and the network infrastructure that supports them.

Reason:
The web server is the most targeted and attacked host on most organisations' network. Security threats to web servers generally result in one or more of the following outcomes:

- Malicious entities may exploit software bugs in the web server, underlying operating system, or active content to gain unauthorised access to the web server. Examples of unauthorised access are gaining access to files or folders that were not meant to be publicly accessible or executing privileged commands and/or installing software on the web server.
- Denial of service (DoS) attacks may be directed to the web server denying valid users an ability to use the web server for the duration of the attack.
- Sensitive information on the web server may be distributed to unauthorised individuals.
- Sensitive information that is not encrypted when transmitted between the web server and the browser may be intercepted by an unauthorised party and then stolen, modified, or disclosed.
- Information on the web server may be changed for malicious purposes. Web site defacement is a commonly reported example of this threat.
- Malicious entities may gain unauthorised access to BCE's computer network via a successful attack on the web server.
- Malicious entities may attack external organisations from a compromised web server, concealing their actual identities, and perhaps making the organisation from which the attack was launched liable for damages.
- The server may be used as a distribution point for illegally copied software, attack tools, or pornography, perhaps making the organisation liable for damages.

4. 4 **Firewalls**
Firewalls are an essential security control for an organisation with an Internet connection. A firewall is a device or collection of components (computers, routers, and software) that enforces a boundary between two or more

networks. They are ideally situated to inspect and block traffic and coordinate activities with network intrusion detection systems. While firewalls provide a means of protection against malicious attacks, they should not be relied on as the only defence. Organisations should complement firewalls with strong security policies, management oversight, and other controls.

Establish a firewall policy that addresses, at a minimum:

- Necessary firewall capacities [type of firewall(s) used];
- Firewall topology and architecture;
- Permissible traffic; and
- Monitoring, testing, and updating.

Reason:
A firewall policy is a component of the overall security policy and documents how management expects the firewall to function.

(i) **Testing**
Test firewall security regularly, especially after any major network configuration changes.

Reason:
Regular testing of firewall security, especially after changes, ensures that controls are functioning effectively and as intended.

(ii) **Logging**
Activate audit logging, copy logs to a secure file system, and review logs regularly to determine if any unauthorised or unexpected activities have occurred.

Reason:
Appropriate logging controls ensure that security personnel can review and analyse log data to identify unauthorised access attempts and security violations, provide support for personnel actions, and aid in reconstructing compromised systems. Log files often contain sensitive information; therefore, management should strictly control and monitor access. Certain audit logs may be required to be archived as part of a record retention policy or to collect evidence.

(iii) **Change Controls**
Establish change control procedures and maintain manual or automatic maintenance records for all program changes.

Reason:

To minimise the corruption of information systems, management must strictly control the implementation of any changes to the firewall and ensure the changes do not compromise the security of either the system or the operating environment. (iv) **Segregation of Duties** Ensure that logical access controls support segregation of duties. **Reason:** Segregation of duties provides a method for reducing the risk of accidental or deliberate systems misuse. An individual should not be allowed to make and also approve changes to the firewall configuration or logging system. Authorisation to make changes should be separate from authorisation to approve changes.		
4.5 **Event Protection** Event protection is an essential control against security events, such as network attacks (i.e., denial of service) or the use of malicious code (i.e., viruses, worms, trojan horses, etc.). Network attacks can prevent legitimate users from accessing the organisation's services. Malicious code can perpetrate various attacks from corrupting data to damaging infrastructure. Event protection is also linked to intrusion detection and response. Refer to discussion of Intrusion Detection Systems (IDS) in the Operations section. (i) **Controls** Train staff about the risks from malicious code. Establish controls to: • Prohibit the use of untested or unlicensed software; • Review the network regularly for unauthorised software; • Prohibit the downloading of software from the Internet or personal PCs; • Scan all unknown disks, including newly purchased software, before using within the organisation's system; • Prohibit the use of shareware or freeware that has not been validated; and • Promote defensive e-mail practices, such as not opening unexpected messages or those from unknown sources. **Reason:** Protection efforts involve both security awareness training and preventative controls. An unauthorised user could exploit even a small weakness and cause significant damage to an organisation's financial condition, ongoing operations, or reputation. (ii) **Anti-virus Software** Maintain current anti-virus software (engine) and update virus definition files frequently (at least weekly). **Reason:**		

Malicious code is created continually and existing code often mutates; therefore, anti-virus products must be updated to protect systems against the latest strains of malicious code. (iii) **Reporting** Routinely report to the CEO the type, frequency, severity, and effect of all security events. Additionally, inform the Board of Advisors of the response and recovery actions taken. Notify the appropriate BCE personnel as quickly as possible when management suspects a security event that affects ongoing BCE operations or other entities. This would also include situations where the organisation activated its disaster recovery or business continuity plan. **Reason:** The Board of Advisors has a fiduciary responsibility to be aware of threats to the organisation and the effectiveness of staff's response and follow-up. This information could show trends and areas of weakness that need further attention. Notifying executive personnel to the existence of an incident enables them to also inform regulators.		

5. Operations

Introduction:
This section encompasses general operations and network operations. General operations involve maintaining and protecting assets and controlling legal liability. Network operations involve maintaining ongoing integrity, efficiency, and availability of BCE's network. Responsibilities and procedures for management and operation of all information process facilities should be established.

Management should ensure that stored and transmitted information is protected from damage, loss, or misappropriation. Failure to do so could result in legal liability as well as severe damage to an organisation's professional and business reputation. Once the latter is damaged or lost, an organisation could find it nearly impossible to continue as a going concern. Therefore, reputation risk can pose a more certain and sudden danger to an organisation's existence than the financial liability that can result from more time-consuming legal action.

Inspection Objectives:
Determine if the Board of Advisors and CEO have established and maintained effective IT operational controls and oversight. This is accomplished through the following inspection objectives:

- **General Operating Controls** – Evaluate the adequacy of management's controls for IT operations (e.g. inventories, software licensing and compliance, hardware disposal, etc.).
- **Network Operating Controls** – Assess management controls for maintaining network integrity, efficiency, and availability.

Inspection Procedures:
Inspection activities should be based on the criticality and complexity of the business functions present at the organisation. The inspection should begin with a review of audit activities and the risk assessment for IT operations.

Essential Practice Statement:
At a minimum, the Essential Practices for IT Operations should be clearly documented and functioning within the internal control environment.

Essential Practice Statements	Responsibility	BCE Reference Document
5.1 **General Operations** (i) **Hardware and Software Inventories** Maintain current hardware and software inventories. **Reason:** Hardware inventories should be maintained to identify assets. Inventories should be used to facilitate: • resource sharing, • software distribution and maintenance, • asset control, • hardware security, and • repair or replacement of hardware. Software inventories should be maintained to identify assets. Inventories should be used to identify: • software for replacement or upgrades, • authorised users, • license compliance, and • unauthorised software. (ii) **Software Licensing** Maintain current software licensing and enforce compliance with licensing agreements. **Reason:** Software licensing and compliance with licensing requirements minimises the legal and financial risks associated with using unlicensed software. As noted above under inventories, an inventory of all software is a key component to controlling this issue, as are detection and protection techniques. (iii) **Equipment Removal/Data Destruction** Establish formal procedures and controls for the secure removal and disposal of information assets. Essential controls include: • Requiring authorisation for removal of equipment, information, or software. • Ensuring all data and software are removed or destroyed prior to equipment disposal. • Ensuring information and equipment to be removed or destroyed is stored in a secure area. **Reason:** Information can be compromised through careless disposal or re-use of equipment. Therefore, storage devices containing sensitive information, as defined by the organisation's data classification system, should be	Office Manager	

physically destroyed or securely overwritten. These actions help protect the organisation from liability by providing security for confidential information, as well as compliance with licensing agreements.		
5.2 **Network Operations** (i) **Intrusion Detection** Establish processes to detect, correct, and report unauthorised system access. Essential elements of the process include: • Detecting external and internal intrusions, • Logging incidents, • Real-time monitoring, • Reporting to management and BCE, • Conducting an impact analysis, • Establishing an intrusion response process and team, and • Updating and maintaining the system. **Reason:** Using an Intrusion Detection System (IDS) enhances BCE's ability to determine if its preventive and protective measures are performing as expected. An IDS also provides some protection against legal liability as it can show an organisation took "reasonably" expected steps to prevent damage, loss, or theft of privileged information. (ii) **Web Site Monitoring** Review the web site to detect unauthorised changes and implement corrective action if necessary. **Reason:** Ensure the web site is available and its integrity is maintained and reputation risk is minimised. (iii) **Internet Use Monitoring** Establish, monitor, and enforce Internet Usage policies and procedures. **Reason:** Ongoing monitoring of internet usage allows management to: • Protect corporate resources (e.g., employee time, network resources); • Prevent inappropriate use (e.g., gambling, pornography, share trading, downloading files, etc.); • Limit legal liability; and • Minimise reputation risk. (iv) **Internet Data Transmissions** Identify and classify all internet transmissions. Secure data transmissions of confidential and sensitive		

information as defined in the organisation's data classification system.

Reason:
Unless encrypted, information sent via the internet is exposed to disclosure, theft or modification and creates potential legal exposure and reputation damage.

(v) **Network Traffic Monitoring**
Monitor network faults, performance, configuration, security, and accounting management.

Reason:
The network system is an integral part of communications infrastructure. Problems affect many or all users quickly and visibly. Projections of future capacity requirements should be made to ensure that adequate processing power and storage are available. A network administrator should monitor network efficiency statistics, ensure that files are backed up regularly and stored off-site, establish and maintain adequate virus protection, review network activity reports, and react to network alerts and alarms.

(vi) **Monitoring Network and Firewall Exploits**
Regularly review the technical alerts/advisories and recommended solutions provided to monitor new threats and implement timely corrective measures to firewalls, network operating systems, and applications.

Reason:
In order to protect the confidentiality, integrity, and availability of data and systems, network administrators must constantly monitor new exploits and ensure that measures to protect against them are applied to systems. Computer hackers and intruders continue to exploit newly discovered holes in firewalls and network systems and devise new attacks.

(vii) **Patch Management**
Implement a patch management program that includes:

- Monitoring vulnerabilities and patches for all software identified in the systems inventory,
- Evaluating the impact of the patches on the organisation's information technology
- Testing the patches to validate expected functionality, and
- Installing the patches throughout the network. systems and environment,

Reason:
Inadequate patching of software vulnerabilities exposes an organisation to significant risk. Although software vendors often develop an update or "patch" to correct identified weaknesses, it is the software user's responsibility to update systems or install patches in a timely manner. Flaws in software code that could cause a program to malfunction generally result from programming errors that occur during software development. The

increasing complexity and size of software programs contribute to the growth in software flaws. By exploiting software vulnerabilities, hackers and others who spread malicious code can cause significant damage, ranging from web site defacement to taking control of entire systems, and thereby being able to read, modify, or delete sensitive information, destroy systems, disrupt operations, or launch attacks against other organisations' systems. (viii) **Network Architecture** Maintain current diagram of network architecture. **Reason:** The network diagram depicts the current network layout and design. It is a tool that the network administrator uses to identify inter-relationships, enforce security, detect problems, minimise risk, and help restore operations.		

6. Business Continuity

Introduction:

All organisations are required to develop, maintain, and test a business continuity plan. These plans enable mission critical systems and functions to be resumed in the event of a disruption. The planning process evaluates an organisation's various departments, business units, or functions to identify critical information systems and business functions. A well researched, current, and comprehensive continuity plan will greatly aid management in selecting reasonable cost solutions in highly stressful disaster situations. Effective business continuity planning should:

- Minimise disruptions of service to the organisation and its customers;
- Ensure timely resumption of operations; and
- Limit financial loss.

Inspection Objectives:

Determine if the Board of Advisors and CEO have established and maintained effective business continuity processes. This is accomplished through the following inspection objectives:

- **Board of Advisors and CEO Oversight** – Evaluate Board of Advisors and CEO oversight of business continuity activities (e.g. planning, management reporting, policies and procedures, audit, etc.).
- **Assessment Planning** – Assess the effectiveness of the organisation's business continuity planning process (development, maintenance, testing, and training).

Inspection Procedures:

Inspection activities should be based on the criticality and complexity of the business functions present at the organisation. The inspection should begin with a review of audit activities and the risk assessment for business continuity.

Essential Practice Statement:

At a minimum, the Essential Practices for Business Continuity should be clearly documented and functioning within the internal control environment.

Essential Practice Statements	Responsibility	BCE Reference Document
6.1 **Risk Assessment (Business Impact Analysis)** Conduct a risk assessment to develop response strategies, which: • Identify events and likelihood of those events that could cause interruptions to business processes and services; • Assess impacts from loss of information and services from both internal and external sources; • Assess the criticality of all business areas; and • Identify and prioritise critical services, operations, and personnel provided by internal and external service providers. **Reason:** Prior to developing the business continuity plan, the criticality of information resources (applications, data, networks, system software, facilities) that support an organisation's critical business process must be determined. With management support, both information systems processing and end user personnel should participate in this analysis.	CEO	Risk Log Contingency Plan
6.2 **Business Continuity Plan** Establish and maintain an organisation-wide business continuity plan that addresses: • Critical services and operations provided by internal and external sources; • Resources needed to support the critical functions; • Steps to be taken in a business disruption; • Coordination with outside parties where necessary; • Board of Advisors approval and annual review; • Defined Business Continuity and Recovery Teams; • Responsibility for Disaster Declaration; • Notification Tree (Employees, Customers, BCE Approved Centres, vendors, local authorities, etc.); and • Testing process and schedule. **Reason:** A Business Continuity Plan provides the vital preplanned framework for initiating recovery operations immediately following a disruption. It also provides guidance for damage assessment and the planned actions that must be taken to resume critical services and restore full business operations with minimum delay.	CEO	Risk Management Policy Contingency Plan Policy Strategic Planning Management Handbook *Sections:* ▪ Strategic Plan ▪ Quality Plan
6.3 **Defined Recovery Process** Establish IT recovery strategies and procedures for mission critical systems, which: • Prioritise system recovery; • Define responsibilities; • Establish expectations for recovery time; and		

• Allow flexibility by providing alternate solutions when necessary. **Reason:** Recovery strategies are necessary to limit the consequence of damaging events and ensure the timely resumption of critical operations. There are various strategies for recovering critical information resources. The appropriate strategy is the one that is most efficient and effective based on the relative risk level identified in the business impact analysis. This strategy is often dictated by the defined recovery timeline and expectations.		
6.4 **Training** Train personnel involved in executing the Business Continuity Plan and recovery strategies. Review and update training needs as changes in plans occur—at least annually. **Reason:** Regular training should be conducted in the agreed emergency procedures and processes, including crisis management. This should ensure that the execution of the Business Continuity Plan is effective when a disruption occurs. It is also important that an effective cross training programme be in place to ensure that vital functions can be effectively performed if key personnel are unavailable at the time of a disruption.		
6.5 **Testing** Test the plan(s) at least annually. The testing process includes: • Scope, goals and objectives commensurate with defined risk; • Reporting to management/board; • Corrective action(s); and • Plan updates to incorporate test results. Based on the risk assessment, consider the following types of testing methodologies: • Desk review; • Simulation; • Technical recovery; • Testing at alternative site; and • Comprehensive Business Continuity Plan Test (include all critical functional units). **Reason:** The Business Continuity Plan should be tested using a fully developed test scenario, a simulated disruption, planned monitoring of results, and appraisal of the entire process with plan revisions, as necessary. Since emergencies do not happen often, periodic testing of the plan is needed to ensure that it is still adequate and that there are skilled personnel to implement it. Tests also serve as training in emergency, backup, and recovery procedures. One of the purposes of the business continuity test is to determine how well the plan works or which portions of the plan need improvement.		

6.6 **Backup and Offsite Storage** Develop and implement backup, storage, and rotation procedures of critical systems including hardware, software, and documents. Consider the following in the backup and storage process: • Location of backup media (in-house and offsite); • Physical and data security at the backup site; • Backup routines for corporate and branches; and • Current list of personnel authorised to access the off-site storage location. **Reason:** To ensure that critical business activities are not interrupted, secondary storage media (CDs, DVDs, removable hard disk or flash disks) are used to store and backup programs and associated data. This media is stored offsite to ensure that it will be available for restoration if the primary business location is inaccessible. The location of and controls over the offsite facility are important to ensure the security of sensitive information.		
6.7 **Insurance** Obtain insurance coverage to guard against risk of loss that exceeds the board and organisation's risk tolerance. **Reason:** Insurance is an effective method to transfer risk from the organisation to insurance companies. It guards against loss from risk that cannot be completely prevented. Generally, coverage is acquired for events with little probability of occurring, but with significant potential for financial loss or other disastrous consequences. Insurance should cover physical losses such as building, equipment, software, etc., and also the costs of business disruption.		

7. Systems Development

Introduction:
Systems development is the process of defining, designing, testing, and implementing a new software application or program. It could include the internal development of customised systems, the creation of database systems, or the acquisition of third party developed software. Written standards and procedures must guide all information systems processing functions. The organisation's management must define and implement standards and adopt an appropriate system development life cycle methodology governing the process of developing, acquiring, implementing, and maintaining computerised information systems and related technology.

Inspection Objectives:
Determine if the board of Advisors and CEO have established and maintained effective systems development methodology. This is accomplished through the following inspection objectives:

- **Board of Advisors and CEO Oversight** – Assess the adequacy of systems development oversight by examining related policies, procedures, and methodology.
- **Risk Assessment**—Determine the level of systems development activities existing within the organisation. If systems development activities for mission-critical systems are handled primarily through a service provider, evaluate management's due diligence to ensure appropriate documentation and controls exist within the service provider's development processes. Assess the adequacy of the organisation's risk assessment process for systems development.
- **Internal Controls**—Evaluate the effectiveness of preventive and detective controls designed to identify material deficiencies on a timely basis. The internal audit function should identify systems development as an area for evaluation and review.

Inspection Procedures: Inspection activities should be based on the criticality and complexity of the business functions present at the organisation. The inspection should begin with a review of internal and external audit activities and risk assessments for systems development.

Essential Practice Statement:
At a minimum, the Essential Practices for Systems Development should be clearly documented and functioning within the internal control environment.

Essential Practice Statements	Responsibility	BCE Reference Document
7.1 **Systems Development Life Cycle (SDLC) Standards and Procedures** Establish written standards and procedures for systems development and maintenance for the systems to be developed, acquired, implemented, and maintained. Review SDLC methodology to ensure that its provisions reflect current generally accepted techniques and procedures. **Reason:** SDLC documented standards and procedures ensure a consistent approach and controls are maintained throughout a systems or application development process.	CEO Programme Development Manager Officer Manager	
7.2 **SDLC Management and Controls** Ensure adequate SDLC management processes and controls exist. Essential management processes and controls over the system development (project) process include: • Appropriate strategic planning for projects within the IT short-and long-term plans, including authorisation and reporting requirements from senior management to the board; • Periodic reporting to the board on project status and target completion dates (including budget variance reports); • Requirements for internal audit involvement in mission critical projects; and, • Requirements for security officer/team involvement regarding security controls. **Reason:** Appropriate management processes and controls over the systems development process ensures efficient use of resources and minimises risk(s) within systems development and programming activities. A general systems development or project management framework defines the scope and boundaries of managing projects, as well as the SDLC or project management methodology to be adopted and applied. Automated project planning, monitoring, and production software aids help control and facilitate the systems development process. Periodic reporting to senior management and the board as well as auditor and security officer involvement enables controls to be considered during the development process prior to implementation into production.	Programme Design & Review Panel	Qualification Development & Assessment Management documents
7.3 **SDLC Documentation** Develop and maintain a well-documented SDLC for all system and application development processes. At a minimum, the SDLC documentation will include: • Project initiation (planning); • Requirements definition (analysis); • System design; • System development; • Testing; • Implementation and support; **Reason:**	Programme Design & Review Panel	Accreditation Handbook *Section:* ▪ BCE Assurance Services Standards

Minimum SDLC standards should ensure that project development is sufficiently controlled to ensure the integrity of the system and IT infrastructure. The development process may differ depending on the method used (prototyping, rapid application development, waterfall, etc.). The process should be flexible while providing maintenance of system integrity and internal controls.		
7.4 **Testing Standards** Document testing standards and procedures. Standard testing procedures include: • A documented test plan; • Types of tests to be used (e.g., unit, parallel, user test, regression); • A restriction of the use of live files in testing to prevent destruction or alteration of live data; • Simulated error conditions to ensure that the program effectively handles all situations; and • Independent verification, documentation, and retention of test results. **Reason:** Testing standards and procedures must be documented to ensure consistency and data integrity during the testing process. The testing phase is designed to prove the reliability of the application or system. Testing is performed in an isolated environment to ensure that new programs do not adversely impact existing production systems. Testing ensures that data will be processed correctly and reliable output will be produced in the desired format.		
7.5 **Change Control Approval** Document standards for managing changes (Change Control) to an existing information systems infrastructure. The Change Control process includes: • Management and business unit approval of the change request; • Specification of change; • Approval for access to source code; • Programmer completion of change; • Request and approval to move source code into the test environment; • Completion of acceptance testing by business unit owner; • Request and approval for compilation and move to production; and • Determination and acceptance of overall and specific security impact. **Reason:** Change management procedures must be documented and followed in order to minimise the likelihood of system disruption, unauthorised alterations, and errors to the existing IT infrastructure.		
7.6 **Change Control Documentation** Document the process for modifying information systems programs. Change Control documentation includes: • Change request date; • Person(s) requesting;		

• Change request approval; • Change request approval and acceptance (Management and business users); • Documentation revision date; • Quality assurance approval; • Final business unit owner acceptance and approval; and • Date moved into production. **Reason:** Change control documentation is necessary to ensure management and users are aware of changes being made to the existing IT infrastructure. Documentation is also necessary to ensure appropriate segregation of duties between production, application, and operation staff.		
7.7 **Emergency Change Control Procedures** Document and control Emergency Program Changes. Control procedures include: • Approval by supervisory personnel; • Review of changes by a knowledgeable supervisor if the source code is changed; • A form used to identify the change, indicate the reason(s) for the emergency change, identify who made the change, record the date the change was made, and document the authorisation signature(s); and • Completion of normal management procedures after the emergency change is made (see Change Control Essential Practice Statements above). **Reason:** Occasionally the need for program change arises that must bypass normal change procedures. Such a change might be required to restore production processing. These immediate (emergency) changes are usually called patches, quick fixes, program temporary fixes, or temporary program changes. The use of such techniques should be strictly controlled to prevent unauthorised changes and to ensure that approved changes are made correctly.		

8. Third Party/Contracting

Introduction:
The intense competition in the Qualification and Assessment services industry has caused organisations to actively seek ways to cut costs and focus on their primary business. The rapid changes in information systems technology have caused many organisations to contract with third-party organisations for information processing, including mission critical applications. This interchange of services between organisations involves certain risks and responsibilities that must be addressed by both the service provider and receiver. While some of these can be defined and delegated within the service level agreement, others must be handled by each party through the implementation of proper operational controls. A legal counsel who is familiar with the terminology and specific requirements of a data processing contract should review it to protect the organisation's interests and avoid or minimise problems in the contractual arrangement. This may require hiring legal counsel with specialisation in IT issues.

Inspection Objectives:
Determine if the Board of Advisors and CEO have established and maintained effective controls for technology services provided or received. This is accomplished through the following inspection objectives:

- **Board of Advisors and CEO Oversight** – Assess the adequacy of Board of Advisors and CEO's risk assessment and due diligence efforts.
- **Contract Management** – Evaluate contracts and service level agreements to ensure technology service provider and receiver expectations are clearly defined.
- **Performance Monitoring** – Assess management's ongoing monitoring of the technology service provider or receiver and related contracts.

Inspection Procedures:
Inspection activities should be based on the criticality and complexity of the business functions present at the organisation. The inspection should begin with a review of audit activities and the risk assessment for technology service providers and receivers.

Essential Practice Statement:
At a minimum, the Essential Practices for Technology Service Providers and Receivers should be clearly documented and functioning within the internal control environment.

Essential Practice Statements	Responsibility	BCE Reference Document
8.1 **Risk Assessment** Conduct a risk assessment to ensure an outsourcing relationship is consistent with BCE's short-and long-term goals. A risk assessment considers: • Strategic goals and objectives of BCE; • Staff's ability to oversee outsourcing relationships; • Importance of the services to BCE; • Contractual obligations and requirements for the service provider; • Contingency plans, including availability of alternative service providers, costs and resources required to switch service providers; and • Necessary controls and reporting processes. **Reason:** The Board of Advisors and CEO are responsible for understanding the key risks associated with outsourcing arrangements and ensuring that effective risk management practices are in place.	CEO	Risk Management / Contingency Plan Policy Risk Management Log Contingency Management Log
8.2 **Due Diligence** Perform and document due diligence to ensure technology service providers are managed adequately, competent technically, stable financially, and insured appropriately. **Reason:** Performing the due diligence allows management to evaluate service providers to determine their ability, both operationally and financially, to meet the organisation's needs. Insurance coverage provided by the service provider should complement and supplement the organisation's coverage. The coverage should be reviewed to determine if it is adequate and consistent with what the organisation would have purchased without an external provider. Where the service provider's coverage is not sufficient, the organisation should consider obtaining additional coverage.		
8.3 **Contract** Include the following elements in the written contract: • Quality measures (Service Level Agreements or minimum levels of service); • Pricing; • Data ownership and confidentiality; • Right to audit; • Control expectations (i.e., security, change control, systems development, etc.); • Remediation; and • Reporting expectations for the Technology Service Provider to BCE. **Reason:** Documenting these measures ensures BCE's interests are protected, misunderstandings are minimised, and		

ongoing service is provided that is consistent with expectations.		
8.4 **Monitoring** Perform and document reviews of service provider's financial information, internal audit reports, status reports, and service level agreement reports. **Reason:** It is essential that BCE implement an oversight programme to monitor each service provider's controls and performance. Although services may be outsourced to achieve certain benefits, the responsibility for outsourced activities remains with BCE's Board. Documenting the process is important for contract negotiations, termination issues, and contingency planning. Specific personnel should be assigned responsibility for monitoring and managing the service provider relationship. The number of BCE personnel assigned and the amount of time devoted to oversight activities will depend in part on the scope and complexity of the services outsourced.		