**Special Examination Risk Assessment Guide  
for Information Technology Systems**

**Table Of Contents**

Information Technology 3

Based on the special examination methodology of the OAG: 3

IT Audit Criteria and sub-criteria 3

Risk Assessment: 4

Appendix – List of Requested Documents for Special Examination Risk Assessment for Information Technology (IT) 15

|  |
| --- |
| Information TechnologyBased on the special examination methodology of the OAG: The purpose of this guide is to assist the auditor in completing a risk assessment of information technology systems and practices during the planning phase of a special examination. At the end of this assessment, the auditor will be in a position to assess whether there are risks related to information technology that could impact the Crown corporation’s **statutory control objectives.**  This guide has been aligned with best practices in the field of information technology auditing as described in COBIT 4.0, ISO17799, ITIL, Val IT and the 2007 Certified Information Systems Auditor (CISA) Review Manual. It has been kept short and as a result, it is possible that due to the specialized nature of the subject matter and the complexity of the IT environment in your entity that you may have to perform additional work. If this occurs, it is recommended that you consult with the Information Technology Performance Audit Internal Specialist.  Before completing this guide, the auditor should gain a general understanding of the entity’s operations. This can be done by reviewing documents such as the corporate plan. To prevent duplication of effort, review the information gathered in the financial attest files. Specifically, the auditor should review the C.8 section of the entity’s most recent teammate file.  The next step includes scheduling a kick-off meeting with the executive responsible for information technology systems, normally the CIO. At this meeting provide the list of documents to be obtained and ensure that the client understands what is being requested (see Appendix). Identify the key personnel who should be interviewed in order to complete the four sections of the risk assessment guide.  After completing the questionnaire and reviewing the documents obtained, the auditor should prepare a short report listing potential lines of inquiry and potential findings that could prevent the entity from achieving its expected results. The report should describe the audit approach to collect the audit evidence, the time and resources that will be required during the examination phase.  If specific lines of enquiry have been approved for the examination phase, additional audit programs will need to be developed (e.g. IT Strategic Planning, IT Project Management, IT Security, IT Service Delivery) |

## IT Audit Criteria and sub-criteria

|  |
| --- |
| The planning, development, implementation, and management of information technology and systems support the organization’s strategic and operational objectives, ensure business continuity, and satisfy informational needs at an acceptable cost and on a timely basis. |
| 1. IT strategic and operational plans are aligned with and support the direction and priorities of the corporation. They should be reassessed periodically and amended in response to changing business and IT conditions. 2. Acquisition of computer-based systems takes into consideration the needs of both individual users and the corporation as a whole, as well as identified risks and tolerance for risks. 3. Information systems are available and usable when required, and are designed appropriately to resist attacks and recover from failures. 4. IM/IT activities provide quality customer service while ensuring the efficiency and effectiveness of processes and operations. |

**INFORMATION TECHNOLOGY**

## Risk Assessment:

| Step | Description | Done  by | Reference |
| --- | --- | --- | --- |
| **1 IT strategic and operational plans are aligned with and support the direction and priorities of the corporation. They should be reassessed periodically and amended in response to changing business and IT conditions.** | | | |
| 1.1 | Refer to the list of documents and review those referenced to this section.   1. As part of the review of the IT Strategic Plan consider the following:    1. The Plan contains an overview of the IT Business Unit vision; IT strategic objectives are linked to organizational objectives; initiatives have timelines and benefits; emerging technologies are discussed; performance indicators and resources are included.    2. The Plan is aligned with the business and IT risks. 2. As part of the review of the IT tactical/operational plans consider the following:    1. The Plans establish precise objectives dates, assigned responsibilities, actions, resources timelines    2. Plans and tasks are understood and accepted by both Business and IT |  |  |
| 1.2 | Through discussions with Senior IT Management obtain an understanding of the governance environment:   1. Is IT included in key executive committees? How? 2. What are the IT issues discussed at these meetings? 3. What other committees does IT participate in? (steering committees, user committees) |  |  |
| 1.3 | Through discussions with Senior IT Management obtain an understanding of the efficiency and effectiveness of the IT annual and strategic planning processes. Consider the following:   1. Does senior IT management have a good understanding of both the business and IT plans? Do they understand how the IT plans support the business plans? 2. Are the IT senior executives involved with the rest of the senior management team in the joint planning across the enterprise? 3. How input is solicited from relevant internal and external stakeholders/business partners in the development of the IT strategic plan? 4. How is information that is used as part of the decision making process, how is the information validated? 5. Who approves the IT strategic plan and when? 6. How are IT strategic plan elements translated into tactical/operational plans? 7. Are there processes in place for plan changes? Are they applied and followed? |  |  |
| 1.4 | Through discussions with Senior IT Management obtain an understanding of the process by which new technology is incorporated into the current IT environment:   1. Are IT opportunities and emerging technologies important elements in the IT strategic plan? 2. How is input solicited / received regarding the use of emerging technologies? 3. How are the benefits of merging technologies determined? (E.g. are potential system gains evaluated?) |  |  |
| 1.5 | Conclude on sub-criteria 1 |  |  |

| Step | Description | Done by | Reference | |
| --- | --- | --- | --- | --- |
| **2 Acquisition of computer-based systems takes into consideration the needs of both individual users and the corporation as a whole, as well as identified risks and tolerance for risks.** | | | | |
| 2.1 | Refer to the list of documents and review those referenced to this section.  As part of the review of this documentation and discussion with IT Management consider the following:  Note: In the absence of a formal project management methodology being in place, the questions below should be asked from the perspective that these processes/procedures should be in place.   1. Is there a project brief (overview) that elaborates on how the requested project aligns with the entity’s strategic direction and plans? 2. Does the methodology call for the creation of the following documents: (business case, project charter, project plan, risk register)? 3. Does the methodology call for the alignment of these key project documents with business and information management directions and plans? 4. Is there a requirement for project structures to define key accountabilities including sponsorship, steering committee and management? 5. Does the methodology cover, at a minimum, the allocation of responsibilities, task breakdown, budgeting of time and resources, milestones, check points and approvals? 6. Do the project managers follow the same project management methodology in a consistent manner? 7. Is the project management methodology easy to adapt to different types and sizes of projects? 8. Is internal audit involved in IT projects and how? |  | |  |
| 2.2 | Through discussion with IT management, and review of monitoring reports obtain an understanding of the processes for maintaining and monitoring of IT systems. Consider the following:   1. How are performance reports used to help achieve the management objectives? 2. Is there an appropriate process of capturing, logging, resolving and following-up on reported problems? 3. Are there mechanisms used to track change requests, approvals, prioritizations, assignments and user acceptance? 4. For major maintenance changes, is a Post-Mortem conducted to determine if planned benefits have been achieved and are consistent with the organization’s business plans. 5. Are actual costs and deliverables compared to the original estimates? |  | |  |
| 2.3 | As part of the review of the Project portfolio and discussions with IT management consider the following:   1. Are there organizational policies in place that describe how projects are prioritized and resourced? 2. To what extent have the cost benefit analyses been used to prioritise and approve the projects? 3. Does the prioritisation process require that candidate projects be linked to business directions and plans? 4. Who determines which projects will be allocated resources? 5. How are the projects limited to ensure adequate resources are available? 6. What is the process for ensuring that required internal IT projects get resourced satisfactorily? 7. How are changes in project priority handled? |  | |  |
| 2.4 | Through discussions with IT Management and by reviewing relevant documents such as risk assessment policies and meeting minutes obtain an understanding as to whether project management decisions are based on risk management. Consider the following:   1. Are large complex projects reconstituted into a set of more manageable and less risky sub-projects 2. How does management effectively co-ordinate all of the individual sub-projects? 3. Does the project have scheduled checkpoints or gates where it is independently reviewed and management can decide on the future of the project and any appropriate corrective action? 4. Is the performance of the project reviewed at each gate, or when the released funds run out? 5. Are risk assessments performed to identify the risks involved and establishing the project's scheduled gates and decision points? 6. Is a risk register and risk log maintained for the life of the project? 7. What tools and methodologies does the organization have to manage the project risks? |  | |  |
| 2.5 | Through discussions with IT Management and the review of related documents, obtain an understanding of the System Development Life Cycle Methodology used by the Organization.   1. Are the internal clients of systems fully involved and committed to ensure that systems meet their business requirements? 2. What are the accountabilities of the Information Technology and systems group? 3. Does the SDLC methodology include the requirement to assess skills required against the existing skills to do the job? 4. Are clients and the IT group involved in the reviews at the project's gates and subsequent decisions on the project's future? 5. Are there processes for evaluating the impact of project scope changes? |  | |  |
| 2.6 | Conclude on sub-criteria 2. |  | |  |

| Step | Description | Done by | Reference | |
| --- | --- | --- | --- | --- |
| **3 Information systems are available and usable when required, and are designed appropriately to resist attacks and recover from failures.** | | | | |
| 3.1 | Refer to the list of documents and review those referenced to this section.  Review the IT Security Policies to ascertain if the following areas are covered:   1. Identity management, user account management, security testing, monitoring, security incident definition, protection of security technology, network security, malicious software prevention, detection and correction. 2. If a Security Committee is in place review the terms of reference and minutes of meetings. 3. If no committee is in place enquire how security matters are communicated to management. |  | |  |
| 3.2 | Through discussion with IT management and the Security Officer, obtain an understanding of the information security program and its governance. Consider the following:   1. Does the organization have an approved IT Security policy? 2. What standards are the entity security policies referenced to? (eg. ISO17799, GSP) 3. Is there a security awareness program? Are both IT and non-IT staff informed regarding security policies and guidelines? 4. Are there reports that summarize the results of the monitoring program? Who reviews them and are significant issues escalated? 5. How often does senior management get involved in progressing security solutions? 6. Would people recognise a security incident when they saw one? Would they know what to do about it? 7. Is there an incident management system in place? If not how does the organization know if there have been attempted attacks or intrusions? 8. How are incidents monitored and reported and to whom? 9. Are there policies in place that ensure that Information is available and disclosed to only those who have a right to know and is protected against unauthorized modification? 10. Are there appropriate policies and procedures in relation to retention of electronic records? 11. How does the organization know that its systems are in compliance with relevant laws and regulations? (Privacy, Copyright, etc.) 12. How has the entity mitigated any IT risks identified? |  | |  |
| 3.3 | Through discussion with the IT Management obtain an understanding of the IT continuity program. Consider the following:   1. Is there an up to date IT DRP that covers applications, systems, networks and data? 2. When was the IT Disaster Recovery Plan last tested? 3. Is there a list of critical IT resources and are they ranked in priority for recovery purposes? 4. Are there the required tools and processes to perform a frequent backup on data and operating software? 5. What scope of event is assumed for the continuity plan (major disruption with no IT resources available or only minor disruption with all IT resources available)? 6. Have recovery time objectives been established for all corporate services and functional areas? 7. Is there a documented escalation process that shows how continuity plans are invoked? 8. Is there an offsite critical backup media storage facility? How is this site managed and have back-ups been tested for recovery? |  | |  |
| 3.4 | Conclude on sub-criteria 3. |  | |  |

| Step | Description | Done by | Reference | |
| --- | --- | --- | --- | --- |
| **4 IM/IT activities provide quality customer service while ensuring the efficiency and effectiveness of processes and operations.** | | | | |
| 4.1 | Refer to the list of documents and review those referenced to this section. |  | |  |
| 4.2 | Through discussion with Information Systems Management, obtain an understanding of practices employed to ensure quality customer service. Consider the following:   1. Is there an appropriate level of internal business client direction and involvement in IT? 2. Do formal service level agreements covering at a minimum: availability, reliability, performance, capacity for growth, levels of support required for users, continuity planning and security exist? 3. How does the organization monitor and report on the achievement of the specified service criteria and the problems encountered? 4. Is there a service improvement program in place to pursue cost justified improvements in service levels? 5. Is there a framework and are processes in place to ensure compliance with legal, regulatory and other standards? (Sensitivity Analysis in the TRA, License Management, Security Clearance) |  | |  |
| 4.3 | Through discussion with IT Management and consultation of related documents, obtain an understanding of the practices in place to address situations where the organisation outsource some IT system and/or services. Consider the following:   1. Are there documented procedures and a methodology for selecting and managing third party suppliers? Are they followed? 2. Are contractual arrangements with third parties reviewed by appropriate parties? 3. Are third party service level agreements clearly articulated? How is the performance of third party service providers monitored? 4. Are the third parties required to adhere to security and confidentiality standards? 5. Does the IT Group or internal audit perform appropriate audits of third party services? |  | |  |
| 4.4 | Through review of related documents such as contracts and discussion with the IT Project Manager, obtain an understanding of the process for the on going monitoring of service delivery by third parties working on entity projects. Consider the following:   1. Do the third parties involved in the development have a strategy and plan for knowledge transfer to the internal resources? 2. Does the transition plan guarantee appropriate maintenance and enhancements of the system in the future? 3. Are post-mortems and closure documents defined for the sub-projects or for similar projects? |  | |  |
| 4.5 | Conclude on sub-criteria 4. |  | |  |

# Appendix – List of Requested Documents for Special Examination Risk Assessment for Information Technology (IT)

| **Documents** | | **Ref.** | **Comments** |
| --- | --- | --- | --- |
| 1 | IT Strategic Plan | **1** |  |
| 2 | IT Operational and Capital Budgets (current year and multi-year) | **1, 2** |  |
| 3 | Governance structure related to IT (key committees, TOR and sampling of minutes) | **1** |  |
| 4 | Statistics / Metrics used to evaluate the performance of IT Services | **1** |  |
| 5 | Most recent organization chart and job descriptions of senior IT personnel | **1** |  |
| 6 | Corporate wide-Threat and Risk Assessment | **1** |  |
| 7 | IT-Threat and Risk Assessment | **1** |  |
| 8 | Business impact Analysis (Overall and /or individual application or systems) | **3** |  |
| 9 | Impact analysis of laws and regulations on IT processes (i.e. privacy, electronic commerce, intellectual property..) - Overall and /or individual applications or systems | **3.2** |  |
| 10 | Vulnerability assessment /penetration testing reports(Overall and /or individual application or systems) | **3** |  |
| 11 | Procedures for IT incident handling | **3** |  |
| 12 | Organization’s Business Continuity plan/ evidence of update | **3** |  |
| 13 | Test result of Business continuity plan testing / most recent results | **3** |  |
| 14 | IT Disaster Recovery Plan / evidence of update and most recent plan testing results | **3** |  |
| 15 | IT policies and procedures for electronic data handling, classification and retention. | **3.2** |  |
| 16 | Security Policies / Security Awareness Training Materials | **3** |  |
| 17 | Recent Network Flowchart - Overview | **4** |  |
| 18 | Inventory of key applications (identify those that are mission-critical) | **2, 3** |  |
| 19 | IT project development methodology | **2** |  |
| 20 | IT Contracts (Outsourcing of services)  eg. Web Hosting, ISP, Help Desk, E-commerce, etc. | **4** |  |