Generic Valuation Tool

Information Technology

Recordkeeping Liaison Centre
Library and Archives Canada
Telephone: 819-934-7519 or 1-866-498-1148 (toll free in Canada and the US)
Email: bac.centredeliaison-liaisoncentre.lac@canada.ca

Generic Valuation Tool (GVT)
INFORMATION TECHNOLOGY (IT)

How to use this tool:

- This tool is designed for IM specialists to use with relevant business areas when identifying information resources of business value (IRBV) and retention specifications.
- The IRBV and retention specifications contained in this document are recommendations only and should be customized to apply in each institutional context. The complete document should be read before using any recommendations.
- **This GVT does not provide Government of Canada institutions with the authority to dispose of information.** GVTs are not Records Disposition Authorities (RDA) and do not replace the Multi-Institutional Disposition Authorities (MIDA).

Validation: The business processes and IRBV of this GVT have been validated by subject matter experts from the following departments: Shared Services Canada (Spring 2014).

Defining the Activity

Information Technology Services are identified at the sub-program level of the Treasury Board Secretariat's (TBS) *Guide on Internal Services Expenditures: Recording, Reporting and Attributing*[1] (Guide) and are common across the Government of Canada (GC). Information Technology Services involve activities undertaken to achieve efficient and effective use of information technology to support government priorities and program delivery, to increase productivity, and to enhance services to the public. The management of information technology includes planning, building (or procuring), operating and measuring performance[2].

Information technology (IT) plays an important role in government operations, and is a key enabler in transforming the business of government. Information Technology is an essential component of the government's strategy to address challenges of increasing productivity and enhancing services to the public for the benefit of citizens, businesses, taxpayers and employees[3].

The creation of Shared Services Canada has resulted in some of the activities described below no longer being performed in certain organizations. However this GVT

---

1 http://publiservice.tbs-sct.gc.ca/mrrs-sgrr/about-apropos/instructions-consignes/docs/services-eng.asp#Toc6 If the hyperlink does not work, please contact im-gi@tbs-sct.gc.ca to request a copy of the document.

2 ibid

3 http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12755&section=text

includes all of the activities listed in the *Profile of Information Technology Services*[4] and departments are urged to use it for the IT related business processes that remain within their departments.

This tool may be used as a starting point for those organizations mandated to perform IT, or IT related services as they proceed with the identification of their IRBVs. In these cases, the business processes as defined in this GVT must be carefully compared to the processes undertaken within these organizations to ensure they are suitably aligned and address any additional activities that may be conducted.

Relationship to Other GVTs
Business processes and activities often overlap. When the IRBV from an activity is identified in another GVT, there is a note in the table of IRBV and retention recommendations (below) to direct the user to the proper tool.

Management and Oversight: There is a strong relationship between the Management and Oversight GVT and the management of information technology. Many of the high level planning processes are already identified under the planning section of management and oversight, as is the development of all policies relating to operations. Additionally, IRBV created in the investment planning activities seen below in section 3.5 (IT Financial Management) are also captured in Management and Oversight.

Human Resources Management: As is commonly found in the internal services, training and disciplinary actions are common business processes that organizations undertake, and to maintain consistency in the management of IRBVs, these particular processes are found in the Human Resources Management GVT.

Communication Services: The communication of notices to staff of software or hardware updates or security notices are a common occurrence in the management of information technology, however, all IRBV related to this process are located in the Internal Communications section of the Communications Services GVT. Additionally, all a activities surrounding the collection and use of information resources related to web analytics are addressed in the Communication Services GVT.

Acquisition Services: The management of information technology involves the procurement of the hardware and software necessary for the organization to carry out its mandate. All activities related to the acquisition of new hardware and software, or the contracting of services to develop hardware or software are addressed in the Acquisition Services GVT.

---

[4] http://www.tbs-sct.gc.ca/cio-dpi/webapps/technology/profil/profil00-eng.asp

Materiel Management: As many of the operational activities of managing information technology also involves the management of the physical objects (servers, desktop or laptop computers, telephones, etc.), all activities related to the physical management (maintenance, disposal) of these items is located in the Materiel Management GVT.

Financial Management: The financial management process within IT have considerable overlap with the Financial Management GVT; the preparation of budgets, accounting summaries, etc. will all be captured in the Financial Management GVT. However, there are some elements of financial management within the management of information technology that are not captured in Financial Management, such as the setting of costing levels which are unique to IT, and remain within this tool.

Business Processes

The *Profile of Information Technology Services* (June 2008) is a TBS guideline that "provides an enterprise view and reference point for GC's IT Programs that supports the development of consistent IT service descriptions and the basis for common planning, design and communications of GC IT Services across government."[5]. The Profile describes both service groupings and business processes for IT, but places more emphasis on the service groupings rather than the processes; for the purposes of this document, that emphasis has been altered and the focus is on the processes and the IRBV created in order to provide clear guidance to users. As per the Directive on Management of Information Technology[6], departments are to develop and maintain efficient and effective departmental IT practices as informed by Information Technology Infrastructure Library for Service Management (ITIL[7]) and Control Objectives for Information and Related Technology (COBIT[8]). Accordingly, the processes outlined in this document have been modelled on those described under ITIL and COBIT with additions to conform to TBS policy and procedure.

The Profile of Information Technology Services groups the processes into three broad categories: IT Program Management Process, IT Service Delivery Processes and IT Service Support Process. These broad groupings and the detailed processes described under them form the basis for the management of IT.

---

5 http://www.tbs-sct.gc.ca/cio-dpi/webapps/technology/profil/profil02-eng.asp
6 http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?section=text&id=15249
7 ITIL is a set of processes for IT service management; it underpins ISO/IEC 20000, and is copyrighted by HM Government (United Kingdom).
8 COBIT is a framework created by ISACA for information technology governance. ISACA is an international professional association focused on IT governance.

The business processes listed below may not be performed by all service groupings, or they may not be performed in the order laid out here; however, these processes form a collective image for how IT is managed.

IT Services Program Management Processes[9]
This group of program management functions is dedicated to managing the direction, investment, and overall performance of the program. The IT Services Program Management Processes fall into three groups:

1. Plan and Organize:
This business process sets the direction and objectives for the IT services program. It also includes the processes required to manage the resources common to the program. Processes within this group include define a strategic IT plan; define the enterprise architecture; determine technological direction; define the IT processes, organisation and relationships; manage the IT investment; communicate management aims and direction; manage IT human resources; manage quality; assess and manage IT risks; and manage projects.

2. Acquire and Implement:
This business process develops and/or acquires and implements IT solutions and their enhancements or maintenance. Processes in this group include identify automated solutions; acquire and maintain application software; acquire and maintain technology infrastructure; enable operation and use (including user training); procure IT resources; manage program changes; and install and accredit solutions and changes.

3. Monitor and Evaluate:
This business process monitors and evaluates the overall effectiveness of an IT services program. Processes in this group include monitor and evaluate IT performance; monitor and evaluate internal control; ensure regulatory compliance; and provide IT governance.

IT Service Delivery Processes
This group of processes focuses on service-specific planning, provisioning, delivery, continuity, security and decommissioning processes for the services provided by the program.

4. Service Level Management:
Service Level Management involves the processes of planning, coordinating and reporting on Service Level Agreements (SLAs) between the IT service provider and customer/client group and the ongoing review of service achievements to ensure that

---

9 http://www.tbs-sct.gc.ca/cio-dpi/webapps/technology/profil/profil02-eng.asp

service levels and quality are consistently delivered and maintained. Service Level Management should seek to ensure the quality of IT services by aligning technology with business processes in a way that is cost effective.

5. IT Financial Management:
IT Financial Management involves three main processes - budgeting, accounting, and cost recovery charging – to ensure the cost-effective stewardship of IT assets and resources used in providing IT services. Charging is an optional activity and is dependent on the charging policy of the organisation as a whole. The main objective of financial management is to evaluate and control the costs associated with IT services while customers are still offered a high quality of service and there is efficient use of the necessary IT resources.

6. Availability Management:
Availability Management is concerned with the design, implementation, measurement and management of the IT infrastructure to ensure the business requirements are consistently met, according to agreed levels. It is responsible for optimising and monitoring IT services so they can function reliably and without interruption so as to comply with service level agreements at a reasonable cost.

7. Capacity Management:
Capacity Management is the focal point for all IT performance and capacity issues. Capacity Management aims to optimize the amount of capacity needed to deliver a consistent level of current and future services. Capacity management ensures that the information technology processing and storage capacity is adequate to the evolving requirements of the organization as a whole in a timely and cost justifiable manner.

8. IT Service Continuity Management:
IT Service Continuity Management involves undertaking a systematic approach to the creation of a plan and or set of procedures (which are updated and tested regularly) used to prevent, cope with, and recover from the loss of critical services for extended periods, in line with business continuity plans. It is concerned with preventing any unexpected serious interruptions to IT services as a result of natural disasters or system attacks which may have a catastrophic impact on business. The processes captured in this activity only relate to IT, not organization wide business continuity planning.

9. IT Security Management:
IT Security Management involves organizing the collection, storage, handling, processing and management of data and services in such a way that the integrity, availability, and confidentiality of business conditions are satisfied. Security

management activities must ensure that the electronic information is correct and complete, that it is always available for business purposes and is only used by those who are authorized to do so. In the GC, IT security management is a distinct process from the management of personnel and building security, the processes described here relate only to security for information technology.

IT Service Support Processes:
This group of processes focuses on the day-to-day operational services common to all IT services, and are 'visible' to clients/users. They include service/help desk processes which interact directly with IT program customers

10. Service/Help Desk:
The Service/Help Desk is the single contact point within the organization for all users to seek assistance and support for IT services and/or related problems, incidents, questions, and complaints.

11. Incident Management:
The primary goal of the Incident Management process is to restore normal service as quickly as possible following loss of service, and to minimize the adverse impact on business operations, thus ensuring that the best possible levels of service quality and availability are maintained.

Section 18 of the *Operational Security Standard: Management of Information Technology Security*[10] relates explicitly to response and recovery for IT security incidents and provides details on the actions a department is to take in the event of an IT security incident as well as a listing of the information resources a department is required to keep in the event of an incident. Section 18.3 states that "Departments must maintain operational records that show how incidents were handled, documenting the chain of events during the incident, noting the time when the incident was detected; the actions taken; the rationale for decisions; details of communications; management approval or direction; and external or internal reports"[11]. These requirements are not listed as individual IRBV, but it is anticipated that they will be captured as elements within the various IRBV.

12. Problem Management:
The goal of Problem Management is to minimize the adverse impact of incidents and problems on the business that may be caused by errors within the IT infrastructure, and

---

10 http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12328&section=text
11 ibid

to prevent recurrence of incidents related to these errors. Activities undertaken to find and analyse the underlying cause of a particular incident are addressed here.

13. Change Management:
The goal of Change Management is to ensure that standardized methods and procedures are used for the efficient and prompt handling of all changes, to minimize the impact of change-related incidents and improve day-to-day operations. Change management evaluates and plans the change processes to ensure that if a change is made, it is done in the most efficient way possible, following established procedures and ensuring the quality and continuity of the IT service at all times.

14. Release Management:
Release Management is very closely linked with Configuration Management and Change Management, and undertakes the planning, design, build, and testing of hardware and software to ensure that all aspects of a release, both technical and non-technical, are considered together. Release management is responsible for the implementation and quality control of all hardware and software installed on the live environment.

15. Configuration Management:
Configuration Management covers the identification of significant components within the IT infrastructure and recording details of these components in the Configuration Management Database (CMDB). The main task for configuration management is to keep an up-to-date record of all the components in the IT infrastructure configuration and the interrelationships between them.

Retention
Recommended retention specifications in GVTs are determined based on traditional or best practices, a review of government-wide legislation and policy, and validation with subject matter experts. Retention periods are suggestions only; departments must take into account their own legislative requirements and business needs.

Business Value and Retention Recommendations

1. Plan and Organize

Business Processes	Recommendations: Information Resources of Business Value (IRBVs)	Recommendations: Retention Period
Define strategic IT plan **Determine the technological direction** **Manage IT investment** **Assess and manage IT risks** **Manage projects**	*For IRBV please see Management and Oversight GVT*	*For retention please see Management and Oversight GVT*
Define the enterprise architecture **Identify and categorize IT assets** **Define the IT work processes, organization and relationships**	Enterprise architecture maps List of IT Services and systems IT process maps	2 years after last administrative action
Manage IT human resources	*For IRBV please see Human Resources Management GVT*	*For retention please see Human Resources Management GVT*
Communicate management aims and direction	*For IRBV please see Communications Services GVT*	*For retention please see Communications Services GVT*

2. Acquire and Implement

Business Processes	Recommendations: Information Resources of Business Value (IRBVs)	Recommendations: Retention Period
Enable operation and use (including user training)	*For IRBV please see Human Resources Management GVT*	*For retention please see Human Resources Management GVT*
Acquire technology infrastructure **Acquire software** **Procure IT resources**	*For IRBV please see Acquisitions GVT*	*For retention please see Acquisitions GVT*

Business Processes	Recommendations: Information Resources of Business Value (IRBVs)	Recommendations: Retention Period
Maintain technology infrastructure **Maintain software**	*For IRBV please see Materiel Management GVT*	*For retention please see Materiel Management GVT*

3. Monitor and Evaluate

Business Processes	Recommendations: Information Resources of Business Value (IRBVs)	Recommendations: Retention Period
Monitor IT performance **Monitor internal controls (inventory, physical access, logical access)** **Ensure compliance with international standards** **Report to TBS names of officers involved in standards activities**	Performance reports Reports on internal control systems List of officer names and responsibilities	2 years after last administrative action
Provide IT governance	*For IRBV please see Management and Oversight GVT*	*For retention please see Management and Oversight GVT*

4. Service Level Management

Business Processes	Recommendations: Information Resources of Business Value (IRBVs)	Recommendations: Retention Period
Plan Service Level Agreements Identify IT services and service requirements Define, build and manage the IT Service Catalog	Catalogue of services Service level requirements Service specification sheets	2 years after last administrative action

Define, build and negotiate Service Level Agreements (SLAs) Define, build and negotiate Operational Level Agreements (OLAs) Prepare Service Level Requirements (SLR), Service Specification Sheets, and Service Quality Plans (SQP) Identify Underpinning Contract service requirements (UCs) Coordinate and implement Service Level Agreements	Service Level Agreements Operational level agreements Memorandum of Understanding Underpinning contract service requirements Service quality plans	
Report on Service Level Agreements Review service achievements Preparing performance reports. Monitor and manage SLAs, OLAs and UCs Preparing Service Improvement Programmes (**SIP**) Provide management information about Service Level Management quality and operations	Performance Statistics Reports Progress, Benchmark or Monitoring Reports Improvement Plans	2 years after last administrative action

5. IT Financial management

Business Processes	Recommendations: Information Resources of Business Value (IRBVs)	Recommendations: Retention Period
Budget Undertake budgeting for IT services	*For IRBV please see Financial Management GVT*	*For retention please see Financial Management GVT*
Account Identify costs	*For IRBV please see Financial Management GVT*	*For retention please see Financial Management GVT*

Define cost elements Monitor costs Perform IT charging and billing activities		
Charge Define a price setting policy	*For IRBV please see Management and Oversight GVT*	*For retention please see Financial Management GVT*
Establish a tariff for services provided or products offered	Tariff lists	6 years after the end of the fiscal year to which the resource corresponds

6. Availability Management

Business Processes	Recommendations: Information Resources of Business Value (IRBVs)	Recommendations: Retention Period
Design infrastructure availability Determine availability requirements Compile availability plans	Availability Plan Metrics for service interruptions Notices to clients of service interruptions	2 years after last administrative action
Implement infrastructure availability Run diagnostics on the availability of systems and services.	Diagnostic reports	2 years after last administrative action
Measure infrastructure availability Monitor availability Monitor maintenance obligations	Availability Reports	2 years after last administrative action
Manage IT infrastructure availability Report on Incident management quality and operations Prepare progress reports	Progress reports Component Failure Impact Analysis Failure Tree Analysis Service Outage Analysis	2 years after last administrative action

Evaluate the impact of security policies on availability Advise Change Management about the possible impact of a change on availability	Notifications to Change Management	

7. Capacity Management

Business Processes	Recommendations: Information Resources of Business Value (IRBVs)	Recommendations: Retention Period
Develop the Capacity Plan **Model and simulate various capacity scenarios** **Monitor the use and performance of the IT infrastructure** **Solve problems caused by the degradation of service due to increases in demand and partial interruptions to service due to hardware or software faults** **Create and maintain the Capacity Database (CDB)** **Implement capacity-related changes**	Capacity plan Capacity database Input into Service Level Agreements Evaluations of the IT infrastructure Request for change Capacity Management Performance Reports	2 years after last administrative action

8. IT Service Continuity Management

Business Processes	Recommendations: Information Resources of Business Value (IRBVs)	Recommendations: Retention Period
Define scope of IT Service Continuity Management **Conduct Business Impact Analysis**	IT Service continuity management policy Risk assessment on IT infrastructure	2 years after last administrative action

Conduct IT Risk Assessment. **Create IT business continuity plan and procedures** **Define IT Service Continuity Strategy in line with Business Continuity strategy** **Perform IT Service Continuity organization and implementation planning activities** **Implement standby arrangements and risk reduction measures** **Develop IT recovery plans and procedures** **Perform Testing of IT recovery plans and procedures** **Revise plans following changes to the IT infrastructure** **Validate ongoing ability of IT Service Continuity strategies to meet business requirements** **Provide management information about IT Service Continuity**	Risk prevention plan Emergency management plan (for IT) Business resumption plan (for IT) (Disaster) Recovery plan (for IT) Information resources informing users of an interruption or service degradation, procedures and protocols in the case of an incident Changed plans as a result of changed infrastructure Risk analysis reports Risk analysis assessments Disaster drill evaluations Reports on costs associates with prevention and recovery plans Prevention and recovery procedures	
Perform IT Service Continuity educational training and awareness activities	*For IRBV please see Human Resources Management GVT*	*For retention please see Human Resources Management GVT*
Review and audit IT recovery plans and procedures	*For IRBV please see Management and Oversight*	*For retention please see Management and Oversight*

9. IT Security (risk) Management

Business Processes	Recommendations: Information Resources of Business Value (IRBVs)	Recommendations: Retention Period

Plan Establish Security Policy or Standards (response procedures) Create Security Plan	*For IRBV please see Management and Oversight GVT*	*For retention please see Management and Oversight GVT*
Request of CSE to review departmental security procedures and telecommunications systems	Management of Information Technology Self-Assessment Correspondence with CSE (request) Action plan resulting from CSE review Schedule of changes resulting from CSE review	2 years after last administrative action
Share and exchange IT assets	Written security arrangements	2 years after last administrative action
Assess Conduct threat and risk assessment Certify and or accredit systems or services Review Requests for Proposals, and other contracting documentation when IT security is implicated	Incident reports Threat and Risk Assessment Privacy Impact Assessment Vulnerability Assessment Business Impact Assessment Statement of Sensitivity Comments on requests for proposals	2 years after last administrative action
Implement Implement the Security Plan Appoint a COMSEC custodian Coordinate implementation of IT Security Management people, process and technologies Maintain Security Management people, processes and technical infrastructure	Implementation reports Notification to TBS of COMSEC custodian contact information	2 years after last administrative action

Implement training on security measures	*For IRBV please see* *Human Resources Management GVT*	*For retention please see* *Human Resources Management GVT*
Monitor Monitor and evaluate compliance with the plan Review all policies with security implications Supervise the levels of security by analysing trends, new risks and vulnerabilities Notify staff of security risks Monitor compliance with the TBS policy "Operational Security Standard: Management of Information Technology Security (MITS)"	Compliance monitoring reports and evaluations Copies of Security audit reports Requests for change as a result of the audit/self-assessment Communications with staff regarding security risks	2 years after last administrative action
Respond Incident response coordination Incident reporting	Incident reports	2 years after last administrative action
Take sanctions when contraventions to IT policy occur	*For IRBV please see* *Human Resources Management GVT*	*For retention please see* *Human Resources Management GVT*
Report Monitor the networks and online services to detect intruders and attacks Provide management information about Security Management quality and operations	Monitoring reports	2 years after last administrative action
Evaluate and audit the Security Management supporting infrastructure	*For IRBV please see* *Management and Oversight GVT*	*For retention please see* *Management and Oversight GVT*

10. Service / Help Desk

Business Processes	Recommendations: Information Resources of Business Value (IRBVs)	Recommendations: Retention Period
Log and monitor incidents **Prepare incident reports/responses** **Classify problem and document diagnosis** **Apply temporary solutions to known errors in collaboration with Problem Management** **Work with Configuration Management to ensure that the relevant databases are up-to-date** **Manage changes requested through service requests in collaboration with Change Management and Version Management** **Check that the support service required is included in the associated service level agreement** **Communicate with users** **Notify IT Security Coordinator when a security related issue has been reported** **Close the incident**	Call log / Operational events log / database Incident / issue reports Notification to Security Coordinator	2 years after last administrative action

11. Incident Management

Business Processes	Recommendations: Information Resources of Business Value (IRBVs)	Recommendations: Retention Period
Plan	Copy of contact information provided to TBS / Public Safety (IT Security	2 years after last administrative action

Establish mechanisms to respond to IT incidents and to exchange information with designated lead departments Establish procedure for notifying the appropriate operational personnel of incidents Communicate bulletins and advisories to staff as necessary	Coordinator/designate and secondary contact) Up to date contact lists Copies of RCMP IT bulletins Copies of CSE information bulletins and advisories Copies of communications to staff	
Identify Detect and record incidents Classify incidents Provide initial incident support	Results from incident detection tools Monitoring logs Incident log / database	2 years after last administrative action
Respond Investigate and diagnose incidents Resolve incidents and recover service per agreed service levels Close incidents	Incident response procedures Documentation regarding the management of incidents including: Details of incident Actions taken Rationale for decisions Communications Management approval or direction Internal and external reports	2 years after last administrative action
Report Report incidents or threats Participate in threat and risk briefings or teleconferences Consult legal services when suspicion of criminal activity	Incident or threat report Correspondence with Public Safety on incident or threat Notification to appropriate Law Enforcement Agency Correspondence with legal services Notice to users Request for change resulting from an incident	2 years after last administrative action

Recover Perform regular backups of all systems (data, software, configuration data) Test backups Develop restoration procedures Test restoration procedures Determine retention periods Document arrangements for off-site backup (3rd parties) Communicate with Public Safety as necessary	Backup tapes Restoration procedures Documentation of retention periods Agreements with 3rd parties Correspondence with Public Safety	2 years after last administrative action
Analyze Provide management information about Incident Management quality and operations	Incident Closure and Evaluation Report Post incident analysis	2 years after last administrative action

12. Problem Management

Business Processes	Recommendations: Information Resources of Business Value (IRBVs)	Recommendations: Retention Period
Investigate the underlying causes of any real or potential anomalies in the IT service. **Define possible solutions to anomalies.** **Submit requests for changes needed to re-establish quality of service.** **Conduct post-implementation reviews**	Incident database Problem log Problem (management) record Analysis reports on infrastructure Requests for change Knowledge base (database) Reports on classified incidents Post implementation reviews	2 years after last administrative action

13. Change Management

Business Processes	Recommendations: Information Resources of Business Value (IRBVs)	Recommendations: Retention Period
Develop Change Management Policy	*For IRBV please see Management and Oversight GVT*	*For retention please see Management and Oversight GVT*
Monitor and direct the change process **Record, evaluate and accept or reject the requests for changes received** **Hold meetings of the Change Advisory Board** **Coordinate the development and implementation of the change** **Evaluate the results of the change** **Close the change**	Approved and rejected requests for change (authorization, documentation and control of changes) Revised approved request for change Change log Hardware configuration chart Change Advisory Board Terms of Reference, roles and responsibilities Change Advisory Board records of decision Schedule of changes Evaluation reports	2 years after last administrative action

14. Release Management

Business Processes	Recommendations: Information Resources of Business Value (IRBVs)	Recommendations: Retention Period
Establish a planning policy for the implementation of new versions	*For IRBV please see Management and Oversight GVT*	*For retention please see Management and Oversight GVT*
Purchase or build new software	*For IRBV please see Acquisitions GVT* – for purchase of new software or contracting out the build of software when not performed in	*For retention please see Acquisitions GVT*

	house	
Test new versions in an environment that simulates the live environment as closely as possible **Validate the new versions** **Implement new versions in the live environment** **Carry out back-out plans to remove the new version if necessary** **Update the Definitive software library, the Definitive hardware storage and the Configuration Database** **Inform and train users about the functionality of the newly released version**	Definitive software library (inventory) Definitive hardware storage (inventory) Configuration Database Version implementation policy Back-out plan Testing reports Test protocol User acceptance testing case studies Reports from UAT Implementation/release schedule Release/rollout plan Release/rollout procedure Communication with Service Desk Communications with users Training materials Reports on release/rollout	2 years after last administrative action

15. Configuration Management

Business Processes	Recommendations: Information Resources of Business Value (IRBVs)	Recommendations: Retention Period
Identify items within the information technology infrastructure **Record items in the IT infrastructure in the configuration management database** **Monitor items in the configuration management database**	Configuration management database including a register of software licenses Reports on the configuration management database	2 years after last administrative action

Report on items in the configuration management database		