Information and Communications Technology Controls Guide

Foreword

This guide has been developed to assist organisations with identifying areas for improvement regarding their information and communications technology (ICT) controls. It draws on the work undertaken in ICT controls-based audits across the Victorian public sector. It is designed to promote more robust practices and to enhance the ICT control environments at public sector organisations. ICT controls should form part of each organisations' broader security considerations, that should address both internal and external threats and risks. This guide does not replace the standards and guidelines which Victorian public sector organisations must comply with, but rather it complements them.

Public sector organisations are encouraged to assess their ICT control environments against this better practice guide, and use the results to improve their practices.

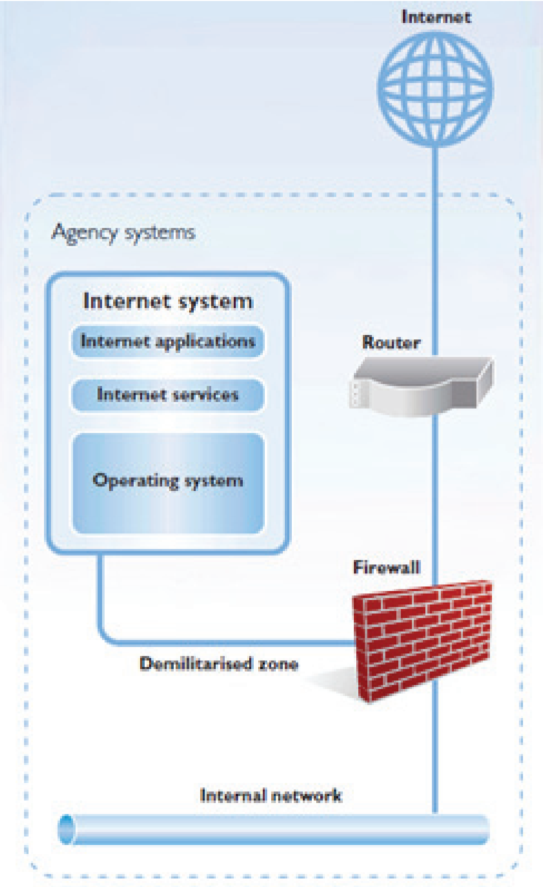
Dr Peter Frost
Acting Auditor-General

February 2016

VAGO
Victorian Auditor-General's Office

The importance of ICT controls

Public sector organisations increasingly use complex and interconnected ICT systems to deliver services to Victorians, and therefore it is vital that they have effective and appropriate controls in place. A conceptual example is illustrated below.



ICT systems

An ICT system is a collection of computer hardware and programs that work together to support business and operational processes. ICT systems are primarily made up of three core components:

- Operating system—core programs that run on the ICT hardware that enable other programs to work. Examples of operating systems include Microsoft Windows, Unix and IBM OS/400.
- Databases—programs that organise and store data. Examples of database software include Oracle database and Microsoft SQL Server.
- Applications—programs that deliver business and operational requirements. Examples of applications include Oracle E-business suite, SAP and TechnologyOne.

These components are typically supported by an organisation's network infrastructure.

ICT controls

ICT controls are policies, procedures and activities put in place by an organisation to ensure the confidentiality, integrity and availability of its ICT systems and data.

ICT controls include the establishment and adherence to appropriate structures for managing:

- organisational governance
- system security
- ICT operations and architecture
- change and release
- system development and implementation
- backup and recovery.

Information and Communications Technology Controls Guide
Published by the Victorian Auditor-General's Office,
Level 24, 35 Collins Street, Melbourne.
www.audit.vic.gov.au
ISBN 978 1 925226 49 2
February 2016

recovery systems solutions

ICT controls checklist

Organisational governance

Industry / recommended practice [control]	**Practice met**	**Action plan**	**Target date**
The organisation is aware of its current and upcoming ICT **compliance obligations**, where applicable. (e.g. Victorian Protective Data Security Standards, Australian Government Information Security Manual (ISM), ISO/IEC 27001 - Information security management, Payment Card Industry Data Security Standard (PCI-DSS) etc.)	☐ Yes ☐ Partially ☐ No		
The organisation has appropriate and detailed **strategies, policies, procedures and standards** in place that: • provide guidance on the management of its ICT operations and processes • adhere to compliance requirements and/or include robust standards.	☐ Yes ☐ Partially ☐ No		
The organisation's **strategies, policies, procedures and standards** include, but are not limited to, coverage over: • ICT security management • user access management • patch management • change and release management • network operations, auditing and monitoring management • backup and disaster recovery management.	☐ Yes ☐ Partially ☐ No		
The organisation's **strategies, policies, procedures and standards** are: • approved by senior management • reviewed periodically to ensure they remain current and applicable.	☐ Yes ☐ Partially ☐ No		
The organisation has **current contracts** in place with its ICT vendors and service providers.	☐ Yes ☐ Partially ☐ No		

Organisational governance – continued

Industry / recommended practice [control]	**Practice met**	**Action plan**	**Target date**
All **ICT risks** to the organisation and/or instances of noncompliance with its policy requirements are rated and included in a risk register. Also: • action plans and owners are assigned to each risk • the risk register is reviewed periodically.	□ Yes □ Partially □ No		
An **ICT Steering Committee** (or equivalent) convenes periodically to oversee the organisation's strategic initiatives, operations, and the ongoing management and mitigation of its risks. This group is also an escalation point as part of the organisation's incident management process.	□ Yes □ Partially □ No		

System security

ICT systems refer to any technical utilities that hosts, maintains, and/or transmits data. These include, but are not limited to applications, databases, operating systems, networks and hardware.

Industry / recommended practice [control]	**Practice met**	**Action plan**	**Target date**
Password and account lockout settings for access to ICT systems are implemented in accordance with the organisation's policies and compliance requirements (where applicable). These requirements are enforceable over all accounts.	□ Yes □ Partially □ No		
Access to ICT system and data are appropriately restricted. In particular: • privileged access is limited to only user, system and service accounts requiring this access in line with their current roles • system and service accounts are configured to be non interactive (i.e. these accounts cannot be used to log in to the system).	□ Yes □ Partially □ No		
User onboarding—access to the system is configured in line with the user's current role, and authorised by appropriate management prior to it being provided to the user.	□ Yes □ Partially □ No		

System security – continued

ICT systems refer to any technical utilities that hosts, maintains, and/or transmits data. These include, but are not limited to applications, databases, operating systems, networks and hardware.

Industry / recommended practice **[control]**	**Practice met**	**Action plan**	**Target date**
User offboarding—access to the system is removed at the point at which the user no longer requires access, or terminates their employment with the organisation.	□ Yes □ Partially □ No		
Formal user access reviews for the system are conducted periodically, and signed off by an appropriate management representative.	□ Yes □ Partially □ No		
Active user IDs and system accounts are **uniquely identifiable** and can be attributed to an appropriate user, system or service.	□ Yes □ Partially □ No		
When a **shared account** is used, accountability over the use of it can be effectively attributed to a specific user.	□ Yes □ Partially □ No		
Audit logs for privileged account activities, sensitive operations and processes are maintained and appropriately restricted.	□ Yes □ Partially □ No		
Audit logs for privileged account activities, sensitive operations and processes are periodically reviewed, particularly to detect anomalous activity.	□ Yes □ Partially □ No		
Patches and firmware are applied to ensure that the ICT system is appropriately maintained in line with organisational requirements and the vendor's recommendations.	□ Yes □ Partially □ No		

ICT operations and architecture

Industry / recommended practice **[control]**	**Practice met**	**Action plan**	**Target date**
The organisation is subject to **periodic internal and external facing penetration tests, compliance assessments, and ICT security audits**. The results of these initiatives are included in the risk register.	□ Yes □ Partially □ No		
The organisation's **network is appropriately segmented** both internally and from external traffic (e.g. through the implementations of firewall-type technologies, demilitarised zones).	□ Yes □ Partially □ No		

ICT operations and architecture – continued

Industry / recommended practice [control]	**Practice met**	**Action plan**	**Target date**
Organisation-wide network monitoring, analysis, management and security solutions are in place, appropriately configured and maintained, and actively monitored. These include: • systems operations management utilities • intrusion detection and prevention systems (IDPS) • anti-virus and malware solutions—installed on all systems • mail and web threat protection solutions • data loss prevention (DLP) solution.	□ Yes □ Partially □ No		
Business and system data is protected in transit and at rest by **robust encryption technologies** (e.g. web application-based traffic, database and network repository content).	□ Yes □ Partially □ No		
Insecure, unused, and non-required system services and ports are disabled throughout the environment (e.g. Telnet and File Transfer Protocol).	□ Yes □ Partially □ No		
Key interfaces are monitored to ensure the completeness and integrity of data.	□ Yes □ Partially □ No		
Access to **view and modify interfaces and batch job schedules is restricted** to authorised personnel. This access is periodically reviewed.	□ Yes □ Partially □ No		
Changes to interfaces and batch job schedules are subject to the change management process.	□ Yes □ Partially □ No		
End-user computers have 'locked-down' builds, which restrict users from performing privileged operations within the network. Similarly, users are not assigned local administrator access to their workstations.	□ Yes □ Partially □ No		
The **data centre (server room) is appropriately equipped, managed, monitored and secured.** Access to this environment is restricted only to personnel who require it, and is reviewed periodically.	□ Yes □ Partially □ No		

Change and release

Industry / recommended practice [control]	Practice met	Action plan	Target date
All changes to the organisation's systems (including emergency and patch-related changes) are performed in accordance with its policies and compliance requirements. These requirements are enforceable over all systems.	□ Yes □ Partially □ No		
A **centralised change management repository** is in place, where all changes to the organisation's systems are logged.	□ Yes □ Partially □ No		
Production systems are appropriately segregated from non-production systems (e.g. development and test).	□ Yes □ Partially □ No		
Access to modify the production systems is restricted only to personnel who support it as part of their current role. In particular, personnel who develop proposed solutions do not have access to the production systems.	□ Yes □ Partially □ No		
Changes to systems are **appropriately approved prior to any development activities** being initiated.	□ Yes □ Partially □ No		
All proposed solutions are **subject to formal and robust acceptance testing**, prior to being implemented into production. These include unit, system, and user acceptance testing.	□ Yes □ Partially □ No		
Only **appropriately approved changes are implemented** into the production environment.	□ Yes □ Partially □ No		
Formal post-implementation testing is undertaken to confirm that the changes introduced into production appropriately satisfied the business requirements, and also did not negatively impact current system functionality and performance.	□ Yes □ Partially □ No		
A **configuration management database (CMDB)** has been established. All modifications to configuration items are attributed to an appropriately authorised change request.	□ Yes □ Partially □ No		

System development and implementation

The list below is high level only. Refer to VAGO’s ‘Investing Smarter in Public Sector ICT better practice guide’ for further detail.

Industry / recommended practice [control]	Practice met	Action plan	Target date
Business requirements are defined for all **new system developments and implementations.** Requirements are reviewed and approved by the appropriate management.	□ Yes □ Partially □No		
System technical requirements are defined for all new system developments and implementations. Requirements are reviewed and approved by the appropriate management.	□ Yes □ Partially □ No		
Data conversion mapping and testing is performed for new program developments and implementations to ensure all data is converted completely and accurately.	□ Yes □ Partially □ No		
New systems and major enhancements are approved prior to being migrated into production.	□ Yes □ Partially □ No		
Appropriate test planning and test execution is performed for all new program developments. Implementations are completed by the appropriate personnel and occur subsequent to appropriate acceptance testing.	□ Yes □ Partially □ No		
System issues are identified, reviewed by management and resolved in a timely fashion.	□ Yes □ Partially □ No		

Backup and recovery

Industry / recommended practice [control]	Practice met	Action plan	Target date
The organisation's **backup and recovery operations** over all of its systems are performed in accordance with its policies and compliance requirements. This guidance is formally documented and details backup scope, schedules, frequency, retention and testing requirements.	□ Yes □ Partially □ No		
The **success of data backups is monitored.** Appropriate personnel are alerted in all instances of incomplete or failed backups, and such events are subject to the organisation's incident and escalation management process.	□ Yes □ Partially □ No		
The **ability to effectively recover organisational data from backups** is periodically tested.	□ Yes □ Partially □ No		
An **ICT disaster recovery plan is in place** for all organisational systems and aligns with the organisation's business continuity planning arrangements. The prioritisation of ICT systems is based on a business impact assessment.	□ Yes □ Partially □ No		
ICT disaster recovery plans and strategies for all systems are tested periodically. Remediation actions identified by testing initiatives are tracked and monitored.	□ Yes □ Partially □ No		

Further references and resources

Further guidance on ICT controls and practices is available through resources such as those below:

- Victorian Protective Data Security Standards – *www.cpdp.vic.gov.au*
- The Australian Government Information Security Manual – *www.asd.gov.au/infosec/ism*
- Control Objectives for Information and Related Technology (COBIT) – *cobitonline.isaca.org*
- Information Technology Infrastructure Library (ITIL) – *www.itsmf.org.au/?page=ITILInfrastructure*
- ISO/IEC 27001 - Information security management – *www.iso.org/iso/home/standards/management-standards/iso27001.htm*
- Payment Card Industry Data Security Standard (PCI DSS) – *www.pcisecuritystandards.org/index.php*
- VAGO Investing Smarter in Public Sector ICT better practice guide – *www.audit.vic.gov.au/reports__publications/reports_by_year/2008/20080730_ict_bpg.aspx*