In-Depth Analysis of 2020 General Computer Controls in State Government Entities.

Team Members

Sai Teja Bathula	**S4038096**
Karthik Kothagattu	**S4086579**
Venkatesh Ejjigiri	**S4087244**
Praneeth Reddy Padamati	**S4044197**

Table of Contents

1. Introduction:

1.1 Western Australia Audit General's Report:

The Western Australian Auditor General's Information Systems Audit Report is an annual report assessing information systems of state government departments, institutions, and relevant tertiary institutions in the western Australian public sector. The audit emphasizes general computer controls (GCCs), which are critical control activities that enable organizations to support and protect IT systems. GCCs encompass activities intended to safeguard information, address risks, and promote organizational reliability.

1.2 Problem Statement:

Weaknesses exposed by the Audit Report in the IT governance framework include information security and business continuity controls. These weaknesses, including the non-current policies and lack of adequate disaster recovery plans, are highly risky for state government entities. The project will target these weaknesses by applying the ISO/IEC 38500 and ISO/IEC 27000 frameworks in the development of solutions towards establishing improvements in IT governance, management of risk, and alignment with organizational objectives.

1.3 Brief on ISO/IEC 38500:

ISO/IEC 38500 is an IT governance standard that gives organizational IT the right guidance in its management. They deal with how to guarantee that its investments support organizational goals and objectives, control risks, and increase value. The standard outlines six principles: responsibility, strategy, acquisition, performance and conformance, a human behavior necessary for fortification of IT governance in the public sector.

1.4 Brief on ISO/IEC 27000 (2018):

ISO/IEC 27000 is perfect in cases where there is a requirement by an organization to have an effective management methodology on information security. As it offers a very correct definition of most of the concepts, terminologies, and principles that turn out to be very useful during the construction of an effective information security management system. This standard is general, flanking various organizations, including business organizations, government, and non-governmental organizations.

1.5 Report Structure:

This report's design is being initiated with an Introduction comprising a brief description of the context of auditing, the key issues highlighted, and the IT governance standards of concern. The Critical Analysis section highlights and particularly emphasizes deficiencies in information security and business continuity, in relation to the principles of ISO/IEC 38500. According to the guidelines provided in the ISO/IEC 27000 series, the Recommendations section enables sensible remedies and guidelines for IT governance. They are concluded by a

Conclusion which distils these and, more pressingly, reminds that the evaluation and monitoring – at periodic time intervals – are needed to maintain effective IT governance.

2. Critical Analysis:

2.1 Information Security:

Here, we use ISO 38500 frameworks to list 7 weaknesses for Information Security and recommendations.

Weakness:	Principle	Definition	Analysis
Outdated or Insufficient Information Security measures	Conformance	IT should support the organization in adhering to all laws and regulations by the existence of well-defined and enforceable policies. [1]	Information security policies should be the most current, covered by relevant regulations and standards that will make an organization's IT environment secure. Outdated policies might not cover new threats, legal issues, or changing technology and thus become exposed.[3]
No assessment of extremely confidential data access to applications, databases, and networks	Responsibility	Everyone within the organization knows their related IT responsibilities and is granted the power to act regarding that role. [1]	Privileged access should be reviewed to ensure access is only granted to pertinent systems and data to mitigate unauthorized actions that may result in a breach of data, data manipulation, or system compromise.[5]
Inadequate procedures for detecting and fixing security flaws in IT Infrastructure	Performance	IT systems and services should meet the organization's needs, give service quality, and lead to business benefits. [1]	IT systems and services should meet the organization's needs, provide high-quality service, and lead to business benefits.
Insufficient awareness programs for employee on Information Security	Human Behaviour	IT decisions need to respect and address the needs and behaviours of people, thus addressing the present and future human behaviours. [1]	If employees are not aware of the security threats and what needs to be done in response to those threats, then they can unknowingly contribute to some security incidents, such as becoming victims of phishing. Awareness programs create a security culture that reduces the likelihood of human error and enhances an organization's security posture.[4]
Inadequate employee training and	Human Behaviour	IT decisions need to respect and address the needs and behaviours of	Human Behaviour in Information security staff training and development focuses on current security threats, protective measures, and best practices, empowering

development programs		people, thus addressing the present and future human behaviours. [1]	every officer to contribute effectively towards security.
Absence of information classification policies or procedures	Strategy	The strategy of the organization considers how IT can help now and, in the future, that IT will meet the needs of the organization. [1]	This means that strategic-level information classification is relevant to the protection of the concerned data about the required level of protection. Without an effective policy in place, an institution may not give required care to sensitive information and therefore may be open to potential loss. Proper classification would balance security measures against data value and sensitivity, ensuring allocation of resources for data protection.
Insufficient password security measures lacking the implementation of multifactor authentication.	Responsibility	Everyone within the organization knows their related IT responsibilities and is granted the power to act about that role. [1]	Organizations must implement effective authentication mechanisms. Poor password controls give no addition of security through MFA and hence open the system to password guessing or theft of valid credentials.

2.2 Business Continuity:

Here, we use ISO frameworks to list 6 weaknesses for Business Continuity and recommendations.

Weakness	**Principle**	**Definition**	**Analysis**
Absence of Business Continuity Plans or Disaster Recovery Plans.	Strategy	The organization has plans about how IT can help now and in the future; it ensures IT meets the needs of the organization. [1]	The organization's neglect in testing Disaster Recovery Plans (DRPs) signifies a shortcoming in verifying their efficacy and the adequacy of recovery procedures in case of disasters, thereby exposing them to unforeseen risks.[6]
DRPs that failed to encompass all essential systems.	Acquisition	IT acquisitions—that is, purchases of hardware, software, and so on—are made for good reasons. Careful analysis of the benefits versus the costs was conducted at the time of purchase, and	The absence of essential systems in the organization's disaster recovery plans suggests a failure to fully recognize their importance in the context of disaster recovery planning, reflecting an insufficient analysis of IT assets.

		regularly reviewed to ensure that such still makes sense. [1]	
Insufficient business impact analysis to effectively prioritize business functions and recovery needs.	Strategy	The organization has plans about how IT can help now and in the future; it ensures IT meets the needs of the organization. [1]	A lack of comprehensive Business Impact Analysis (BIA) may result in a strategic deficiency in recognizing the importance of various business functions, leading recovery initiatives to prioritize less critical areas and resulting in business interruptions.
Outdated and unnecessary Disaster Recovery Plans (DRPs) that do not accurately represent the current information and communication technology (ICT) infrastructure.	Responsibility	Everybody in the organization knows their IT-related responsibilities and has the authority to perform their role. [1]	The obsolete and unnecessary Disaster Recovery Plans (DRPs) reflect a deficiency in accountability and oversight regarding the maintenance of up-to-date recovery strategies and their alignment with the current ICT infrastructure.
Unverified Disaster Recovery Plans and organizations lack awareness of their ability to restore systems.	Responsibility	Everybody in the organization knows their IT-related responsibilities and has the authority to perform their role. [1]	The organization's neglect in testing Disaster Recovery Plans (DRPs) signifies a shortcoming in verifying their efficacy and operational readiness in case of disasters, thereby exposing them to unforeseen risks.
The backups were neither tested nor stored in a secure manner.	Acquisition	IT acquisitions—that is, purchases of hardware, software, and so on—are made for good reasons. Careful analysis of the benefits versus the costs was conducted at the time of purchase, and regularly reviewed to ensure that such still makes sense. [1]	The organization's neglect in testing Disaster Recovery Plans (DRPs) signifies a shortcoming in verifying their efficacy and operational readiness in case of disasters, thereby exposing them to unforeseen risks.

3. Recommendations:

3.1 Information Security:

In view of the identified weaknesses in information security for GCC in Western Australia, I would like to offer the following recommendations: that a comprehensive security framework ISO 27000 [2] be put in place, including the EDM approach, to guide security initiatives in line with organizational goal.

Weakness	Evaluate	Direct	Monitor
Inadequate or out-of-date information security policies	Assess current information security policies against the ISO/IEC 27001 standards in reference to Information Security Policies.	Direct the process of creating new information securities policies based on the ISO/IEC 27001 standard to incorporate all necessary sections and inform all the stakeholders.	Continuously assess and monitor the policies and their compliance with the framework and controls of ISO/IEC 27001 as necessary and on a timely basis.
No review of highly privileged access to applications, databases, and networks	Evaluate the current access control mechanisms and procedures in relation to ISO/IEC 27001.	Supervise the monitoring and scheduling of evaluating privileged access and the practice of the principle of least privilege and access rights.	Regularly audit and utilize automated monitoring systems to monitor the access control processes and maintain ISO/IEC 27001 standards compliance.
Lack of processes to identify and patch security vulnerabilities within IT infrastructure	Assess the processes of vulnerability management and patch management against the requirements of ISO/IEC 27001 (Technical Vulnerability Management).	Direct a formal vulnerability management process that ensures frequent vulnerability assessments, a prioritization scheme, and a remediation schedule compliant with ISO/IEC 27001. The process must encompass all platforms and all applications, regardless of where they reside.	Ensure that the vulnerability management process is effective by conducting ongoing evaluations. These will consist of continuous vulnerability scanning, patch auditing, and reporting. The result will show compliance with ISO/IEC 27001, which makes these actions a requirement for that standard.

No information security awareness programs for staff	Evaluate the present extent of security consciousness among employees, referring to ISO/IEC 27001 and its mention of "Information Security Awareness, Education, and Training."	Direct the creation and execution of a thorough information security awareness program for all employees, ensuring compliance with ISO/IEC 27001.	Monitor regularly how effective the awareness program is. Collect participant feedback to inform decisions and track any security incidents that can be linked to human error.
Lack of staff training and development in information security	Assess the current information security training and development programs against ISO/IEC 27001	Direct the improvement of training programs so that they include up-to-date information on security threats.	Monitor the effectiveness of training programs by assessing enhancements in security protocols, a decrease in incidents, and sustained adherence to ISO/IEC 27001.
Information classification policy or procedures not in place	Use the benchmarks of ISO/IEC 27001 (Asset Management) and ISO/IEC 27002 to assess the necessity of an information classification policy.	Direct the crafting and execution of a policy on information classification that is in accordance with ISO/IEC 27001. This ensures that all informational assets are properly classified and safeguarded based on their sensitivity.	Ensure that everyone complies with the information classification policy by conducting routine audits and assessments. Confirm that all data is controlled properly.
Weak password controls without multifactor authentication	Evaluate existing authentication methods and password policies by the standards in ISO/IEC 27001 (Access Control for Systems and Applications).	Ensure the powerful password policies, including complexity requirements, are put into place and enforce the use of multifactor authentication for access to critical systems, with the aim of aligning these security	Ensure the adequacy of password controls and multifactor authentication by conducting regular security audits and reviewing access logs and incidents. Do these things to ensure that the organization's information security program is in ongoing compliance with the ISO/IEC 27001 standard.

		practices with ISO/IEC 27001.	

3.2 Business Continuity:

The EDM strategy is recommended for Western Australia's business continuity through the maintenance of operational resilience with minimal disruptions due to risk assessment, measures in place, and continuous monitoring.

Weakness	Evaluate	Direct	Monitor
Lack of BCPs or DRPs	The current BCPs and DRPs processes are evaluated against the standards set forth by ISO/IEC 27001, with a specific focus on the Information Security Aspects of Business Continuity Management.	Direct the generation and execution of BCP/DRP following ISO/IEC 27031. This ensures that all vital business operations are included.	Regular monitor, and update BCP/DRP to ensure it is effective and follows the ISO/IEC 22301 standards.
DRPs which did not cover all key systems	We must assess the existing disaster recovery plans for critical systems to ensure they cover all needed elements, using ISO/IEC 27031 as a guide for ICT (information and communications technologies) readiness.	Direct the extension of DRP coverage to all vital systems, ensuring consistency with ISO/IEC 27031 and ISO/IEC 27001 standards.	Conduct regular audits and drills of the Disaster Recovery Plan to ensure all essential systems are covered and that they can be effectively recovered.
Inadequate business impact analysis to prioritize business functions and recovery requirements	Assess the current business impact analysis process in relation to ISO/IEC 22317. This standard offers directives for carrying out a BIA.	Conduct a thorough business impact analysis that prioritizes essential business functions and establishes clear recovery objectives. Ensure that the analysis is in alignment with the standards set forth by	Monitor the business impact analysis process by conducting regular reviews and updates and ensuring that recovery priorities are in line with contemporary organizational shifts and ISO/IEC 22301.

		ISO/IEC 22317 and ISO/IEC 27001.	
Old and redundant DRPs not reflecting current ICT infrastructure	Evaluate the applicability of the current disaster recovery plans to the existing ICT infrastructure using ISO/IEC 27031 as a yardstick for determining ICT readiness.	Ensure the current ICT infrastructure is accurately reflected in the updating of DRPs, with plans that conform to ISO/IEC 27001 and ISO/IEC 27031.	Regularly review, audit, and update DRPs to ensure they are aligned with changes in ICT infrastructure and comply with ISO/IEC 27001.
Untested DRPs and entities not knowing if they can recover systems	Evaluate the existing DRP testing procedures in comparison to ISO/IEC 27001 and ISO/IEC 22301 standards, with a specific emphasis on the efficiency of recovery strategies.	Direct the regular testing of DRP, which includes both simulations and live drills, following ISO/IEC 27031 guidelines to confirm the effectiveness of recovery plans.	Monitor the outcomes of the disaster recovery plan tests, and make any required adjustments to the plan, ensuring that it continues to improve in alignment with ISO/IEC 27001 and ISO/IEC 22301.
Backups were not tested or stored securely	Evaluate the current backup procedures, focusing on their alignment with ISO/IEC 27001 for backup controls and ISO/IEC 27002 for security controls.	Manage the execution of secure backup procedures, including routine testing and secure offsite storage, following ISO/IEC 27001 and ISO/IEC 27031.	Regularly audit and test backups to ensure their integrity and security, to follow ISO/IEC 27001 and ISO/IEC 27002 standards.

Conclusion:

In this report, some of the IT governance risk highlighted in the Western Australian Auditor General's Information Systems Audit Report has been explained. It reviews the capacity of Information Security and Business Continuity according to ISO/ IEC 38500 principles and focuses on the implementation of improvements. To sustain and improve the IT security and availability in state government organizations, it is necessary to apply recommendations outlined in the ISO/IEC 27000. The proposals are intended to rectify audit differences and enhance IT control. Adoption success will improve compliance to standards, link investment decisions to organizational objectives, secure business data, and prepare for disruptions. As for the changes above, constant assessments and evaluations must be done to sustain such advancements. Security plus and upgrades of the same depending on the current threats are crucial to the state government bodies.

References:

1) Holt, A (2013) Governance of IT: An Executive Guide to ISO/IEC 38500, BCS Learning & Development Limited, Swindon.
2) Australian Standards (2018), International Standard, ISO/IEC 27000, accessed 10th August 2024, RMIT Library Database.
3) Australian Institute of Company Directors (2024), Outdated IT systems pose security and operational risks, aicd, accessed 12th August 2024, https://www.aicd.com.au/risk-management/framework/cyber-security/outdated-it-systems-pose-security-and-operational-risks.html
4) Elev8 (2024), The Importance of Cyber Security Awareness Training for Employees, elev8me website, accessed 11th August 2024, https://www.elev8me.com/insights/the-importance-of-cyber-security-awareness-training-for-employees
5) America's Cyber Defense Agency (2023), NSA and CISA Red and Blue Teams Share Top Ten Cybersecurity Misconfigurations, cisa website, accessed 14th August 2024, https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-278a
6) DataGuard (2024), Why business continuity plans fail and what you can do about it, dataguard website, accessed 14th August 2024, https://www.dataguard.co.uk/blog/why-business-continuity-plans-fail/#:~:text=Business%20Continuity%20Plans%20(BCPs)%20often,key%20stakeholders%20within%20the%20organisation.