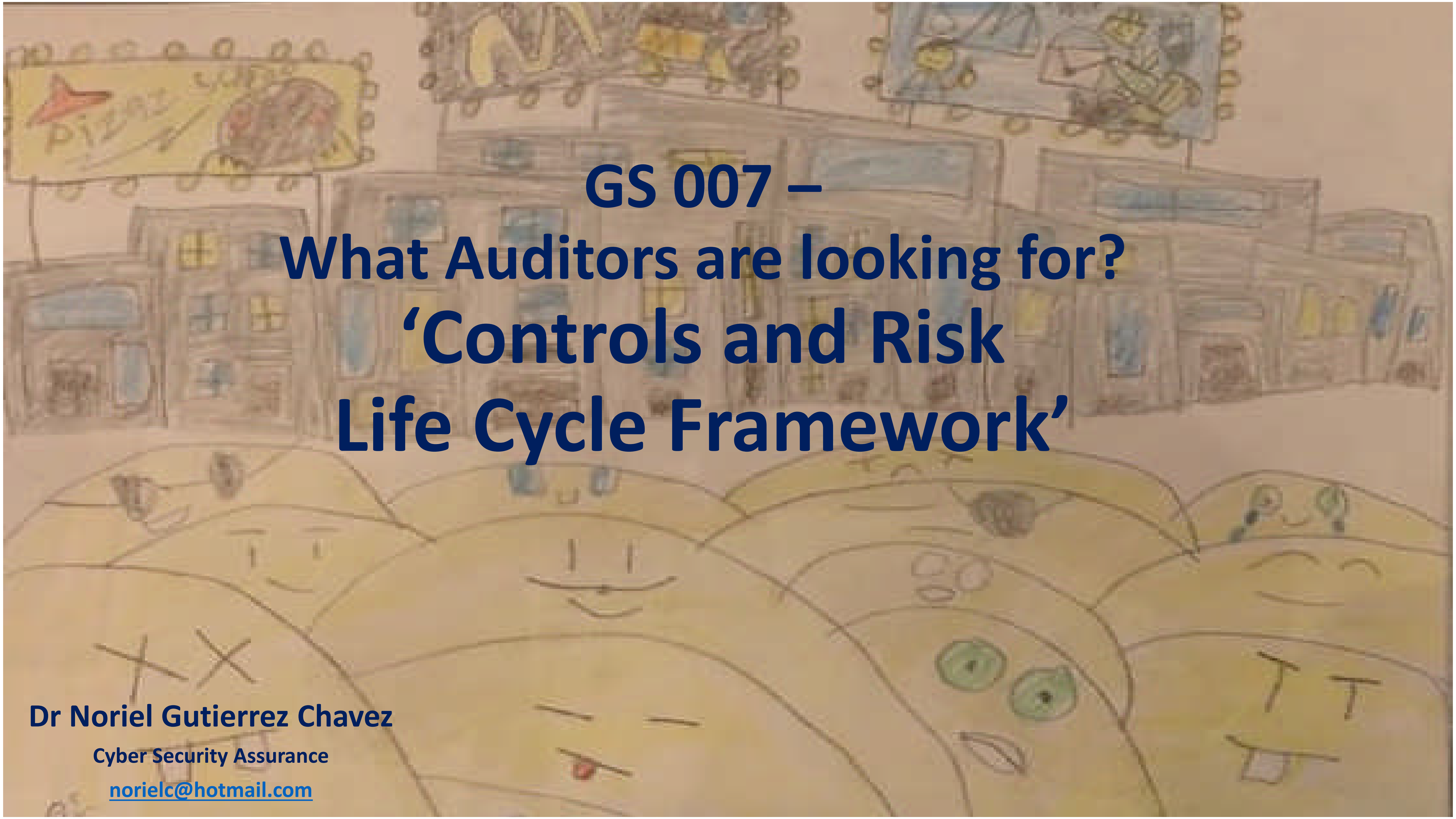


GS 007 – What Auditors are looking for? ‘Controls and Risk Life Cycle Framework’

Dr Noriel Gutierrez Chavez

Cyber Security Assurance

norielc@hotmail.com

What is GS 007?

- It is a standard that prescribes a minimum set of control requirements for service organisations offering investment management services.

- It was created by the Australian Government Auditing and Assurance Standards Board (last updated October 2011).

- It is aligned with International Standards for Assurance Engagements (ISAE) 3402.

- It aims to protect client personal confidential and sensitive information.

Why GS 007?

- GS 007 has become a compliance requirement for service providers to improve their risk management and compliance programs.

- Financial services providers have been increasingly outsourcing their business processes to external organisations. These partners are required to comply with legislative and regulatory audit requirements.

- In addition to financial reporting controls.

- To ensure client confidential and sensitive information are secure and safe.

Why Not GS 007?

- Some organisations think that GS 007 is an onerous standard to comply to.
- GS 007 has a limited scope of control objectives.
- Inconsistency in methodologies and reporting frameworks applied.
- Over-reliance on the extent of assurance.
- Clean audits are hard enough. GS 007 can add to the burden.

Introduction

- As cyber security breaches dramatically increases.
- GS 007 standard can apply to Custody, Asset Management, Property Management, Superannuation Member Administration, Investment Administration or Registry Management. It provides a safety net to ensure the integrity, reliability and confidentiality in Information Technology for these sectors.
- The control objectives outlined in GS 007 are defined by
  - description
  - stating control objectives
  - designing
  - Implementing
  - effectively operating controls
- Auditors responsibility is to express their opinion on the organisation's description, design, and operation of controls related to control objectives stated in the description based on auditor's procedure.
- Then what Auditors is looking for?
- How to use Controls and Risk Life Cycle Framework?

What is the auditor there to do?

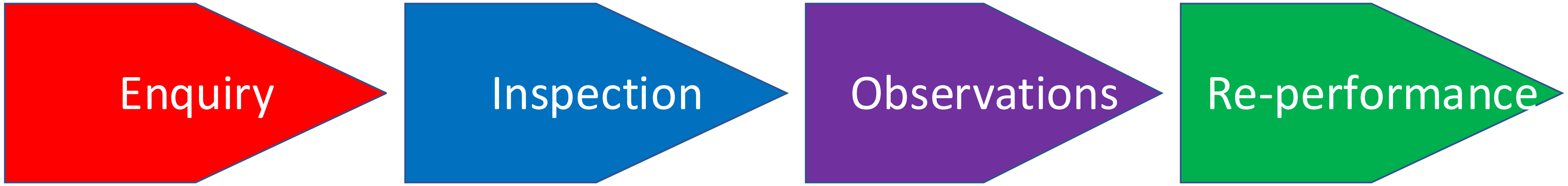
- To report on the description, design, and operating effectiveness of controls in a service organization performing procedures.

- To obtain evidence about the disclosures in the organisation's description of its system in the coverage audit period.

- Auditors are assessing whether the organisation followed what is stated in their control objectives.

- The Auditors can test controls. This includes procedures such as enquiry, inspection, observation and re-performance.

Auditors Description of Nature of Tests



Enquiry

Inspection

Observations

Re-performance

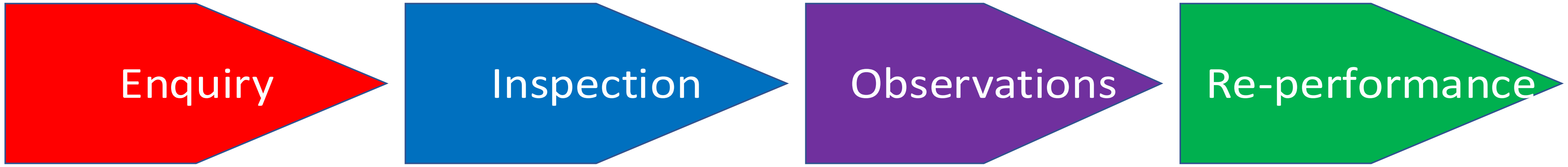
- Enquired to obtain relevant information or representation from appropriate organisation’s personnel.

- Inspected documents and records indicating performance and effectiveness of the controls.

- Observed the application or existence of specific controls as represented.

- Re-performed the control to check the accuracy of their operation.

Organization's Responses to Auditors Test Operations



Enquiry

- Personnel demonstrate accurate evidence to controls.
- Disclose the evidence information of any gaps before the deviation is identified.

Inspection

- Personnel ensure the documents & records have been reviewed.
- Demonstrate the strategic plan to remediate the gap and resolve within the audit period.

Observations

- Personnel ensure to demonstrate the effectiveness of the existing controls.

Re-performance

- Personnel ensure the remediation has been completed to resolve any identified gaps.
- Demonstrate the reconciliation of evidence in the controls.

Organisation’s responses to auditor’s test operations

The recommended approach with the auditors during the audit period is:

- Auditors want to see a proactive approach and improved processes to ensure the control objectives are met.

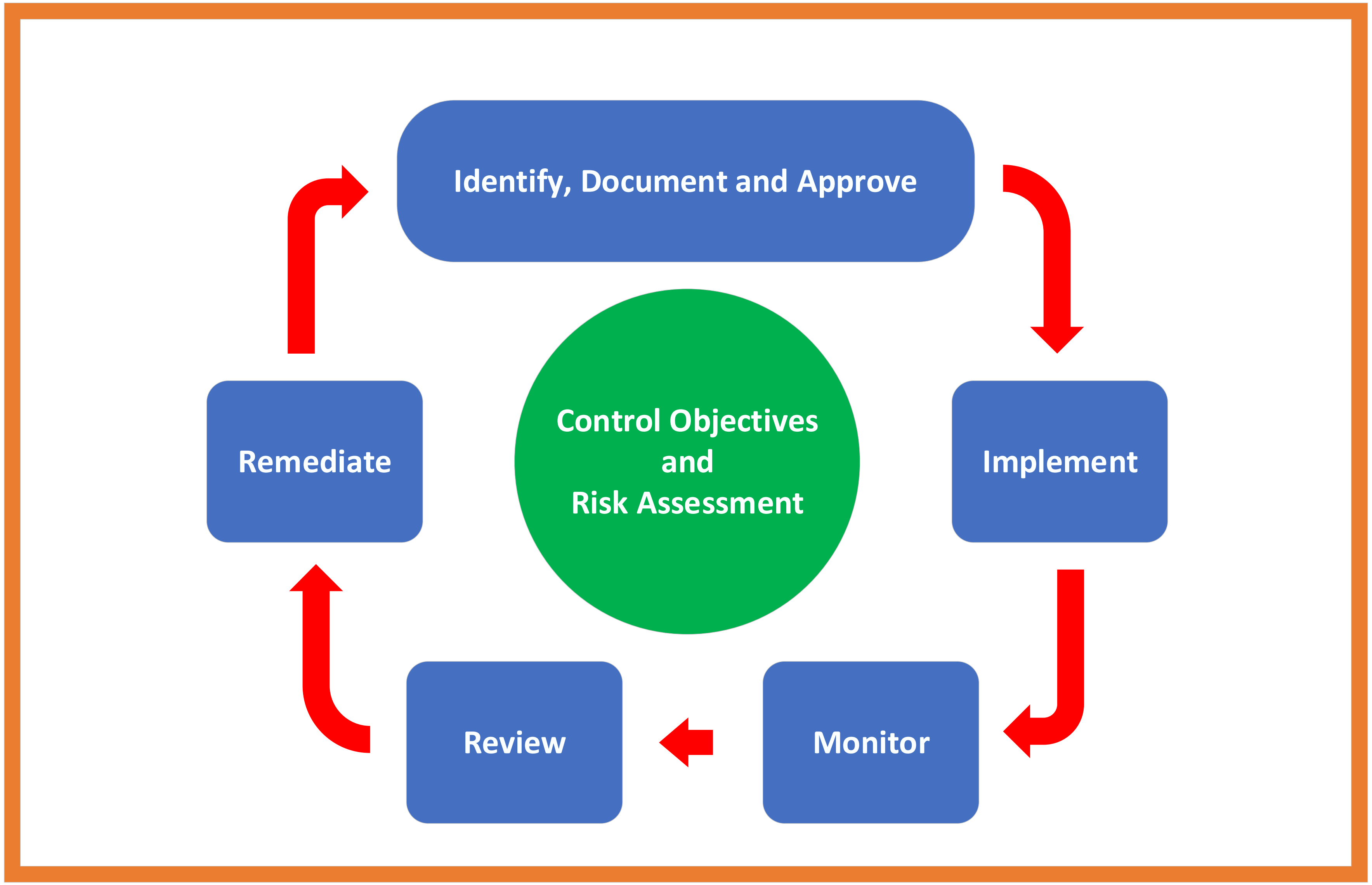
- If an issue occurred, better to disclose the issue and provide the strategic plan for remediation to resolve the issue immediately, within the audit period.

- This will demonstrate to the auditors that the organisation’s honesty, cooperation, and the improvement of culture in risk management and compliance strategies.

The main practical items what auditors are looking for:

- Exceptions that do not align with the defined operating controls.
- False evidence provided.
- Hesitation to cooperate from the organisation’s business operations that will end with a costly exercise.
- Has the organisation followed what it stated were its own objectives.

Controls and Risk Life Cycle Framework



Identify, Document and Approve

Implement

Monitor

Review

Remediate

Control Objectives
and
Risk Assessment

How to use Controls and Risk Life Cycle Framework?

Auditors would like to see that the organisation has a structured governance and the foundation of integrating, conceptualisation, development and implementation of the life cycle framework includes:

- Identify, document, and approve the policies and frameworks with embedded controls, risk, processes and procedures that is based on Australian and international standards and guidance statements.
- Implement security controls, processes and procedures.
- Monitor the implemented security controls, processes and procedures to provide information for analysis.
- Review the monitored information to identify the gaps and issues.
- Remediate the identified gaps and issues to update the policies and frameworks with appropriate security controls, risk, processes and procedures to ensure information are secure and safe.

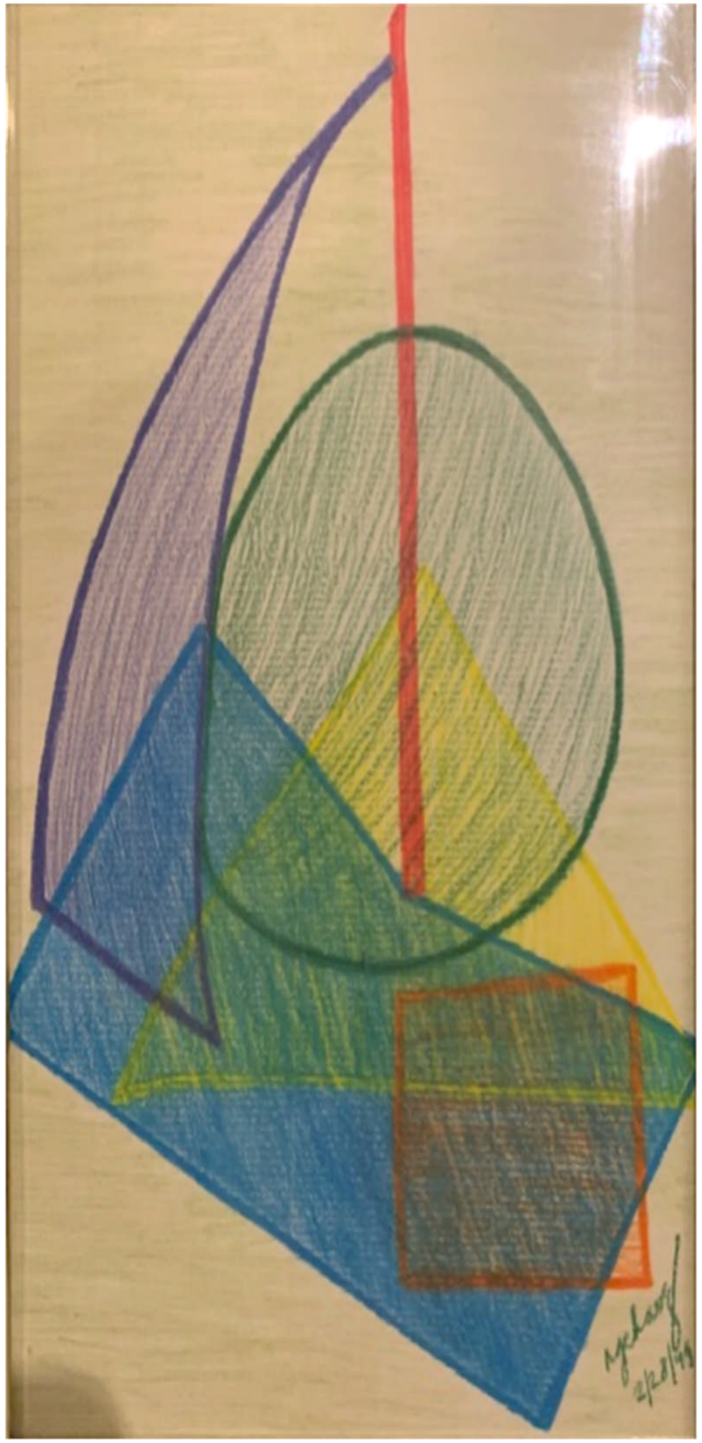
Case Study – Information Security

Access Controls:

- Username and Password:
  - Unique username must be unique and not to be shared.
  - Password complexity must be at least 15 minimum length with a combination of small and uppercase letters, number and special characters.
  - Regularly change password every 90 days.
  - Use of paraphrase to remember lengthy password.

- Restricting access to system data:
  - Logical access to computer systems, programs, master data, client data, transaction data and parameters, including access by administrators to applications, databases, systems and networks, is restricted to authorised individuals via information security tools and techniques.
  - Segregation of incompatible duties is defined, implemented and enforced by logical security controls in accordance with job roles.

- User access reviews
  - Management must regularly perform user access reviews.



Is it difficult to do the basics?

For example, in Information Security control objectives, most common types of deviations or qualifications identified are basic steps to protect the customer information:

- Generic username and password.
- Weak password length and combination.
- Inappropriate super-user access.
- Failure to review user access on a timely basis.
- Failure to revoke user access following employee termination/resignation or transfer.
- Inappropriate segregation of duties between production, development and test environments.

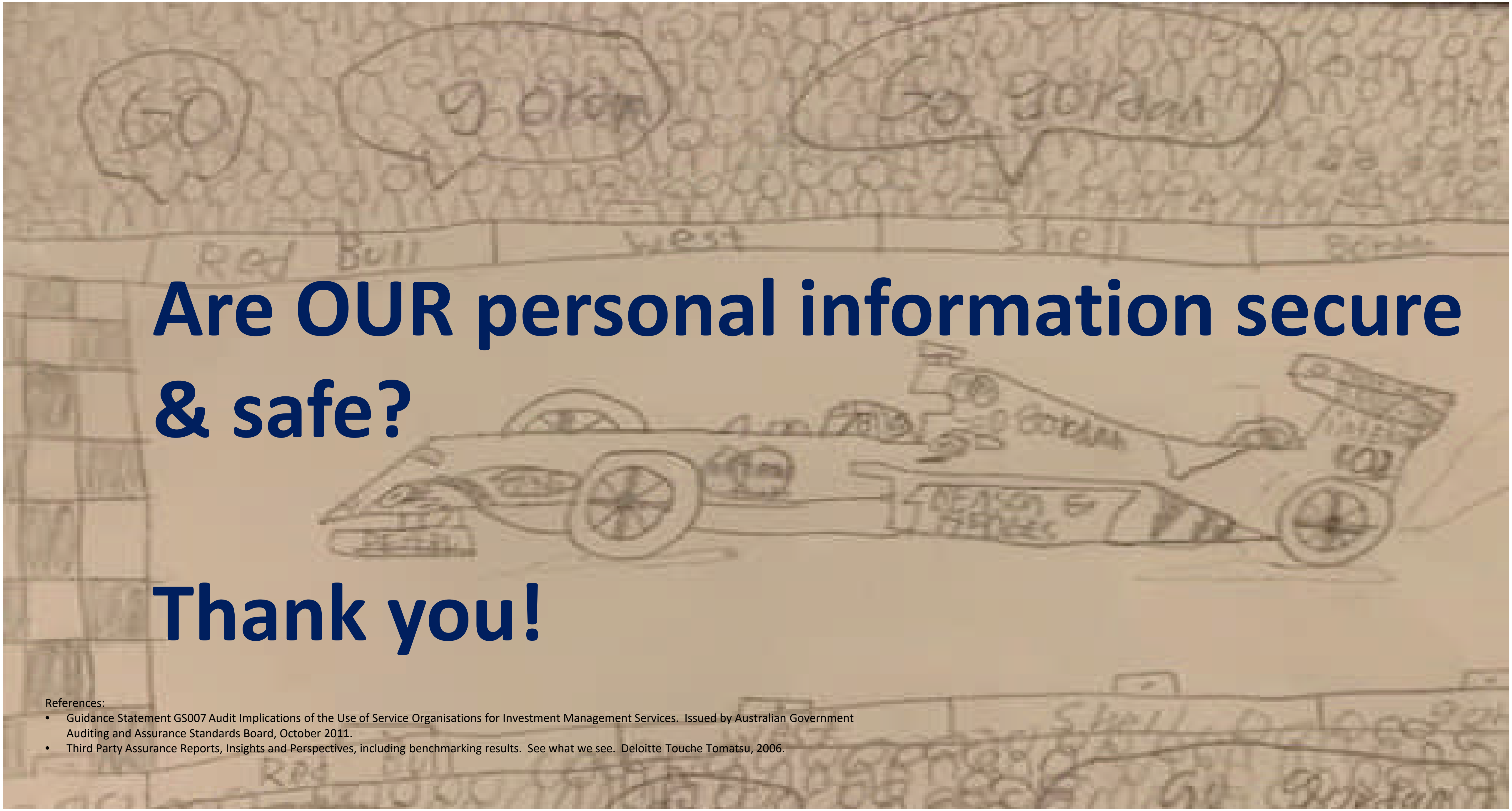
Conclusion

- GS007 – What Auditors are looking for?

- The auditors are looking for the basic security posture requirements that will improve the organization’s risk management governance and compliance program.

- The Controls and Risk Life Cycle Framework is a streamlined set of governance assurance steps and activities that provide the basis for GS007 compliance.

- Is it difficult for organization to perform the basic steps to ensure client ‘OUR’ personal confidential and sensitive information are secure and safe?



Are OUR personal information secure & safe?

Thank you!

References:

- Guidance Statement GS007 Audit Implications of the Use of Service Organisations for Investment Management Services. Issued by Australian Government Auditing and Assurance Standards Board, October 2011.
- Third Party Assurance Reports, Insights and Perspectives, including benchmarking results. See what we see. Deloitte Touche Tomatsu, 2006.