



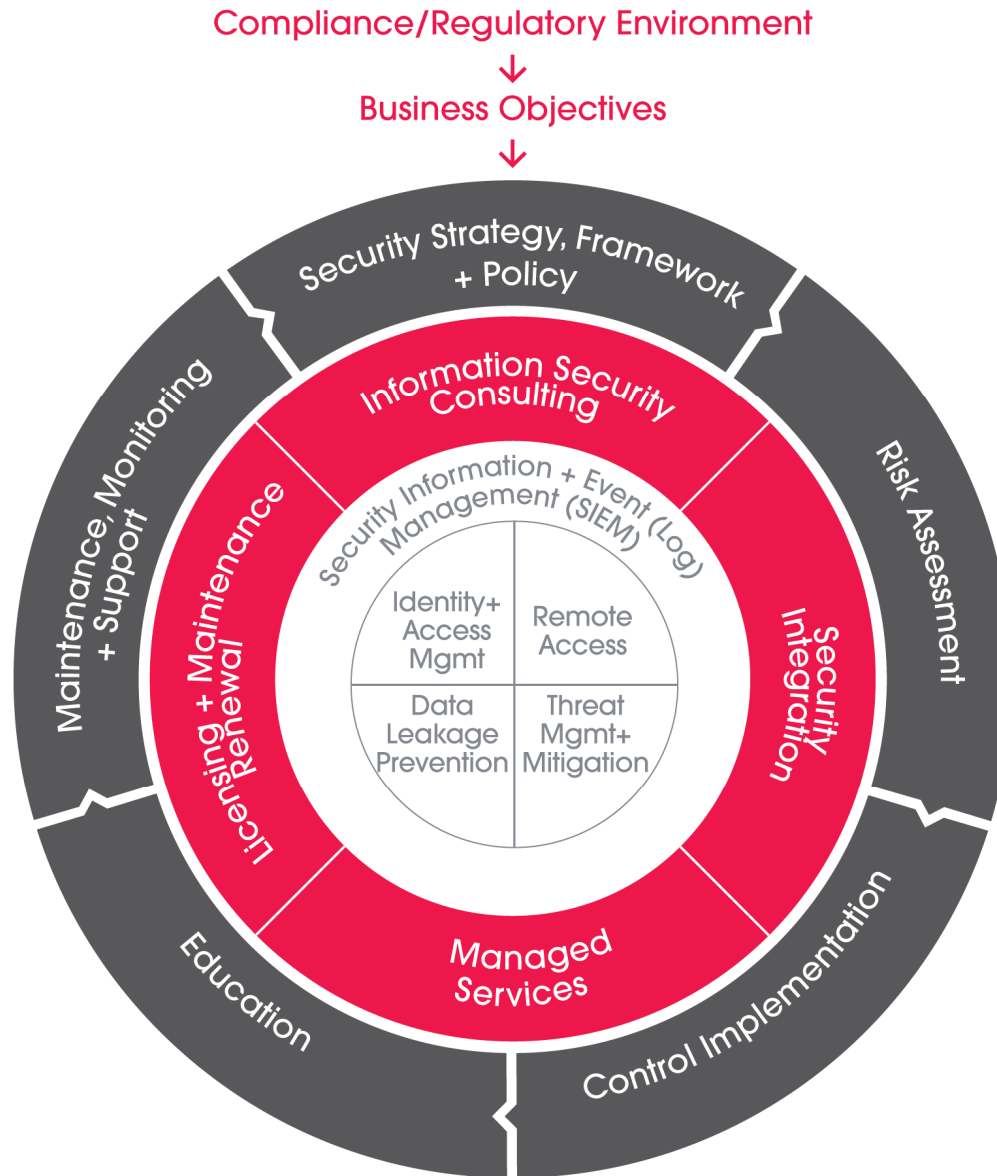
# Aligning IT Strategy to APRA PPG234

Management of security risk in  
information and information technology

# About Loop

- Focused Australian-owned IT Security integration specialist
- 16 years of IT Security experience and expertise
- Trusted security advisor to many leading organisations across a broad range of industries
- Provide a complete LOOP of Information Security solutions and services, designed to provide secure direction for your business

# Loop Technology approach to security

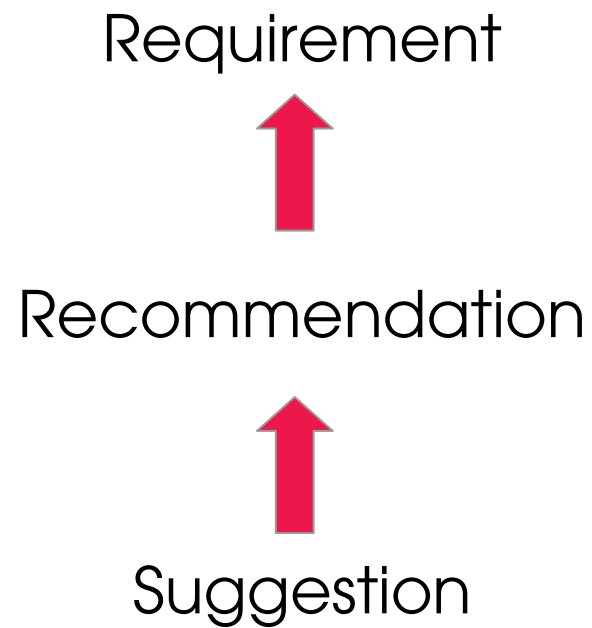
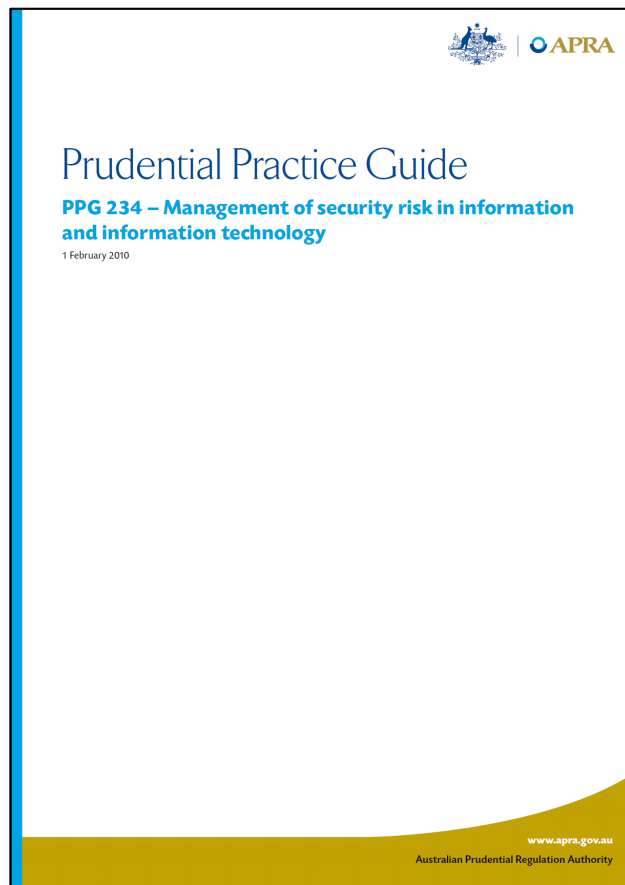




# Security requires solid foundation



# APRA PPG234



# AGENDA

- 12.30pm Arrival, Registration & Welcome
- 12.50pm **Aligning IT Strategy with APRA PPG234**  
Daniel Hooper  
Loop Technology Information Security Lead  
CISM, CISSP
- 1.20pm Lunch Break
- 1.50pm **Technical Considerations within APRA PPG234**  
Louis Rabon  
Loop Technology Services Delivery Manager  
*Dessert Served*
- 2.20pm Q&A
- 2.30pm Event Close



# Aligning IT Strategy with APRA PPG234

Daniel Hooper  
Loop Technology Information Security Lead  
CISM, CISSP

# Introduction to PPG 234

Australian Regulatory Authority Prudential Practice  
Guide 234:

Management of security risk in information and  
information technology (1 Feb 2010)

Assists us with:

- Management of IT Security risk
- Provide guidance to senior management
- Identifying common areas of concern

# Introduction to PPG 234

Guideline (not a Standard):

PPG 234 is not a Standard, just a Guide.

Based on:

- Common findings
- Common practices
- Effective governance

# Introduction to PPG 234

“In APRA’s view, IT security risk will ultimately result in a business risk exposure. Regulated institutions would benefit from clearly defining both IT risk and IT security risk.”

# Introduction to PPG 234

Guideline (not a Standard):

PPG 234 is not a Standard, just a Guide.

Does not:

- Provide prescriptive direction
- Replace ISO, PCI, COBIT, ITIL etc
- Replace regulatory compliance requirements

# Introduction to PPG 234

## IT Security Risk:

“IT Security risk... can be described as the risk of loss due to inadequate or failed internal processes, people and systems or from external events, resulting in a compromise of an IT asset’s Confidentiality, Integrity or Availability.”

APRA, “Prudential Practice Guide PPG234 – Management of security risk in information and information technology”, February 2010, s13.

# Principles

1. IT security risk
2. An overarching framework
3. User awareness
4. Access control
5. IT asset life-cycle management controls
6. Monitoring and incident management
7. IT security reporting and metrics
8. IT security assurance

## Processes

# 1. IT Security Risk

Identify, assess, *classify*, assign ownership, develop controls and manage risks.

IT Security Risk Management should:

- Be on-going, continuous, dynamic
- Identify not only technical threats
- Be aligned to business requirement

# 1. IT Security Risk

## Risk Classification

- Based on business criticality and sensitivity
- Based on IT Asset classification
- Based on Information Asset classification

“Institutions may seek to leverage the existing business impact analysis process to achieve this.”  
s20.

# 1. IT Security Risk

## Risk Classification

- Identify critical IT Assets
- Identify sensitive Information Assets
- Define classification guidelines

Implement customised classification scheme

## 2. Overarching Framework

“The establishment and ongoing development of the IT security risk management framework would normally be directed by an overarching IT security strategy and supporting program of work.”s24

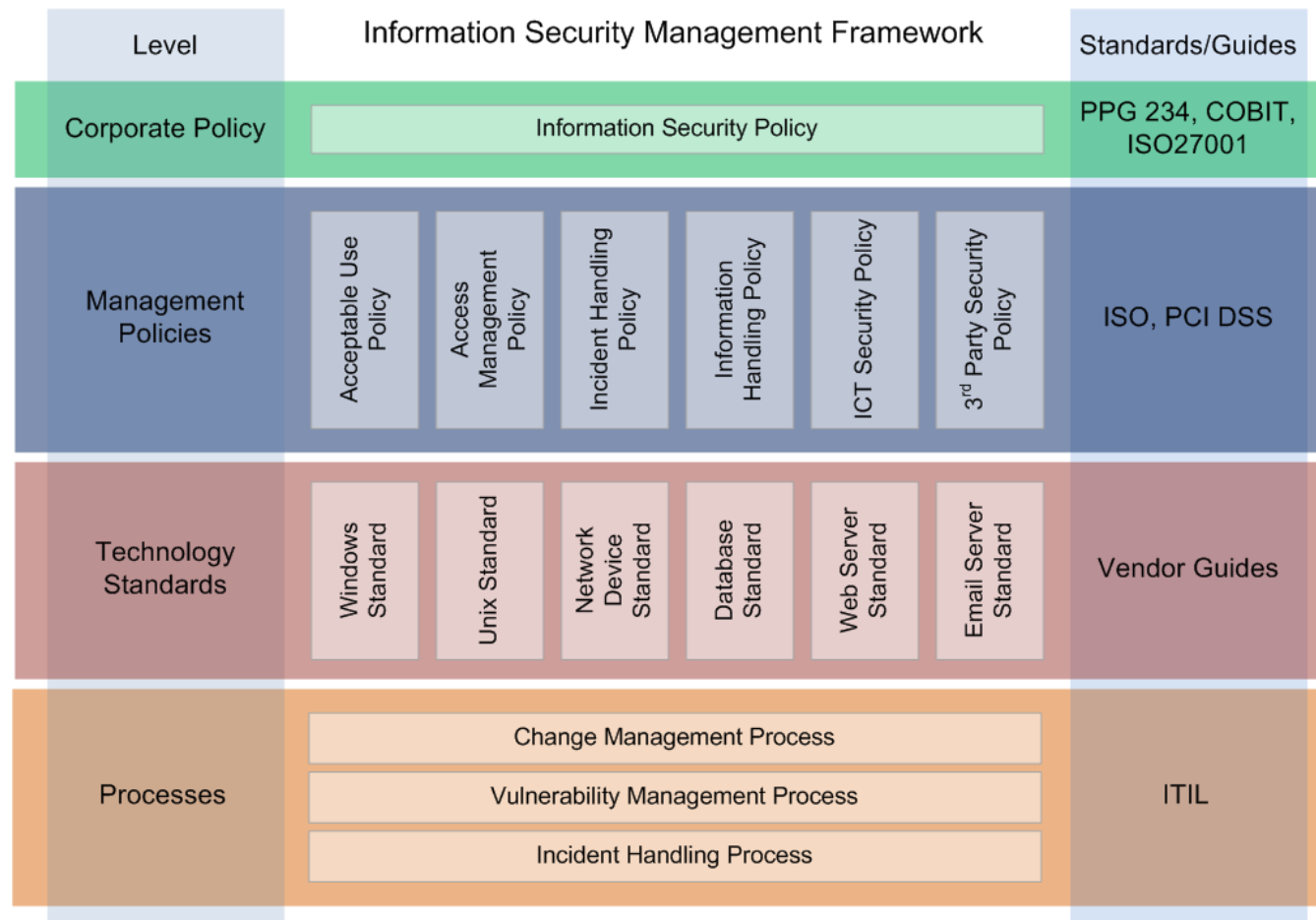
## 2. Overarching Framework

Overarching framework of policies, standards, guidelines and procedures.

Information Security Management Framework includes:

- Information Security Policy
- Technology related Standards
- Processes and procedures for implementation

## 2. Overarching Framework



## 2. Overarching Framework

Framework documentation:

- Necessary policies in place
- Policies reviewed for appropriateness
- Feedback loop for improvement

Ownership, accountability and monitoring for compliance

# 3. User Awareness

“A regulated institution could benefit from developing an initial, and ongoing, training and IT security and awareness program.”s33.



# 3. User Awareness

Education, awareness training and communication of risk.

User Awareness training should:

- Include defined learning objectives
- Communicate pertinent policy statements
- Be tailored to the responsibilities of the audience

# 3. User Awareness

## Common Learning Objectives/Education Areas:

- Personal vs. business use of IT Assets
- Email usage
- Internet usage
- Personal storage devices
- Passwords
- Handling of sensitive information
- Incident reporting

## 4. Access Control

“A key requirement for ensuring IT security is an effective process for providing access to IT assets. A regulated institution would normally only authorise access to IT assets where a valid business need exists and only for as long as access is required.”<sup>s37</sup>



## 4. Access Control

Access to information and systems is to be based on business need.

Factors to consider:

- Principles of least privilege
- Separation of duties
- Role based security (employee, 3<sup>rd</sup> party, contractor etc)
- Inherited access

# 4. Access Control

## Implementing access control:

- Review of Access Control Policy
- Access provided based on IT Asset and/or Information Asset classification and risk assessment
- Monitoring of access to critical or sensitive IT Assets and Information Assets

Define the roles, assign the access,  
monitor the use

## 6. Monitoring and Incident Management

“APRA envisages that a regulated institution would establish a clear allocation of responsibility for regular monitoring, with appropriate processes and tools in place to manage the volume of monitoring required, thereby reducing the risk of an incident going undetected.”<sup>s67</sup>

# 6. Monitoring and Incident Management

Monitoring should include:

- Monitoring for and implementation of required changes to policy, standards, processes and procedures
- Improvement to communication and awareness
- External review and assessment

On-going assessment of effectiveness

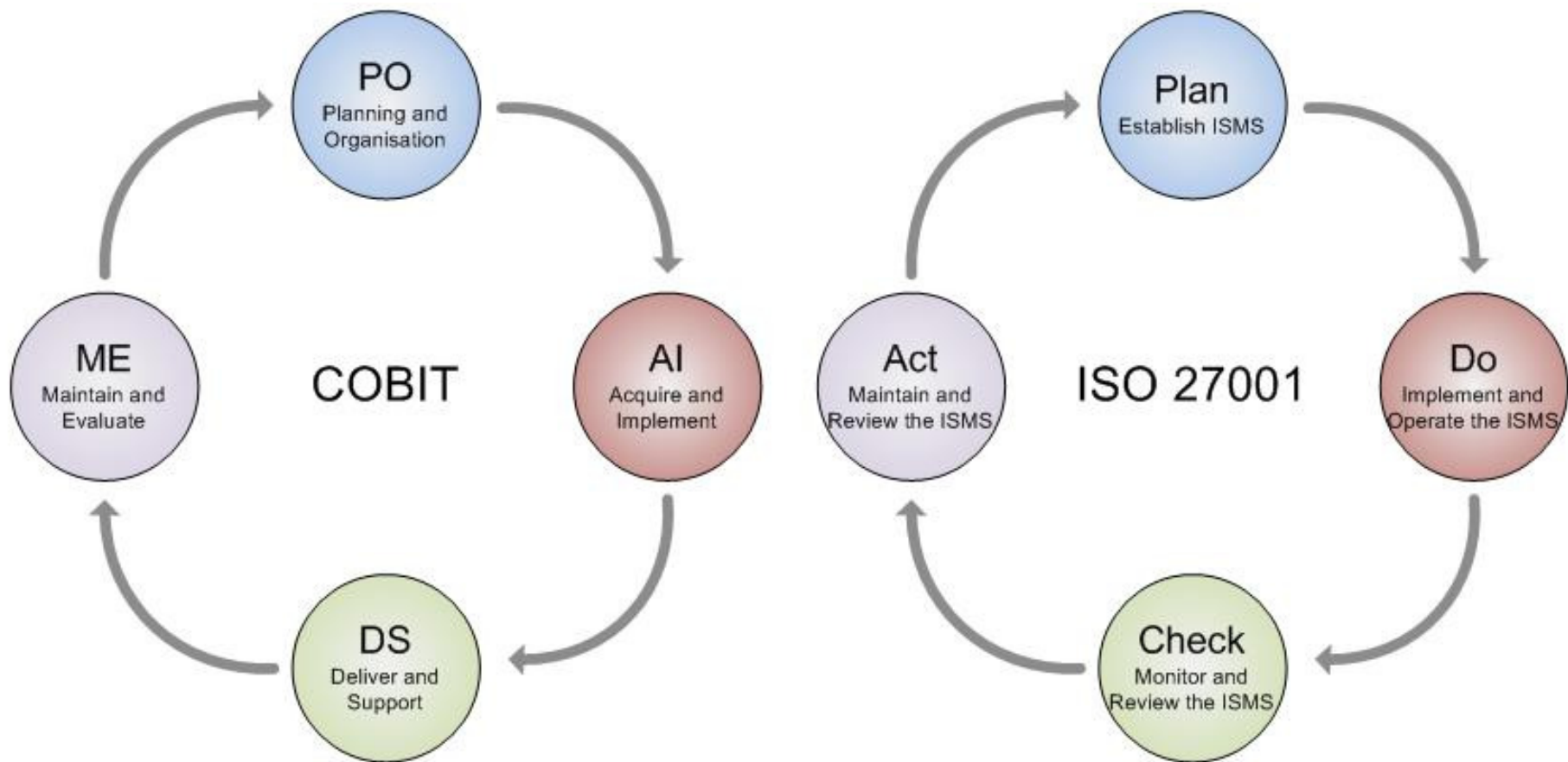
# 6. Monitoring and Incident Management

Incident Management should include:

- Defined roles and responsibilities
- Processes to:
  - Detect
  - Identify
  - Contain
  - Investigate, gather evidence
  - Resolve and *review*

On-going assessment of effectiveness

# Feedback and Review



## 8. IT Security Assurance

“APRA expects that a regulated institution would seek regular assurance that IT assets are appropriately secured and that its IT security risk management framework is effective.”s80

# 8. IT Security Assurance

Formal, systematic and scheduled assessment of control environment

Minimum assurance recommendations:

- Annual external Vulnerability Assessment
- Annual Security Policy & Process Review
- Review of Security Improvement Strategy

# Processes

Documented, communicated, tested,  
improved.

Common IT Security related processes include:

- Change Management
- Vulnerability Management
- Incident Management

# Further Consideration

Areas to consider described in PPG 234:

- Data/information leakage
- Cryptographic techniques to restrict access
- IT asset life-cycle management controls
- Physical security
- Secure software development
- Accountability and audit trails
- And more...

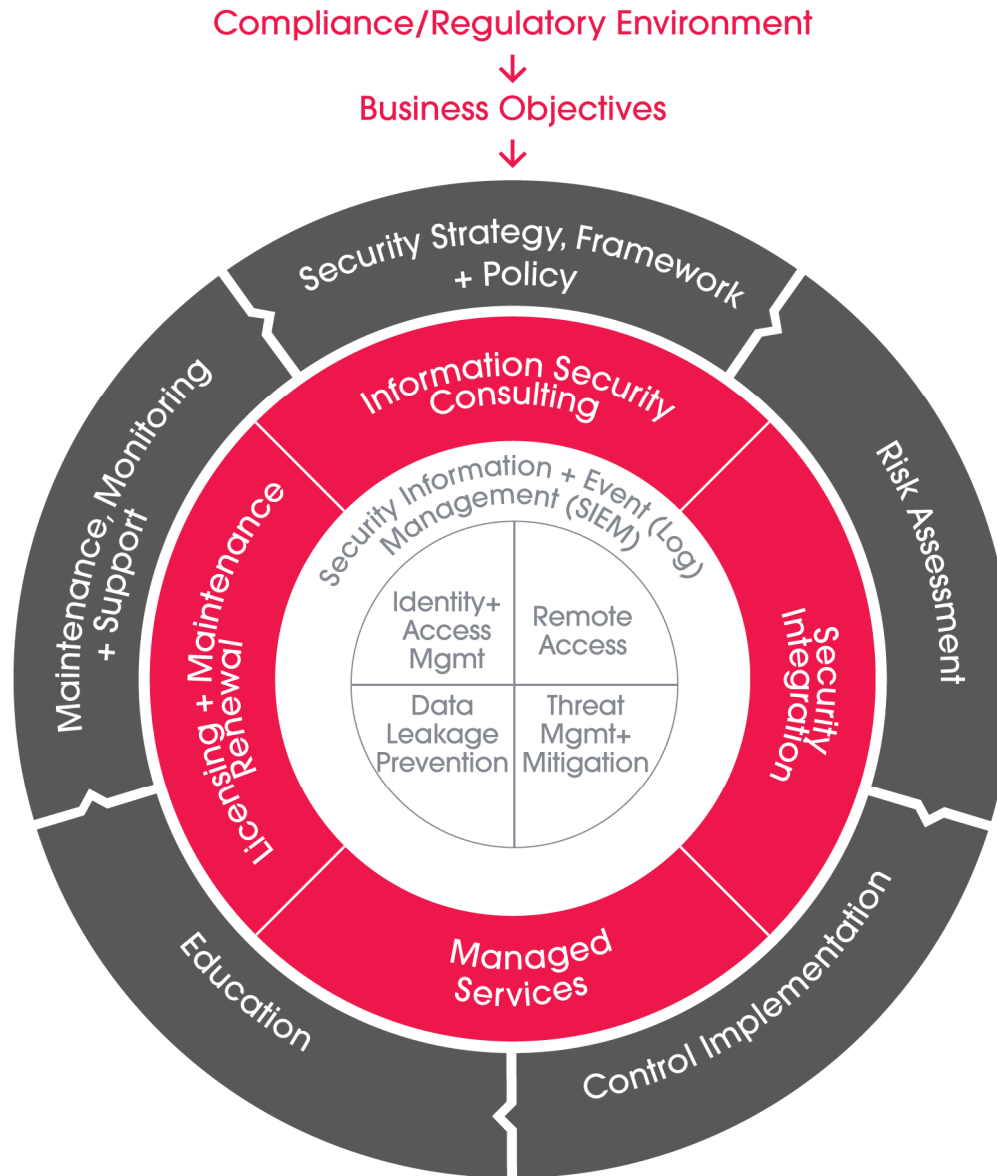
# Non – Technical Controls

	APRA GUIDE							
	IT Security Risk	An Overarching Framework	User Awareness	Access Control	IT Asset Life-cycle Mgt	Monitoring and Incident Mgt	IT Security Reporting and Metrics	IT Security Assurance
Risk Assessment	√	√		√	√	√	√	√
Gap Analysis	√	√		√			√	√
ISMS	√	√						√
IT Security Policy	√	√	√	√		√	√	√
Vulnerability Assessment	√	√					√	√
Penetration Testing	√						√	√

# Non – Technical Controls

	APRA GUIDE							
	IT Security Risk	An Overarching Framework	User Awareness	Access Control	IT Asset Life-cycle Mgt	Monitoring and Incident Mgt	IT Security Reporting and Metrics	IT Security Assurance
Access Control Policy			√				√	√
Security Awareness Training			√					
Incident Handling Strategy	√	√	√			√	√	√
Business Continuity Planning	√	√	√		√	√	√	√
Security Architecture Services	√				√			√

# Loop Technology approach to security





# Aligning IT Strategy to APRA PPG234

Management of security risk in  
information and information technology



# Technical Considerations within APRA PPG234

Louis Rabon  
Loop Technology Services Delivery Manager  
CISSP, GSNA, GCIH

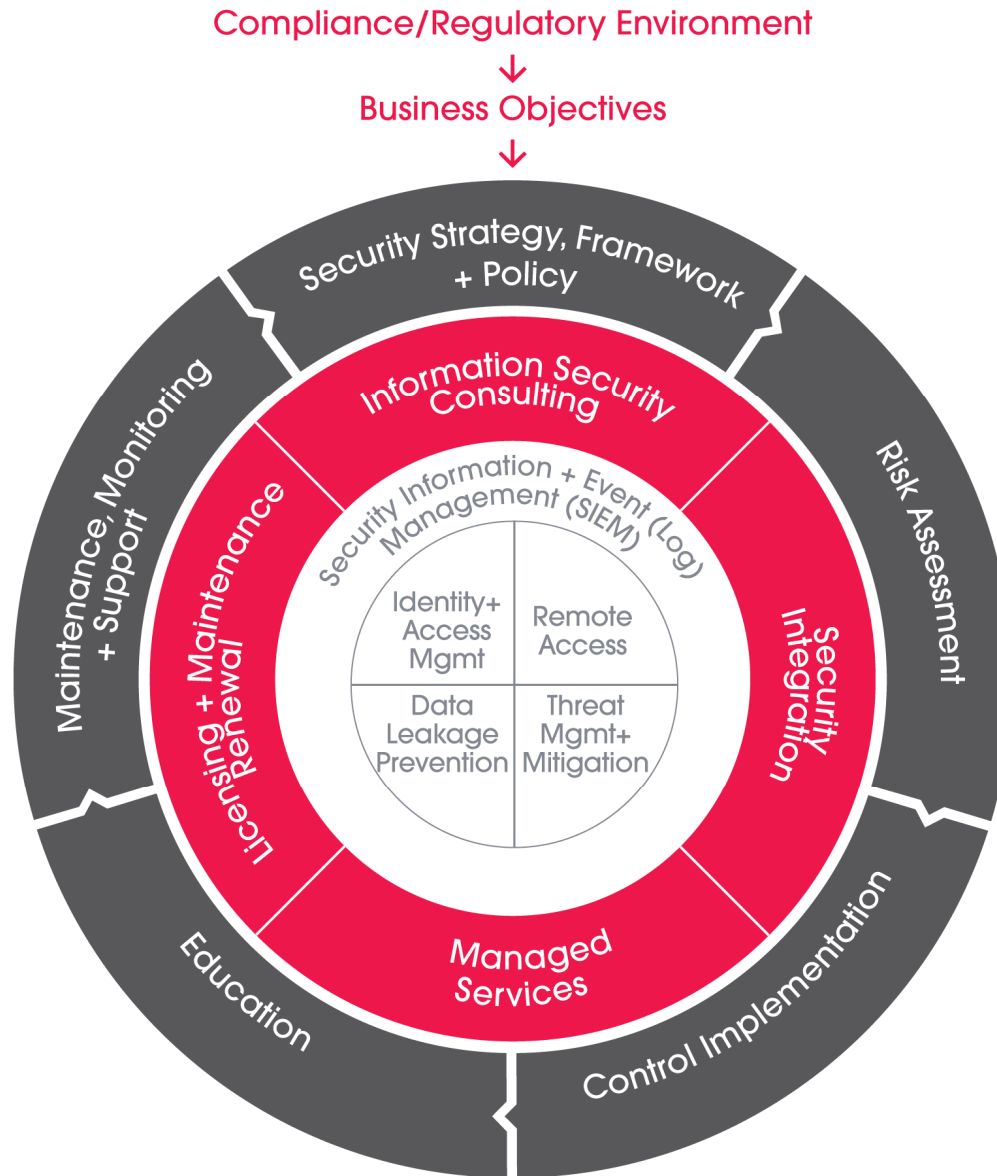


loop  
TECHNOLOGY



Conformity

# Loop Technology approach to security



# Technical Controls

	APRA GUIDE							
	IT Security Risk	An Overarching Framework	User Awareness	Access Control	IT Asset Life-cycle Mgt	Monitoring and Incident Mgt	IT Security Reporting and Metrics	IT Security Assurance
Security Information Event Mgt	√	√		√		√	√	√
Remote Access			√	√		√		
Data Leakage Prevention	√		√	√		√	√	√
Identity Mgt		√		√		√	√	√
Threat Mgt & Mitigation	√	√		√		√	√	√
Licensing, Maintenance & Support					√			√

## 4. Access Control

“A key requirement for ensuring IT Security is an effective process for providing access to IT assets.”<sup>s37</sup>

APRA PPG234 recommends technical access controls for:

- Secure Remote Access
- Data Leakage Prevention
- Identity Management

## 4. Access Control Secure Remote Access

- Point solutions:
  - Access for remote users and remote offices
  - Two-factor authentication the standard
  - SSL VPNs
  - PKI/SSO



## 4. Access Control Secure Remote Access

### Recommendation

- Most institutions have secure remote access solution
- Review secure remote access solution
  - Acceptable Usage policy?
  - Strong authentication
  - Restricted access?
  - Pre authentication checks?

“Include the use of strong password techniques and increasing the number and/or type of authentication factors used.” s41

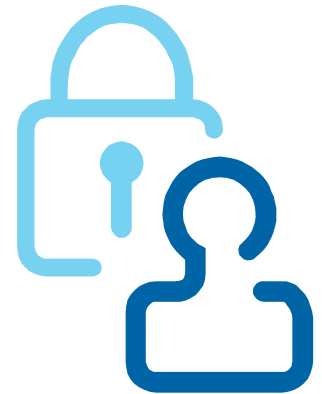
## 4. Access Control Data Leakage Prevention

“Access to sensitive data/ information would be highly restricted to reduce the risk exposure to significant data leakage events.”<sup>s49</sup>



## 4. Access Control Data Leakage Prevention

- Keeping your confidential data within the perimeter
- A multi-tier solution
- Need to address both Data-in-Motion and Data-at-Rest



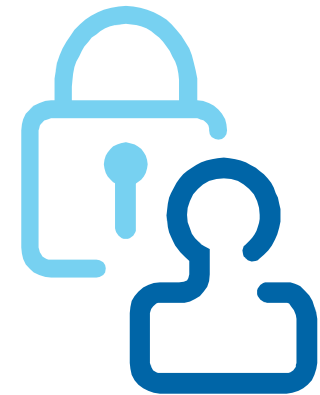
# 4. Access Control Data Leakage Prevention

## Recommendation

- Know your information – Data Classification Policy & Plan
- Use technology to enforce policy

## Quick wins

- Monitoring/ blocking of external devices
- Endpoint/ device encryption
- Monitoring mode of many DLP products will give you insight into what your data is doing



## 4. Access Control Identity Management

For accountability purposes, a regulated institution would normally ensure that users and IT assets are uniquely identified and their actions are auditable.”s45



# 4. Access Control Identity Management

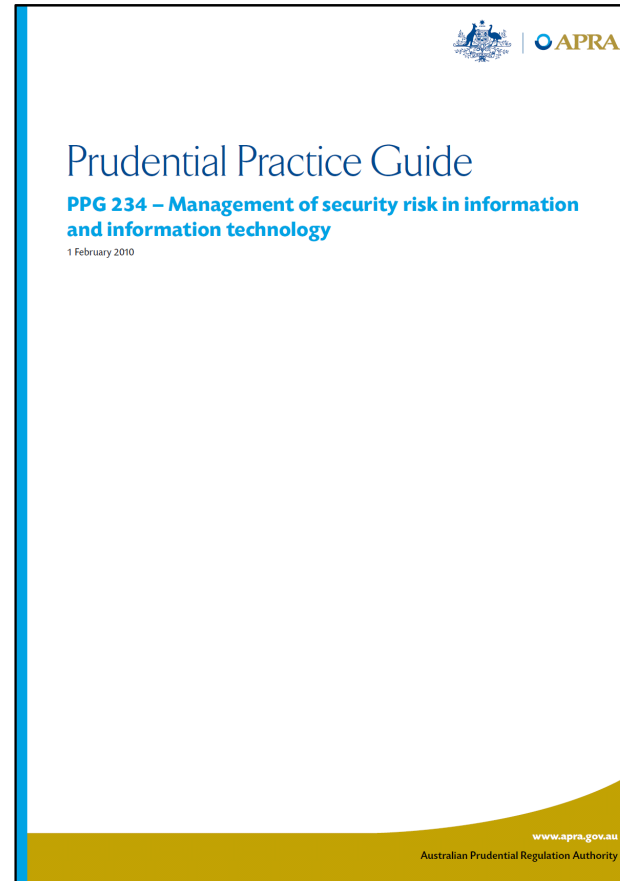
## Identity Management (IDM)

- Access control across different systems
- Can encompass a wide-range of functions
- Major component of Role Based Access Control (RBAC)
- Enables easier tracking of users



# 5. Monitoring & Incident Management

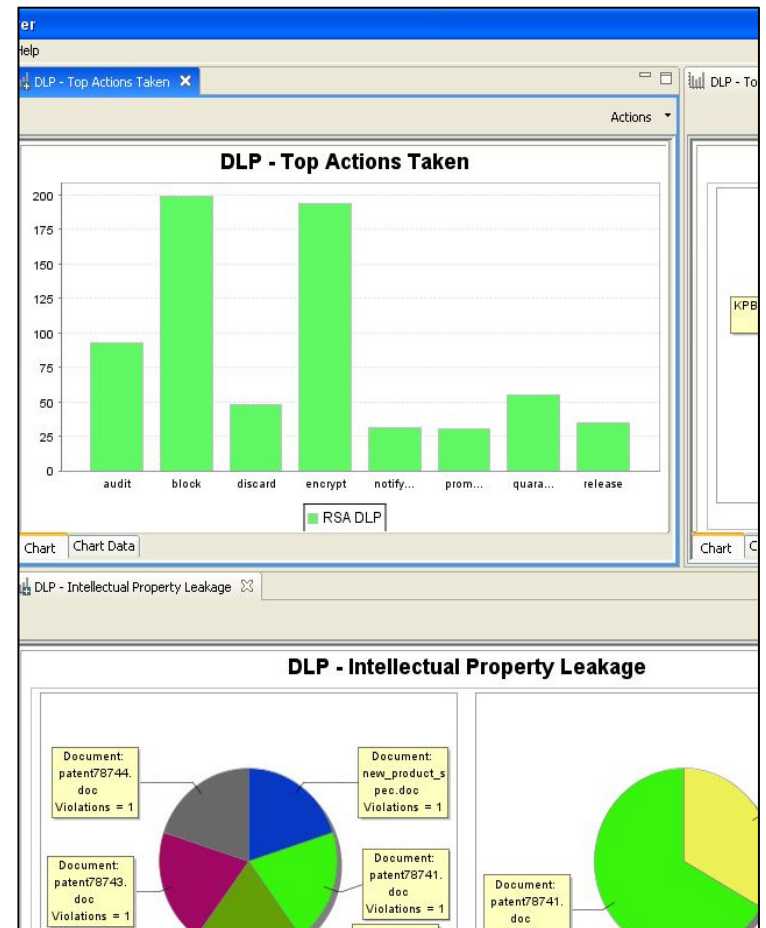
“A regulated institution would normally have monitoring processes in place to identify events and unusual patterns of behaviour.”  
s65



# 5. Monitoring & Incident Management

## SIEM (Security Information Event Management)

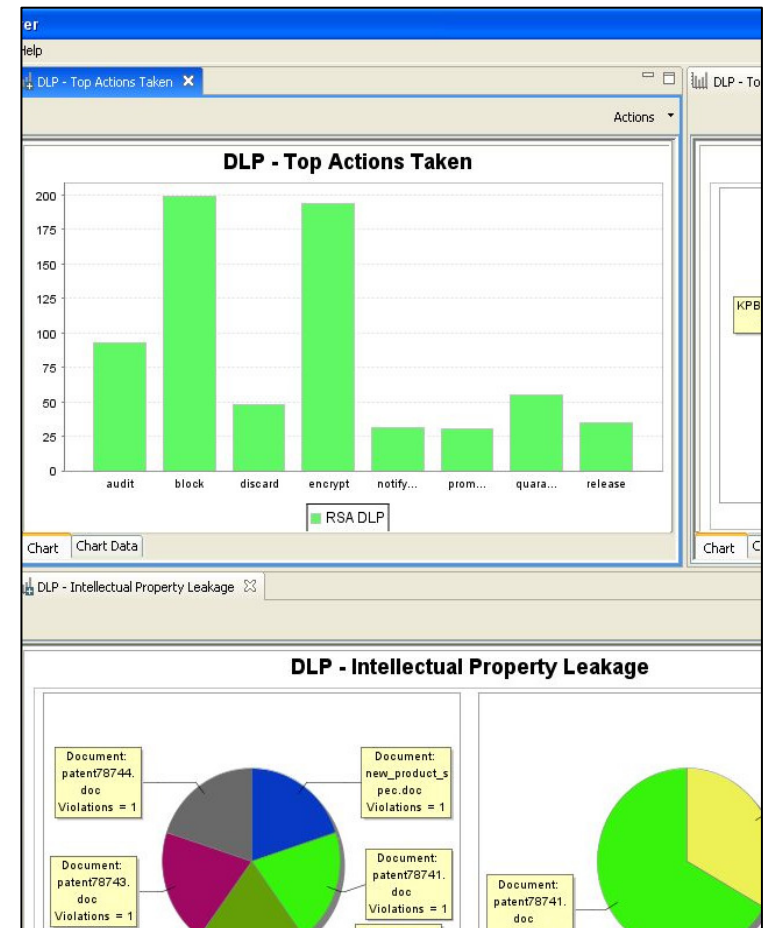
- Log Management, Event Correlation and Alerting
- A Dashboard for incidents within your organisation
- Must be forensically sound
- Ability to receive logs from multiple, disparate systems



# 5. Monitoring & Incident Management

## Recommendation

- Multi-phased approach
- Compliance reporting tool (e.g. PCI)
- Capable of in-depth log event correlation across network
- Enterprise view of multiple security vectors
- Enables auditing against policy



# 5. Monitoring & Incident Management

“A regulated institution would develop appropriate processes to manage all stages of an incident that could impact on services.” s71

- Multiple product solution:
  - AV/HIPS
  - Vulnerability Scanning
  - IPS
  - Centralised Management

# 7. IT Asset Life-cycle Management

- The 3 principles of security: Confidentiality, Integrity and Availability
- Ensure all of your products are up-to-date and supported
- Can help not only with asset tracking but also incident handling

“Ongoing support and maintenance controls would typically be in place to ensure that IT assets continue to meet business objectives.”s54

# Other APRA Principles

Relates to PPG 234: IT Security Risk, An overarching framework, User Awareness, Appendices A-F

- Did not specifically mention end-point solutions because this is mostly process-based
- Security is a moving target, point solutions alone are NOT the answer
- Loop offers services to fill in the gaps and make sure the money being spent on your solutions is accurately placed and as effective as possible

# Summary

- IT Security is a process
- Technical and Non-Technical Controls are required
- Security compliance is not a straight line, it's a circle
- Even with a large internal security department, outsourcing is necessary



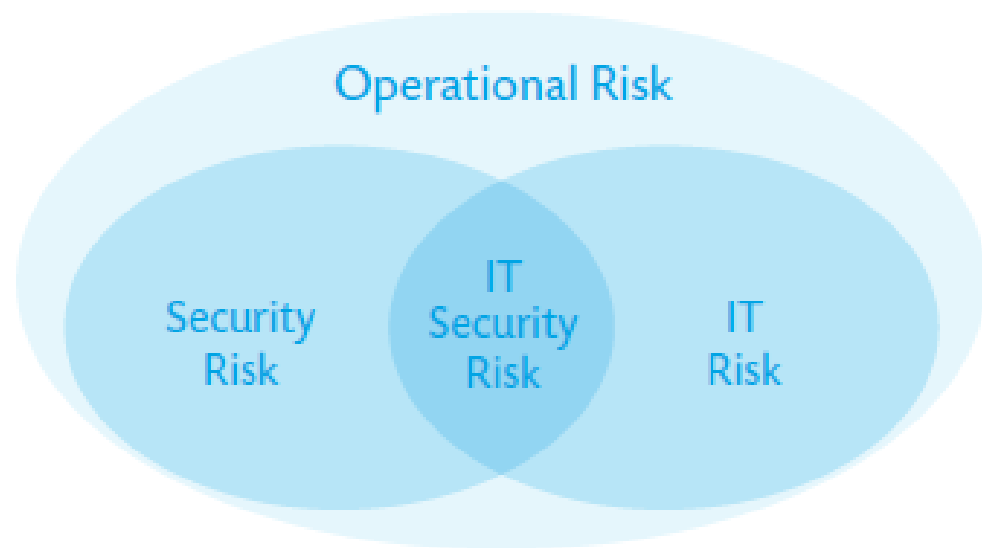
loop  
TECHNOLOGY



Questions?

# Changing Landscape

“In APRA’s view, IT security risk, (as with the broader set of IT risks) will ultimately result in a business risk exposure.”<sup>s14</sup>.



# Where to from here

- Loop is offering an Information Security Management System Review aligned to APRA PPG234
- Engagement including:
  - Workshop defining applicable requirements and how currently being met
  - Risk Assessment
  - Gap Analysis
  - Improvement Report / Implementation Plan
- Speak to a Loop Account Manager to find out more



# Aligning IT Strategy to APRA PPG234

Management of security risk in  
information and information technology