Insights into Security Policies and the University Sector

Kent Adams
Franz Eilert
Gary Gaskell
Dianna Madden
Adrian Tarca

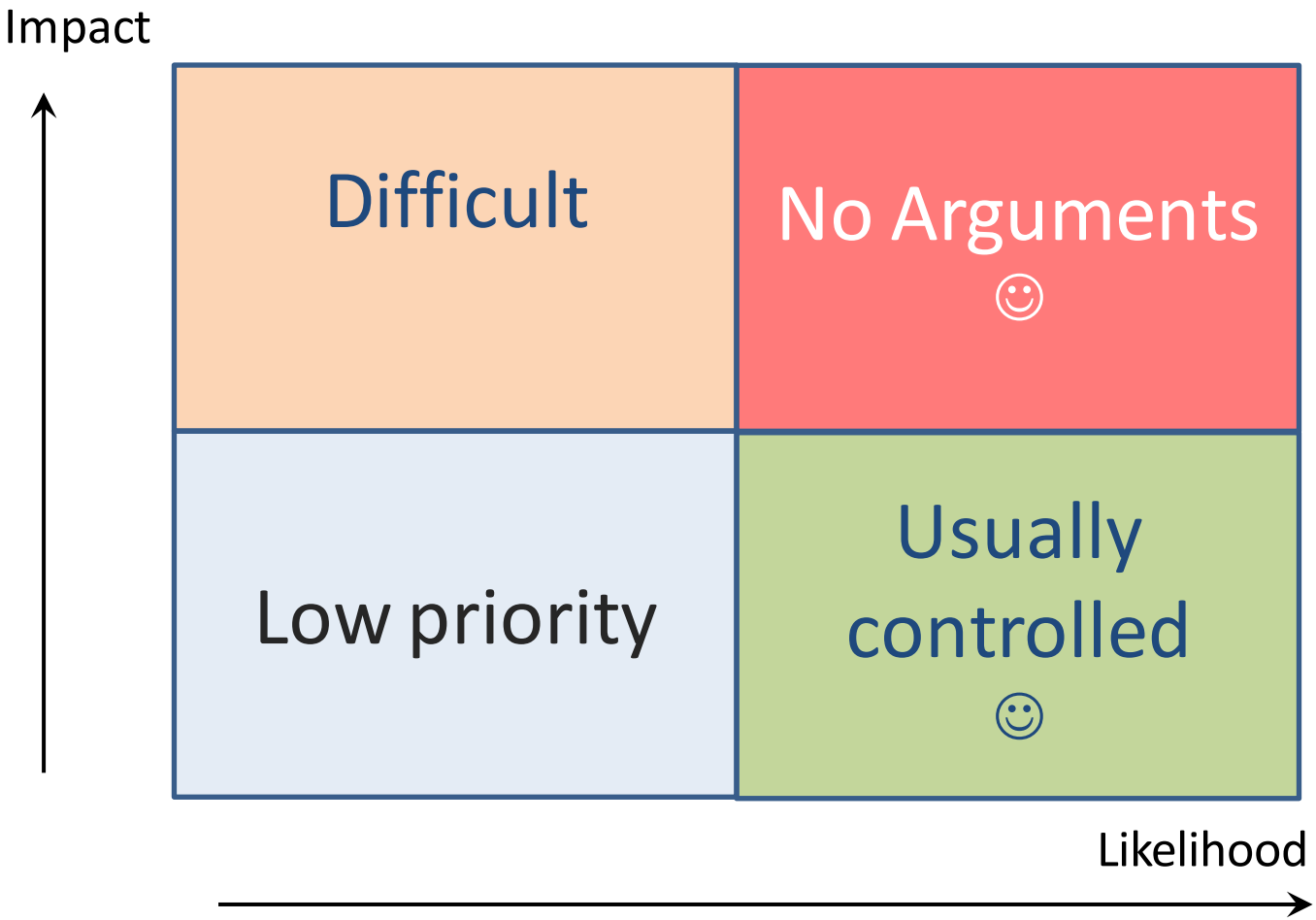
Seaforth Baptist website

Lynnemarshall.com

Overview

- Introduction – Kent Adams
- Project drivers
- Approach
- Outcomes
- Key Success Factors

Support for Controlling Security Risks



Drivers

- A%$*^%(&* --- Auditors
  - ☺
- Executive Management
  - Demonstrate sound risk management
  - “No more surprises”
- Operations Management
  - Enhance consistent application of security
    - i.e. - move to a defined level of Control Maturity

Capability Maturity Model

Optimised
Managed
Defined
Repeatable
Initial/Adhoc

The Mandate

Fix the “Security Policy”

The Approach

- Not just update IT security policies
  - Implement a framework
- Consult all stakeholders
  - Avoid the perception of a ‘power grab’
- Team approach
  - JCU staff & consultants
- Principles
  - Policy approved by an accountable person
  - Threats change – so must the response
  - Security controls are at different levels
    - “policy should match this”

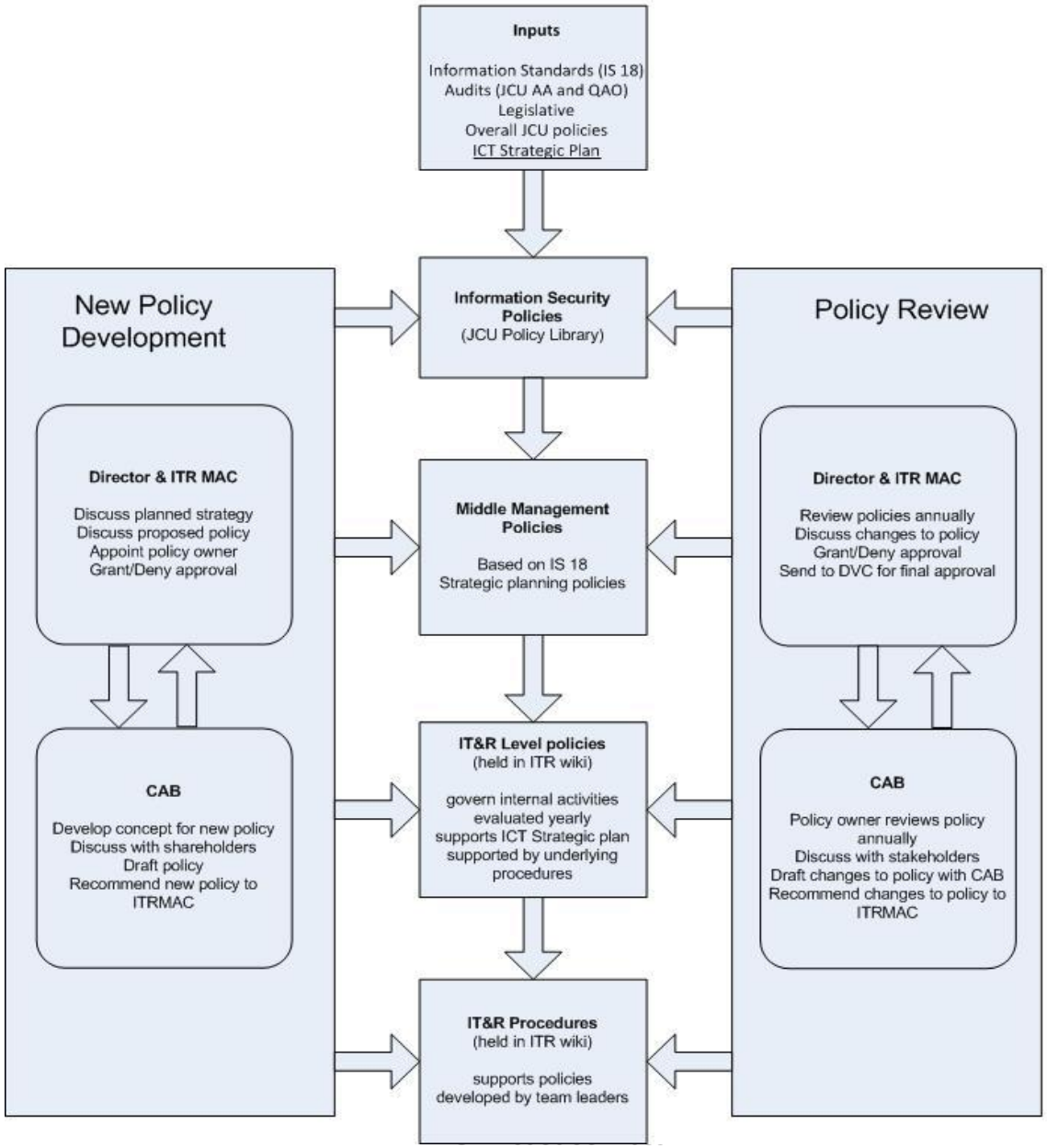
Solution – Part 1 (decomposition)

Level	Policy type	Location
Executive	Overarching information security policy	Univ Policy Library
Managerial	Corporate management policies	Univ Policy Library
Technical	Information Technology specifics	IT wiki
Operational	Procedures and “How-To” documents	IT wiki Procedure Manuals in other Business Units

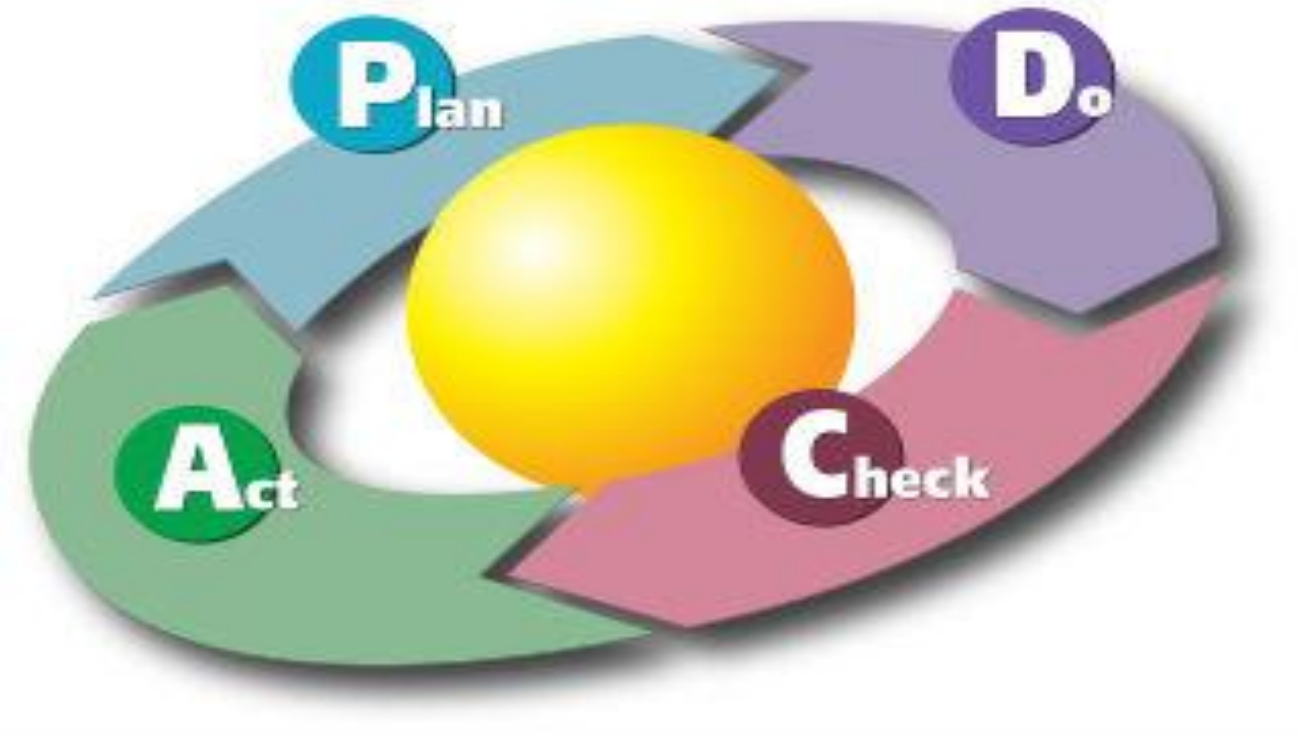

Executive Management Policy
(Information Security)
Managerial Policy
(Physical security)
IT Policy
(Physical Security of Technology Assets
Corporate Processing
Storage Devices
Communications Equipment)
Technical Standards
(IS 18)
Operational Procedures
(access to machine room)
Guidelines
(Staff Privacy)

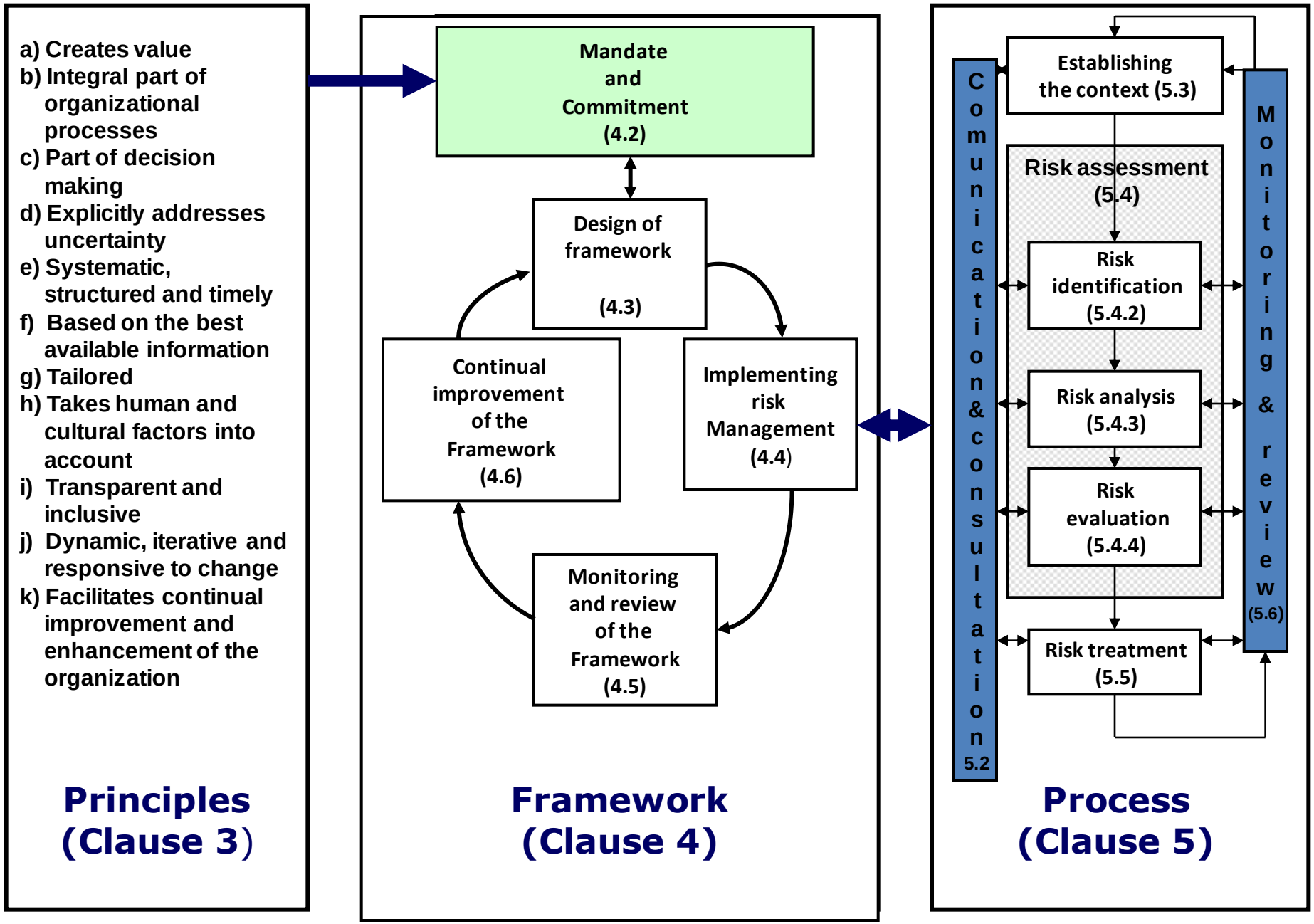
Part 2

JCU Information Security Framework – Policy Lifecycle



Solution Part 3 – (A lifecycle)





ISO 31000:2009 Figure 1 – Relationship between the principles, framework and process

Project Steps

- Know the context
- Build support (exec and IT)
- Build a good team
- Policy “gap analysis”
- Deliver the framework
- Test the framework
  - Deliver ‘high priority’ policies (see gap analysis)

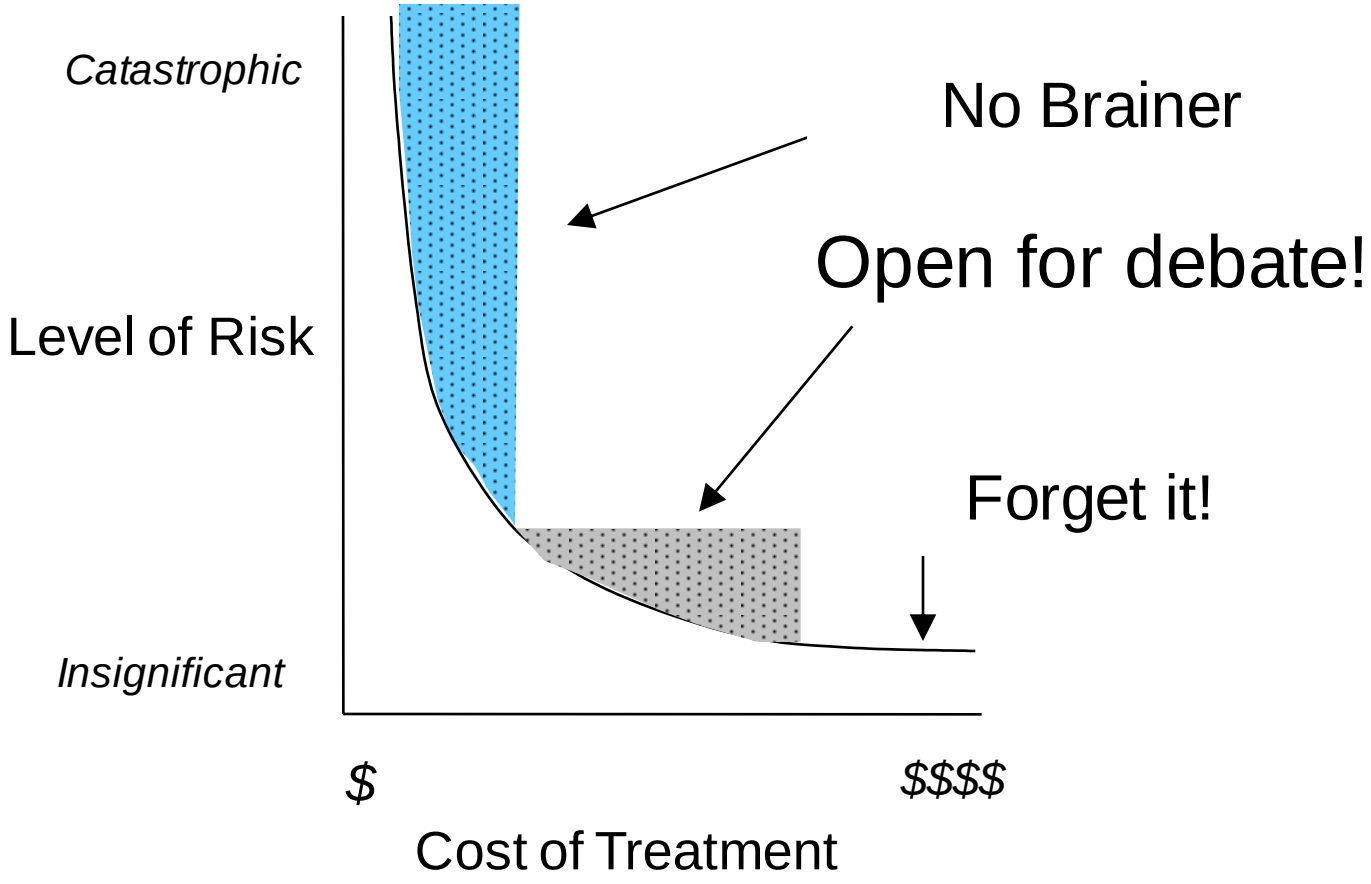
Standards and Guides

- ISO 27001, & 2
- Qld Govt Info Standard 18 – Information Security
- ISO 31000 and 31010
  - Formerly AS 4360
- ISO 27005
  - ISO 31000 interpreted for security

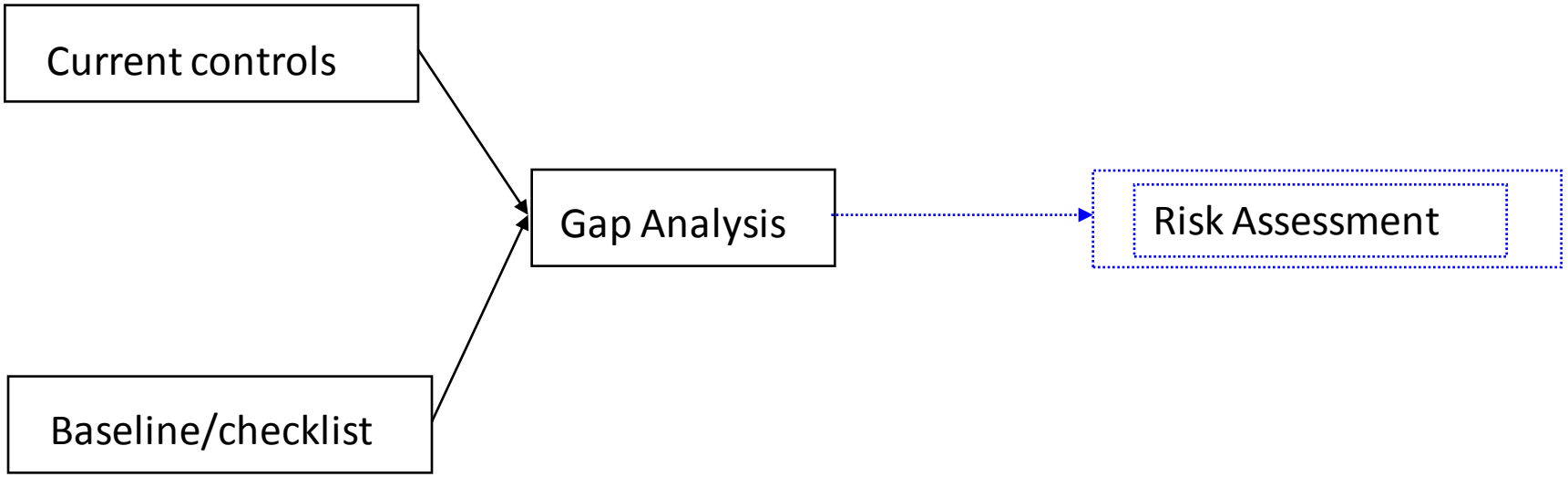
Key Success Factors

- The framework – not just a "security policy"
  - ***Stratified policy architecture***
  - Diversified policy stakeholders and approvers
- Executive support
  - Incl – Business support
- 80 – 20 rule
- A team with 'we're here to help you' message
  - Rather than . . . .

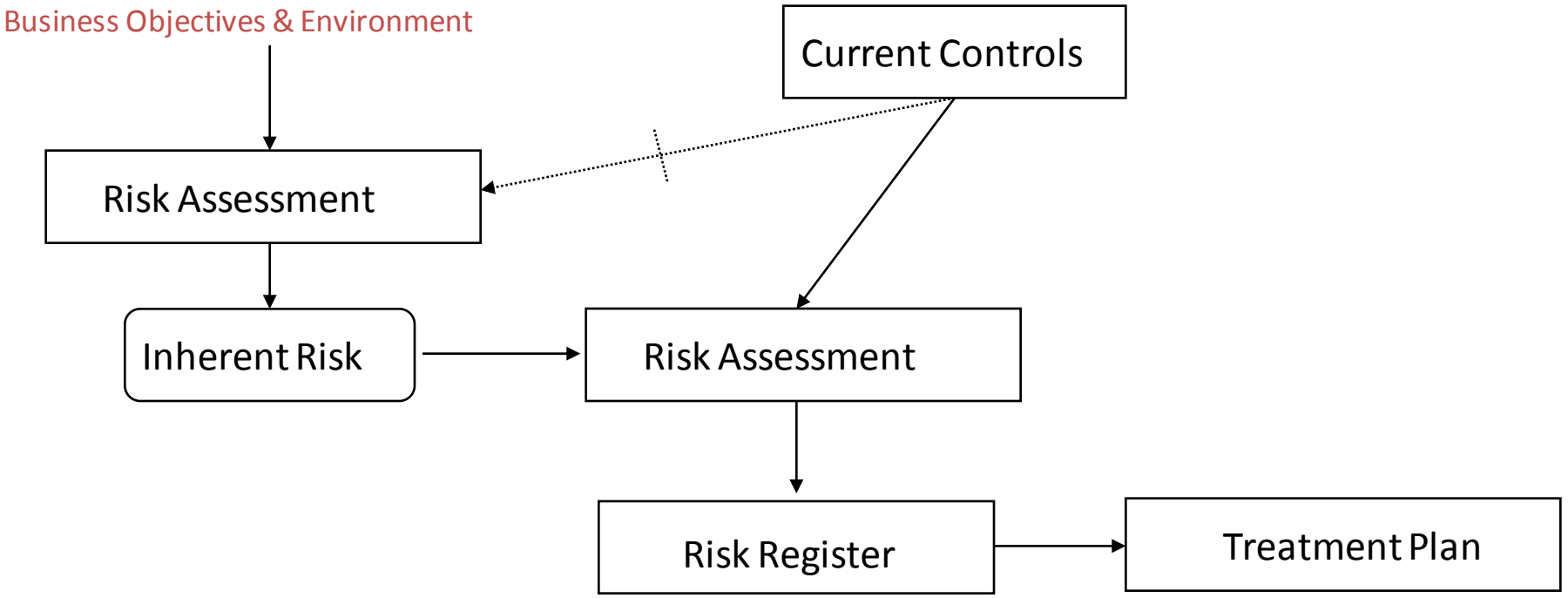
Risk Management Decisions



Gap Analysis



Inherent Risk



Executive level policy – Policy library

JCU Information Security Policy

Management level Policies – Policy library

Policy, planning & Governance	Asset mgt	HR mgt	Physical & environmental	Communications & operations mgt	Access mgt	System acquisition, dev & maint	Incident mgt	Business continuity mgt	Compliance mgt
• Use of comm & computing facilities • Statement on use of computing facil • Access to archives • Web compliance • Web security	• Pubs by staff • Records mgt • Retain email • Research repos • Student info access	• Records mgt • Retain email • Web compliance	• Cabling standards • Student info access • AV funding • Virus protection • Wireless LAN use	• Use of comm & computing facilities • Spam email • Records mgt • Retain email • Student info access • Archive access • Web security	• AARNET use • Use of comm & computing facilities • Spam email • Statement on use of computing facilities • Student info access • Archive access • Web compliance • Wireless LAN use	• A/V funding • Virus protection • Web security • Web addressing	• Spam email	• Staff pubs • Records mgt • Retain email • Research repos • Student info access • Archive access	• AARNET? • Cabling standards • Copyright • Staff pubs • Records mgt • Retain email • Research repos • Student info access • Archive access

IT&R level policies - wiki

Policy, planning & Governance	Asset mgt	HR mgt	Physical & environmental	Communications & operations mgt	Access mgt	System acquisition, dev & maint	Incident mgt	Business continuity mgt	Compliance mgt
	• Support staff home network access • Mobile phone policy			• HPRC quota • HPRC directory use		• Support staff home network access • Mobile phone policy • HPRC VM policy		• HPRC Backup • HPRC recovery of files • HPRC CVS/SVN use	

IT&R Procedures - wiki

Existing policies

Proposed policies

Might be policies

Contacts

Gary Gaskell, Infosec Services Pty Ltd
(CISSP, CISM, CISA, SBCI, MACS (Snr), CP, M App Sc, B Eng, B IT)

gary.gaskell at infosecservices.com.au
Ph 0438 603 307

You don’t have to manage risk

. . . . .