AIR NEW ZEALAND

Kia ora

A STAR ALLIANCE MEMBER

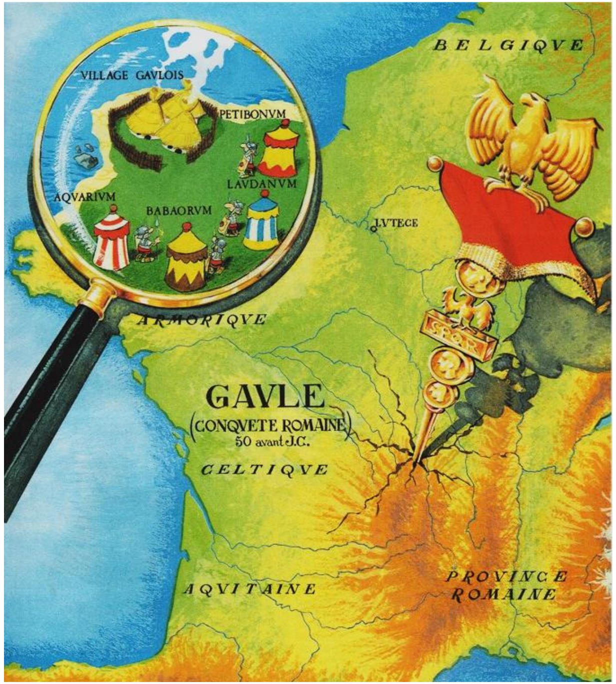
AIR NEW ZEALAND

Managing Cyber Threats and Risks at Air New Zealand

Risk NZ Conference 2017

18th August 2018

A STAR ALLIANCE MEMBER


VILLAGE GAVLOIS
PETIBONVM
LAVDANVM
AQVARIVM
BABAORVM
BELGIQVE
LVTECE
ARMORIQVE
GAVLE
(CONQVETE ROMAINE)
50 avant J.C.
CELTIQVE
AQVITAINE
PROVINCE
ROMAINE

TelstraClear

Spark nz

Fonterra

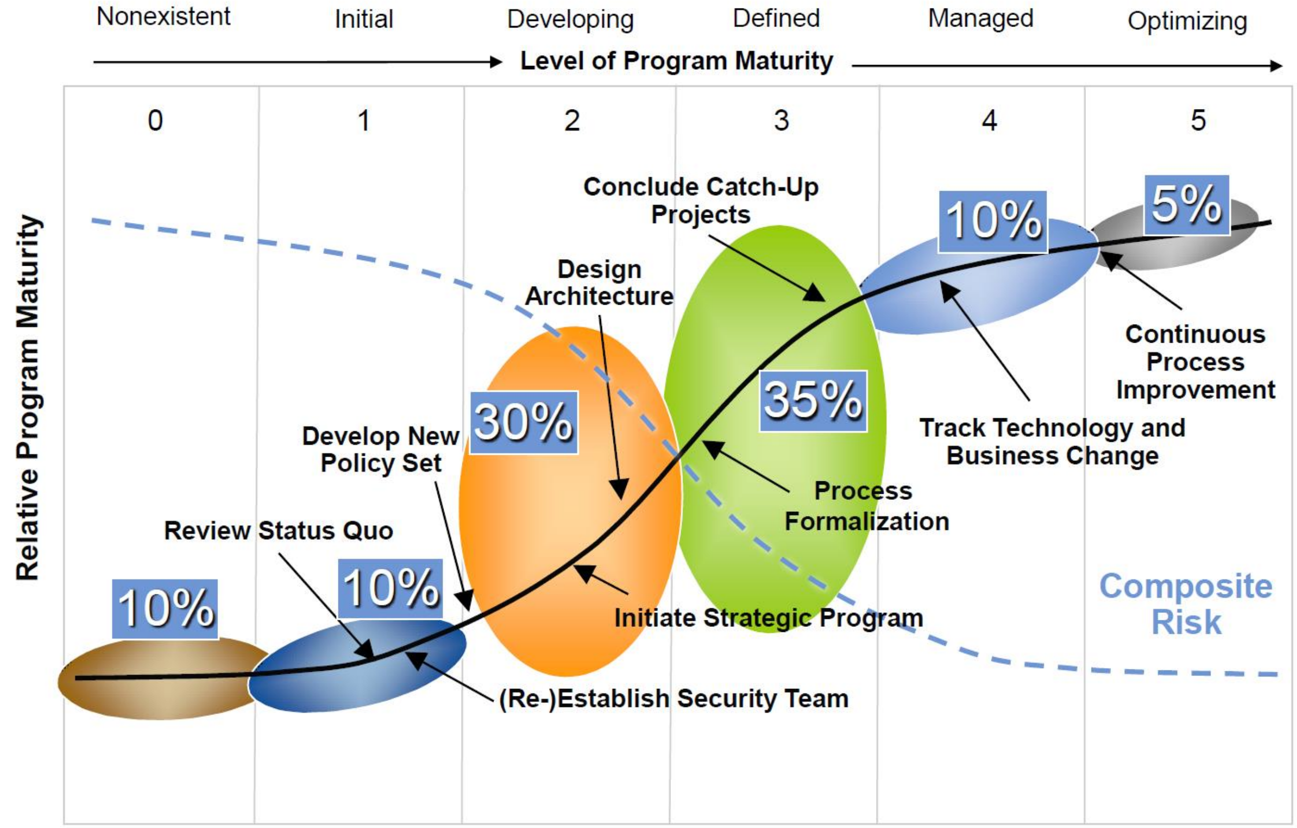
Information Security

IT Risk Management

IT Disaster Recovery

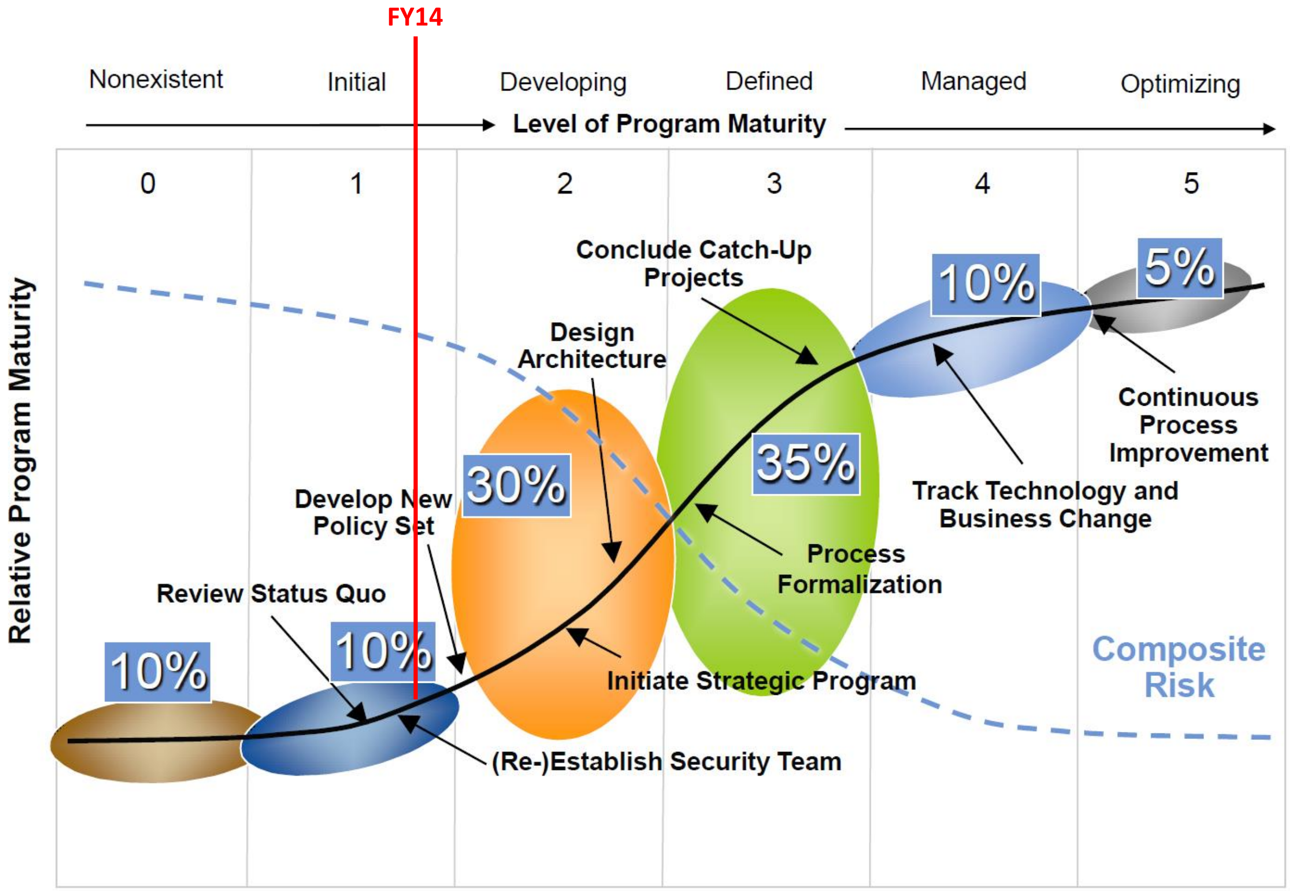
Our three-year vision

“To take a concerted step up the security maturity curve towards being world class.”



NOTE: Population distributions represent typical, large G2000-type organizations

Gartner


FY14
Nonexistent
Initial
Developing
Defined
Managed
Optimizing
Level of Program Maturity
0
1
2
3
4
5
Relative Program Maturity
10%
10%
30%
35%
10%
5%
Review Status Quo
Develop New Policy Set
Design Architecture
Conclude Catch-Up Projects
Process Formalization
Initiate Strategic Program
(Re-)Establish Security Team
Track Technology and Business Change
Continuous Process Improvement
Composite Risk

NOTE: Population distributions represent typical, large G2000-type organizations

Gartner

Programme goals

1. Improve Air New Zealand security maturity to meet the Audit Committee and ExCo expectations
2. Reduce the risk to sensitive information of unauthorised access and information leakage
3. Improve the detection capabilities for security incidents
4. Increase PCI score and ensure no penalties are enforced due to non-compliance with PCI DSS
5. Decrease the number of security-related audit findings
6. Remediate all high ‘Red Team’ and internal pen testing findings
7. Implement vendors’ best practices

Guiding principles

1. The programme will not boil the ocean; we will make targeted decisions around scope to ensure value is delivered in an incremental manner.
2. Security maturity is a journey and will take some years to achieve. However this programme will lay the foundation for the years ahead.
3. Items in scope have been assessed against industry best practise to ensure our focus is right.
4. Solutions will strike the right balance between security and UX.
5. Incumbent tools and solutions will be reused where possible.
6. Risk-based approach > Compliance-based approach

Programme Structure

Environment Hardening

Harden our client and server fleet

Network Security

Segregate our network in line with PCI requirements and security best practices to ensure our critical information assets are adequately protected from internal and external threats

Implement new firewalls and security controls at the edge of our network to stay ahead of new/emerging cyber threats

Security Monitoring

Improve detection and reporting capabilities by implementing a SIEM (Security Information and Event Management) platform and supporting processes to provide better security insights and real-time understanding of our security posture

Identity Management

Ensures the right individuals have access to the right digital resources at the right time

PCI Remediation

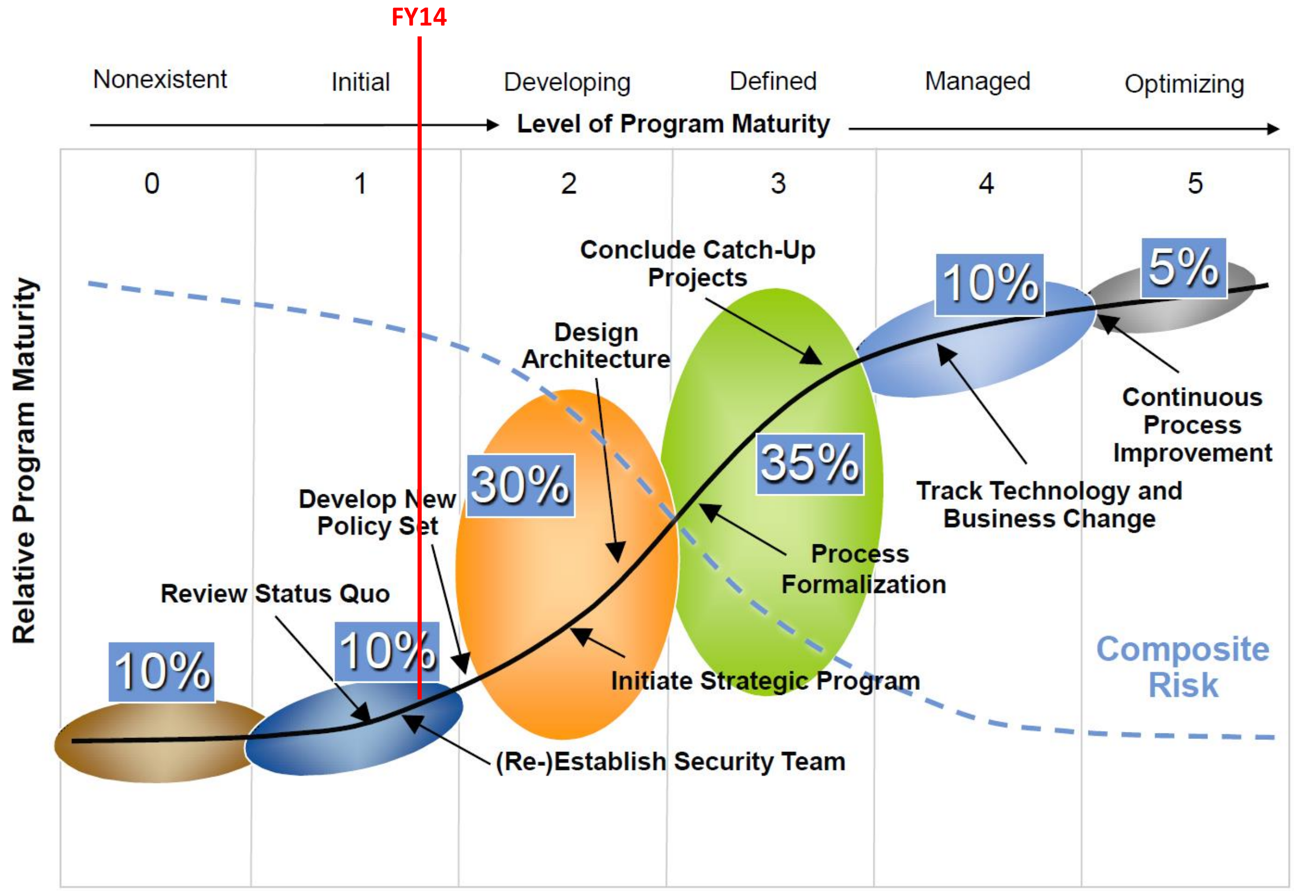
Address specific areas of PCI non-compliance and governance defects.

This includes:

- Implementing a PCI scanning tool to discover unmasked or exposed credit card data at rest
- Producing security policies and standards

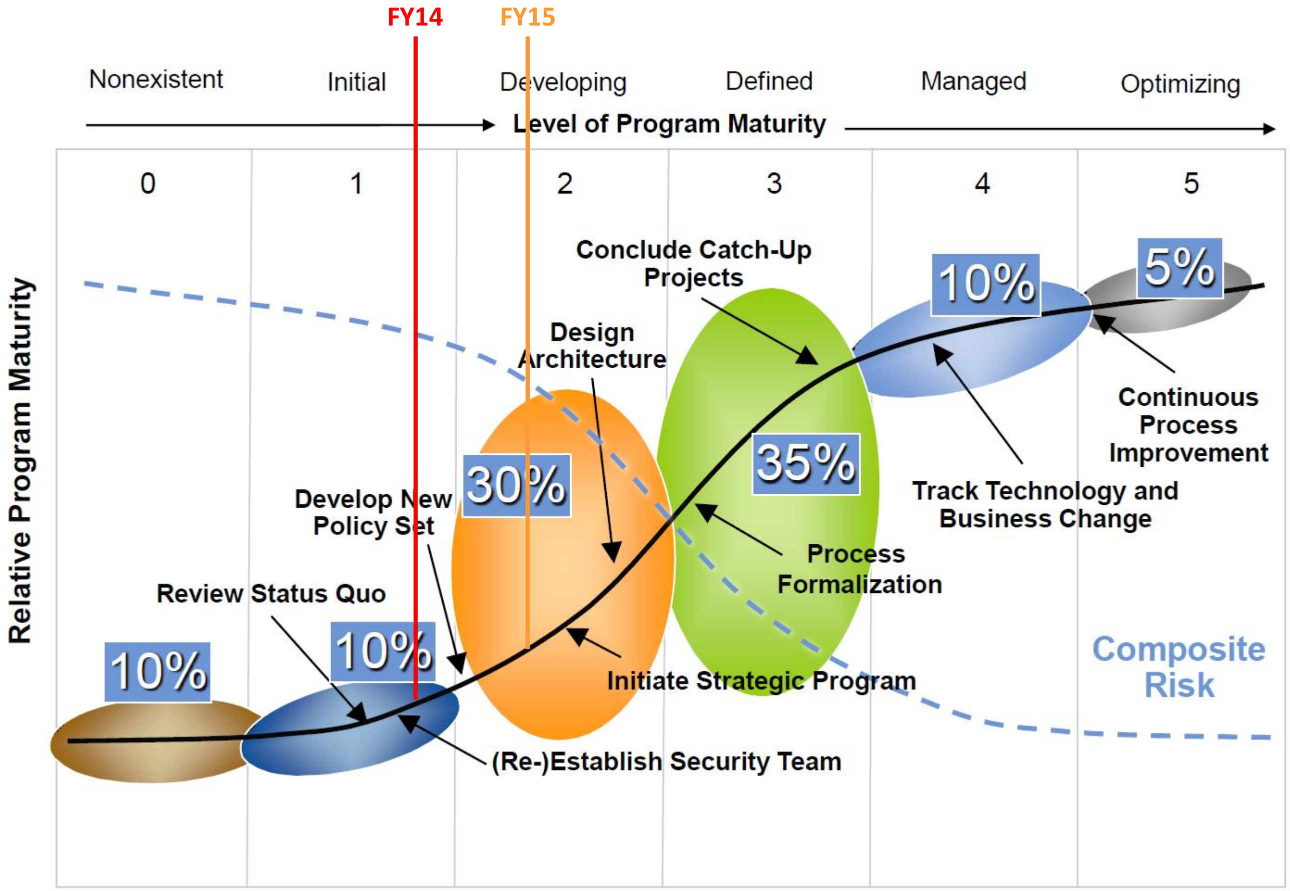
Assurance activities, scorecard & metrics

1. Improve Air New Zealand security maturity to meet the Audit Committee and ExCo expectations

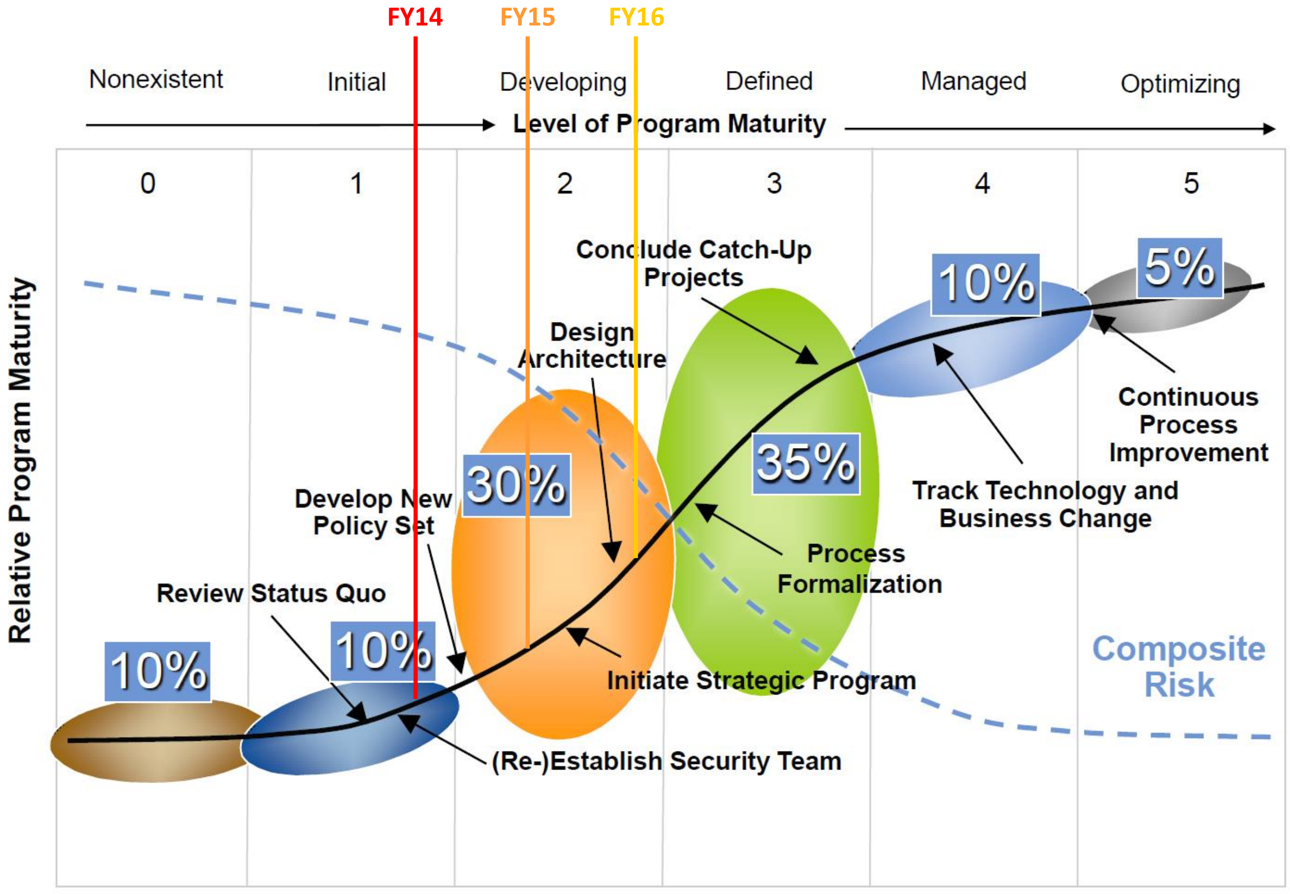

FY14
Nonexistent
Initial
Developing
Defined
Managed
Optimizing
Level of Program Maturity
0
1
2
3
4
5
Relative Program Maturity
10%
10%
30%
35%
10%
5%
Review Status Quo
Develop New Policy Set
(Re-)Establish Security Team
Initiate Strategic Program
Design Architecture
Conclude Catch-Up Projects
Process Formalization
Track Technology and Business Change
Continuous Process Improvement
Composite Risk

NOTE: Population distributions represent typical, large G2000-type organizations

Gartner

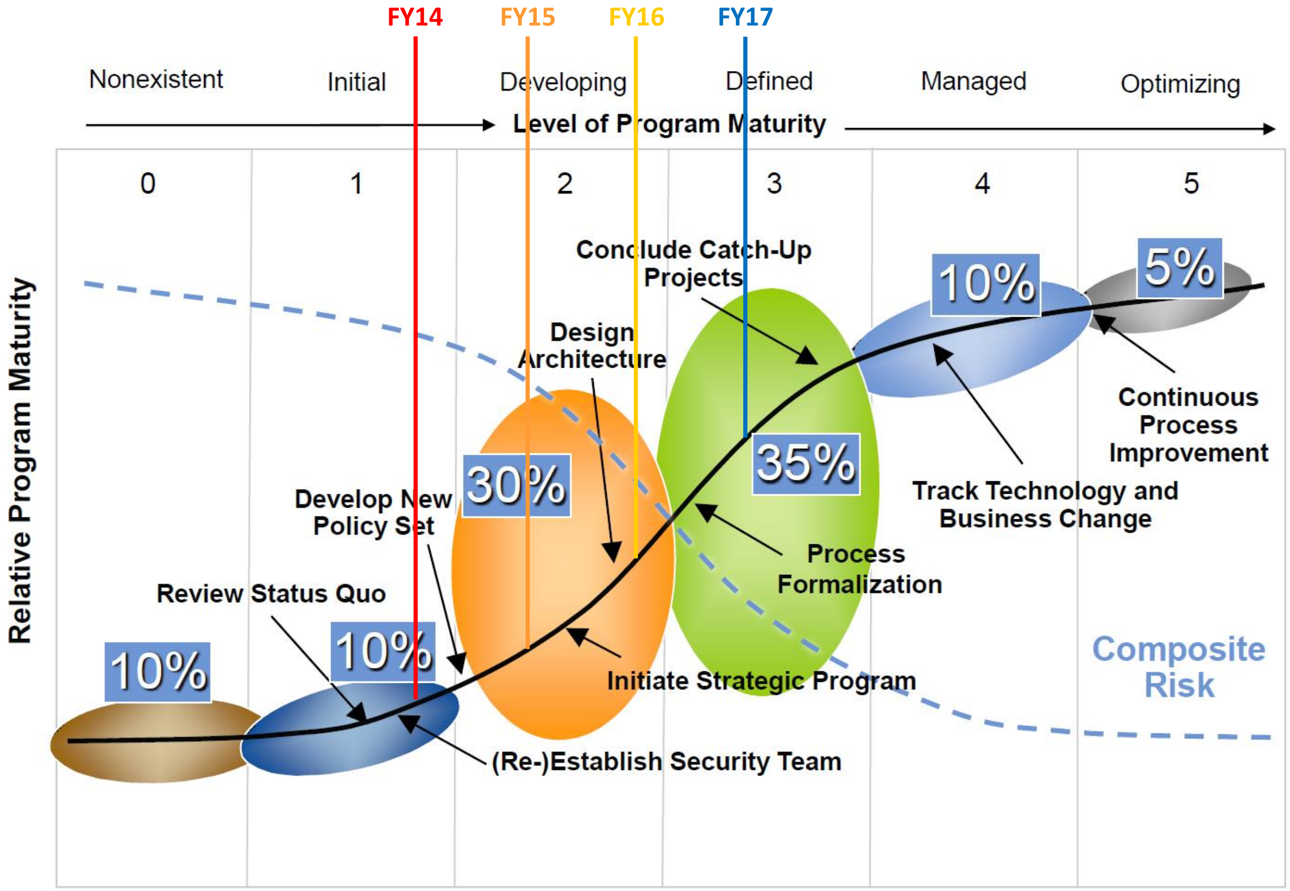

FY14
FY15
Nonexistent
Initial
Developing
Defined
Managed
Optimizing
Level of Program Maturity
0
1
2
3
4
5
Relative Program Maturity
10%
10%
30%
35%
10%
5%
Review Status Quo
Develop New Policy Set
Design Architecture
Conclude Catch-Up Projects
Process Formalization
Track Technology and Business Change
Continuous Process Improvement
Initiate Strategic Program
(Re-)Establish Security Team
Composite Risk

NOTE: Population distributions represent typical, large G2000-type organizations


FY14
FY15
FY16
Nonexistent
Initial
Developing
Defined
Managed
Optimizing
Level of Program Maturity
0
1
2
3
4
5
Relative Program Maturity
10%
10%
30%
35%
10%
5%
Review Status Quo
Develop New Policy Set
Design Architecture
Conclude Catch-Up Projects
Process Formalization
Track Technology and Business Change
Continuous Process Improvement
Initiate Strategic Program
(Re-)Establish Security Team
Composite Risk

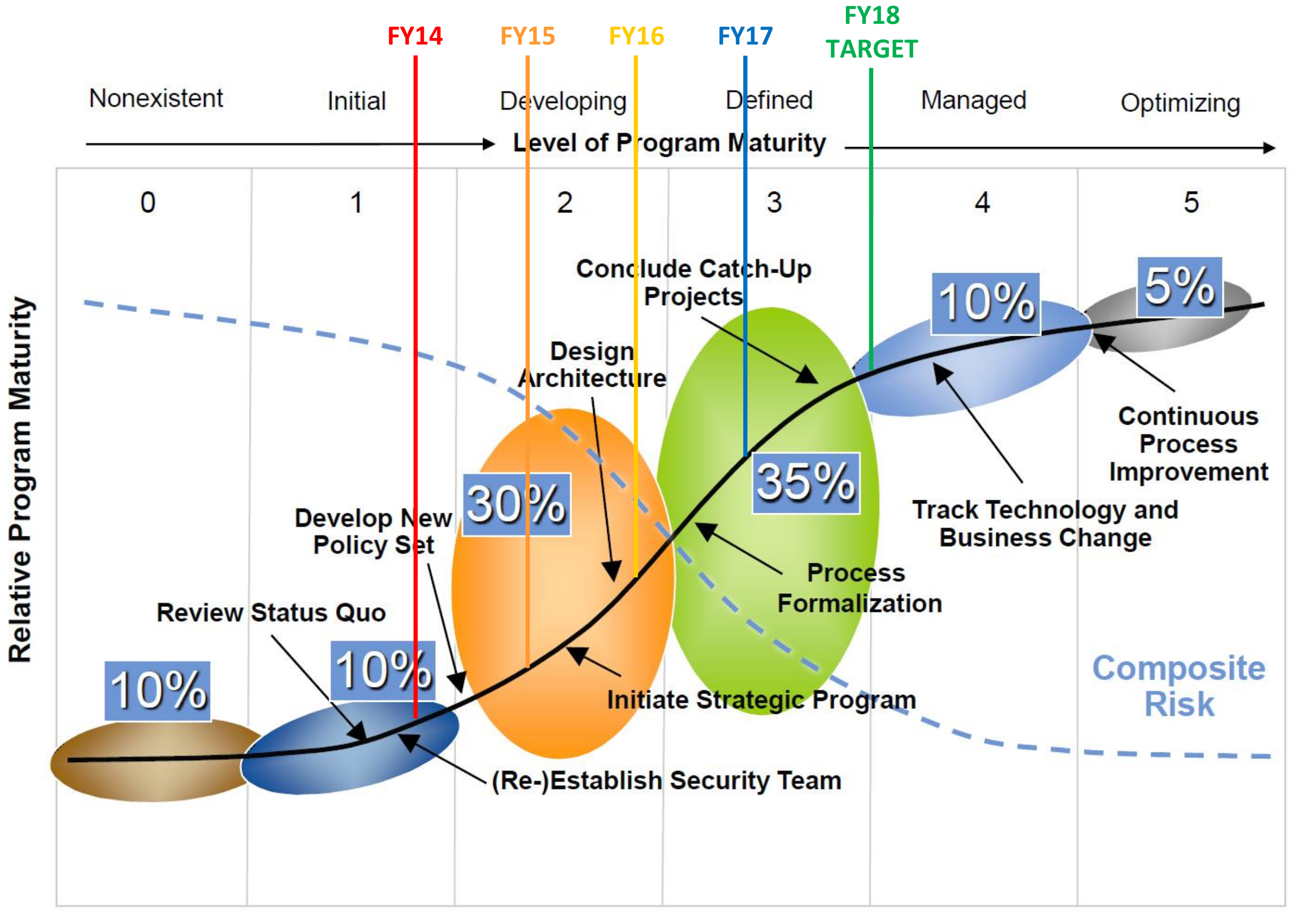
NOTE: Population distributions represent typical, large G2000-type organizations

Gartner


FY14
FY15
FY16
FY17
Nonexistent
Initial
Developing
Defined
Managed
Optimizing
Level of Program Maturity
0
1
2
3
4
5
Relative Program Maturity
10%
10%
30%
35%
10%
5%
Review Status Quo
Develop New Policy Set
Design Architecture
Conclude Catch-Up Projects
Process Formalization
Track Technology and Business Change
Continuous Process Improvement
Initiate Strategic Program
(Re-)Establish Security Team
Composite Risk

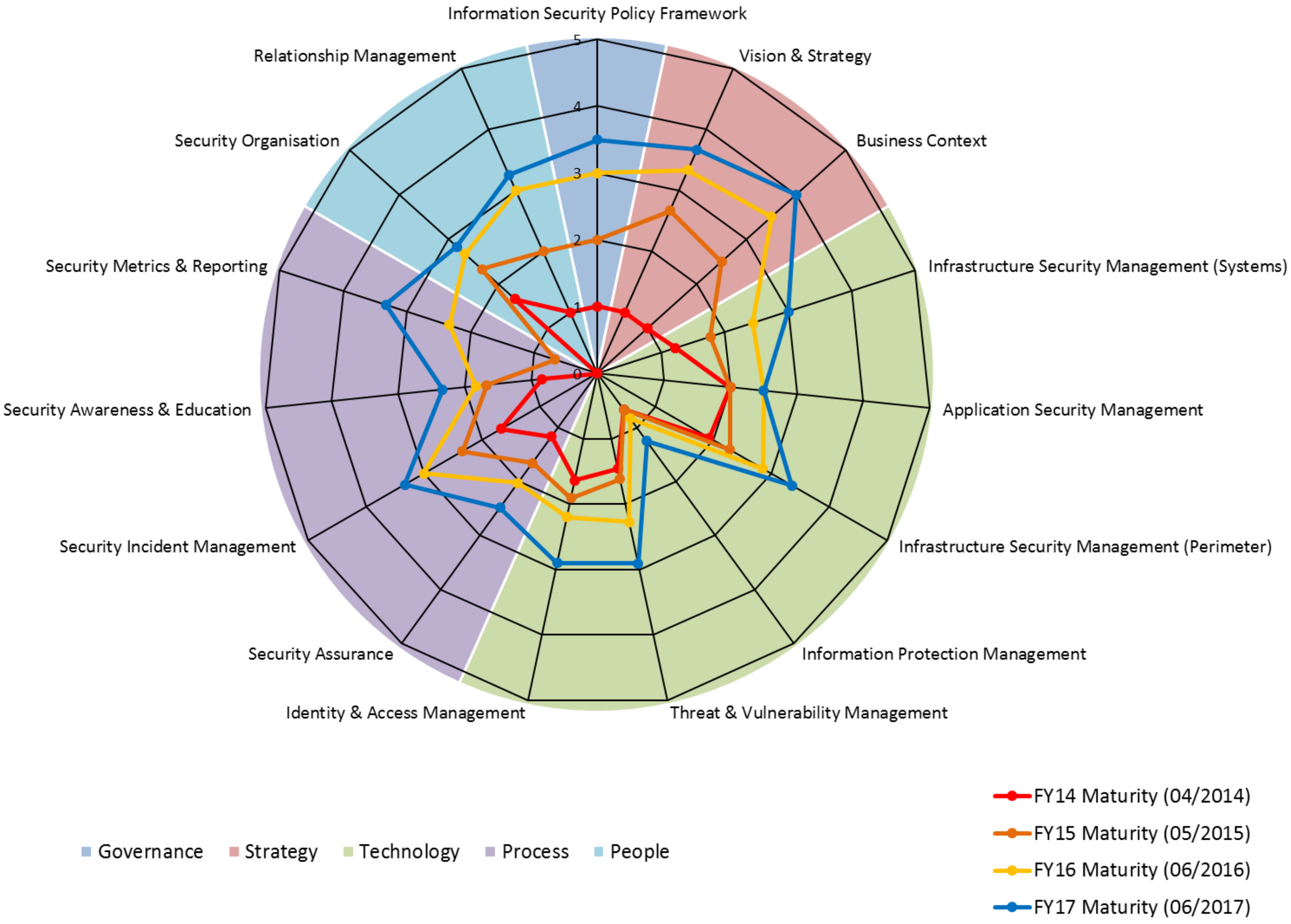
NOTE: Population distributions represent typical, large G2000-type organizations

Gartner

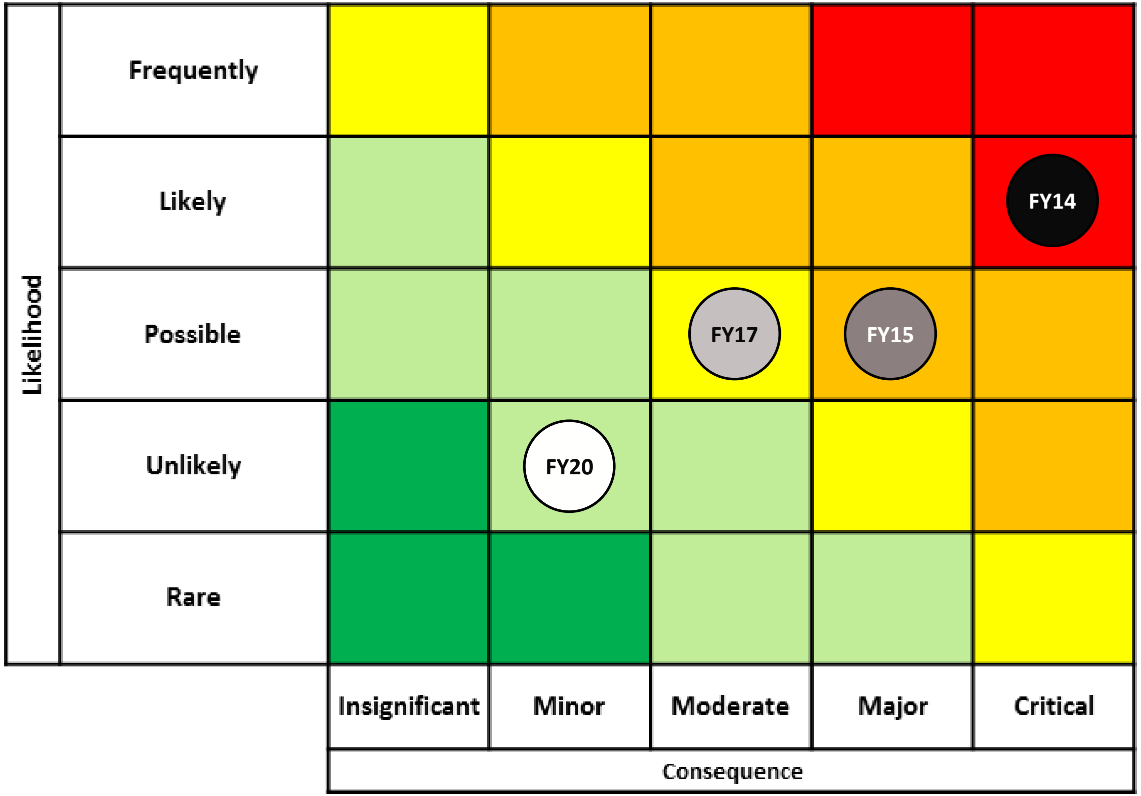


NOTE: Population distributions represent typical, large G2000-type organizations

Gartner


Information Security Policy Framework
Vision & Strategy
Business Context
Infrastructure Security Management (Systems)
Application Security Management
Infrastructure Security Management (Perimeter)
Information Protection Management
Threat & Vulnerability Management
Identity & Access Management
Security Assurance
Security Incident Management
Security Awareness & Education
Security Metrics & Reporting
Security Organisation
Relationship Management
5
4
3
2
1
0
Governance
Strategy
Technology
Process
People
FY14 Maturity (04/2014)
FY15 Maturity (05/2015)
FY16 Maturity (06/2016)
FY17 Maturity (06/2017)

2. Reduce the risk to sensitive information of unauthorised access and information leakage



Likelihood	Frequently					
	Likely					FY14
	Possible			FY17	FY15	
	Unlikely		FY20			
	Rare					
		Insignificant	Minor	Moderate	Major	Critical
		Consequence				

- 🟩 Very Low
- 🟩 Low
- 🟨 Medium
- 🟧 High
- 🟥 Very High

No major security incident over the last 3 years

3. Improve the detection capabilities for security incidents

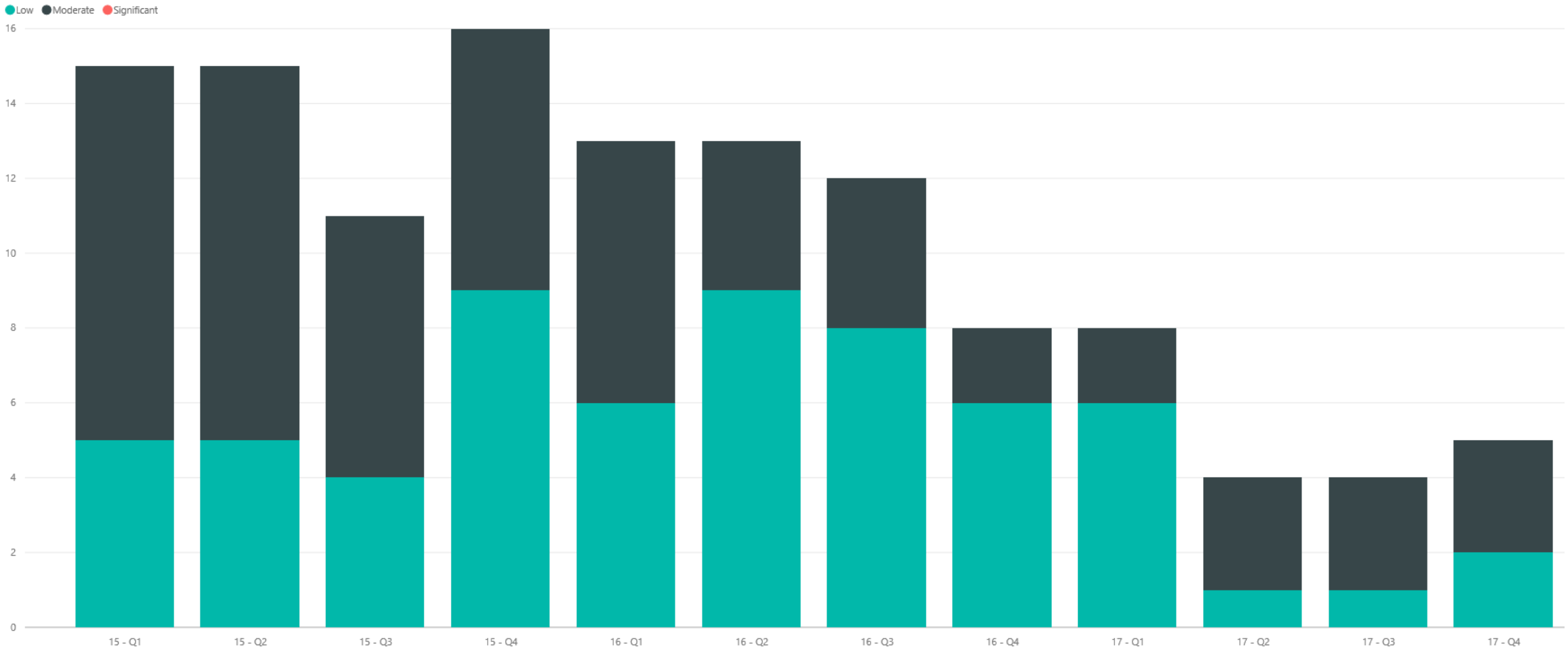
Significant improvement in terms of operational readiness

Number of devices logging to SIEM: ~1900

4. Increase PCI score and ensure no penalties are enforced due to non-compliance with PCI DSS

More than 100% increase in PCI compliance score between Dec 2014 and Dec 2016

5. Decrease the number of security-related audit findings


● Low
● Moderate
● Significant
16
14
12
10
8
6
4
2
0
15 - Q1
15 - Q2
15 - Q3
15 - Q4
16 - Q1
16 - Q2
16 - Q3
16 - Q4
17 - Q1
17 - Q2
17 - Q3
17 - Q4

6. Remediate all high ‘Red Team’ and internal pen testing findings

x3 ‘Red Team’ exercises (conducted by different third-parties) since mid-2015, unable to establish a foothold into the internal Air New Zealand network or gain access to sensitive data

7. Implement vendors’ best practices

- All Air NZ laptops received full security suite (e.g. EMET, BitLocker, Cisco AMP)
- 295 public facing computers at 22 NZ airports updated with security hardening configuration and tools, incl. application whitelisting
- 14 domestic airports further secured with network port security to prevent non-Air NZ devices being plugged in
- All system administrators issued with a 2FA token
- Significant reduction in number of Windows domain administrators, from 26 down to 8
- Active Directory hardening complete; the level of compliance with security best practices and Microsoft recommendations (using CIS benchmark) from 49% to 91% with no adverse effects to the production environment.
- Windows 2012 Server hardening complete; the level of compliance with security best practices and Microsoft recommendations has gone (using CIS benchmark) from 67% up to 91%
- Windows 7 SOE hardening complete; the level of compliance with security best practices and Microsoft recommendations (using CIS benchmark) has gone from 42% up to 85%
- New password policy for both privileged and ‘standard’ users
- Proxy consolidation: implementation of Cisco proxies
- Firewall migration from Checkpoint to Cisco underway

(Personal) key takeaways

Have a well-structured and coherent one-pager that represents your transformation programme, incl. visuals, drivers & goals, scope (in and out) and metrics

“Dream big”: be ambitious and ready to “knock the knockers”

Setup a powerful Steering Committee with reps from across the business (IT/Digital, GRC, Legal)

Do not underestimate operational impact but be ruthless when it comes to implementing your programme

Assurance activities are as important as the strength and quality of your controls

Baseline initial state and report on progress to key stakeholders on a regular basis

Define ASMART objectives/targets

“No bullshit” policy: be open, honest and transparent

Information Security is not rocket-science: do not reinvent the wheel and leverage best practices and vendors’ recommendation as much as you can

This is a transformation, not a change: forget about v1.2 and think v2.0 instead

This a cultural shift: make sure systems & network admins, and outsourcers, are on board. Define expectations early, agree on standards, communicate, follow through and measure.

Ban the following quotes (*):

“Why would we change, it’s always been like that”
“It’s too hard”
“I can’t do my job anymore”

Success depends more on your overall vision, your ability to lead and the quality of the people & project team than on funding

Air New Zealand won the 2016 iSANZ ‘Best Security Project/Initiative’ Award for its Information Security Transformation programme

AIR NEW ZEALAND

Thank you

A STAR ALLIANCE MEMBER