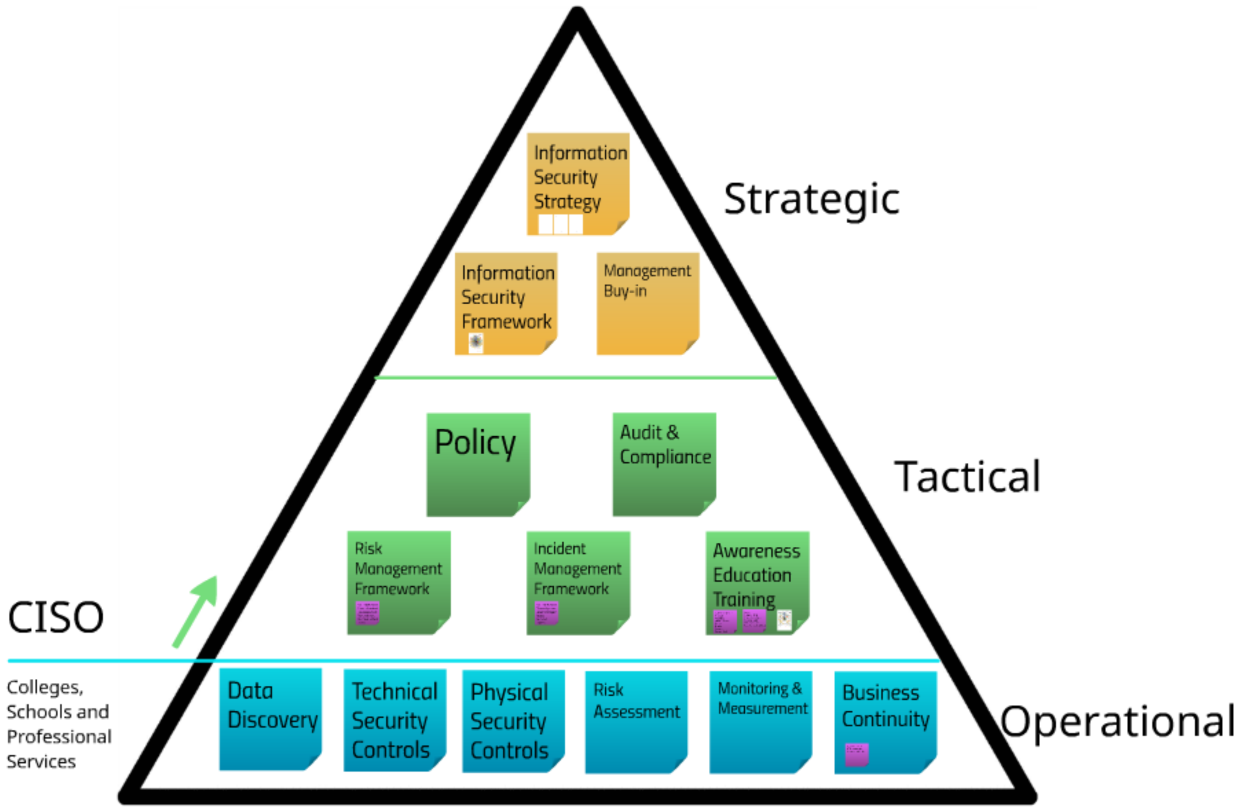
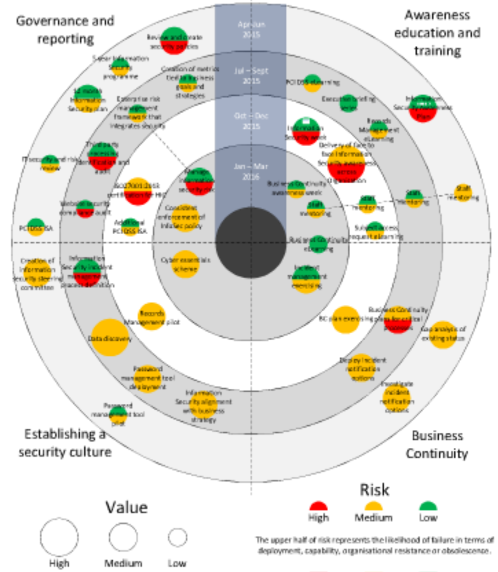
INFORMATION SECURITY ELEMENTS


Information Security Strategy
Information Security Framework
Management Buy-in
Strategic
Policy
Audit & Compliance
Tactical
Risk Management Framework
Incident Management Framework
Awareness Education Training
CISO
Colleges, Schools and Professional Services
Data Discovery
Technical Security Controls
Physical Security Controls
Risk Assessment
Monitoring & Measurement
Business Continuity
Operational

University of Dundee
Information Security Plan 2015/16

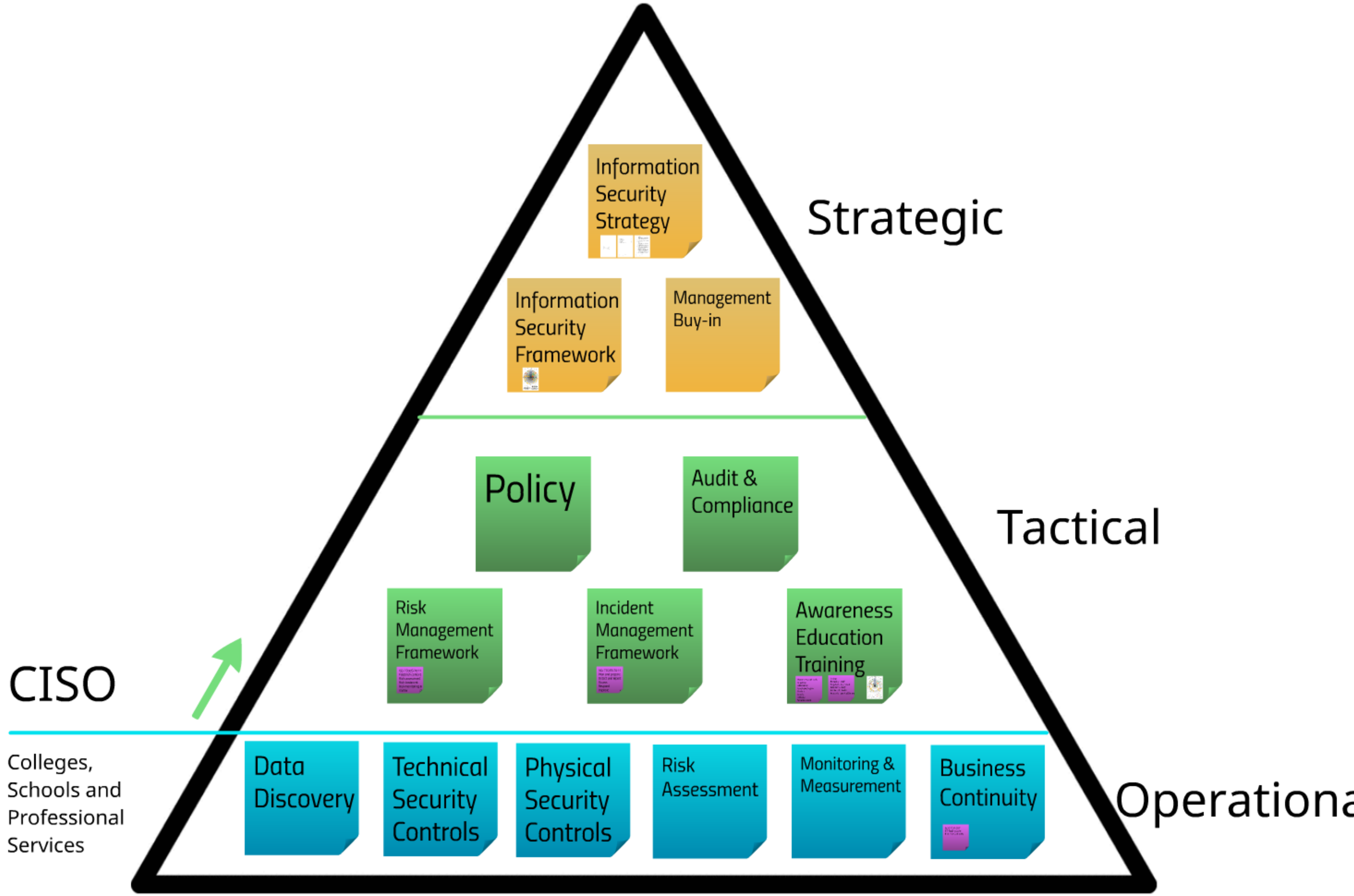


Value represents the potential benefits that can be derived and has been assessed by effect on cost, positive behaviour change, adherence to compliance and functional benefit.

The upper half of risk represents the likelihood of failure in terms of deployment, capability, organisational resistance or obsolescence.

The lower half of risk represents the impact should the activity not be undertaken in terms of reputational damage, operational or financial exposure.

INFORMATION SECURITY ELEMENTS



Strategic

Information Security Strategy

Information Security Framework

Management Buy-in

Tactical

Policy

Audit & Compliance

Risk Management Framework

Incident Management Framework

Awareness Education Training

CISO

Colleges, Schools and Professional Services

Operationa

Data Discovery

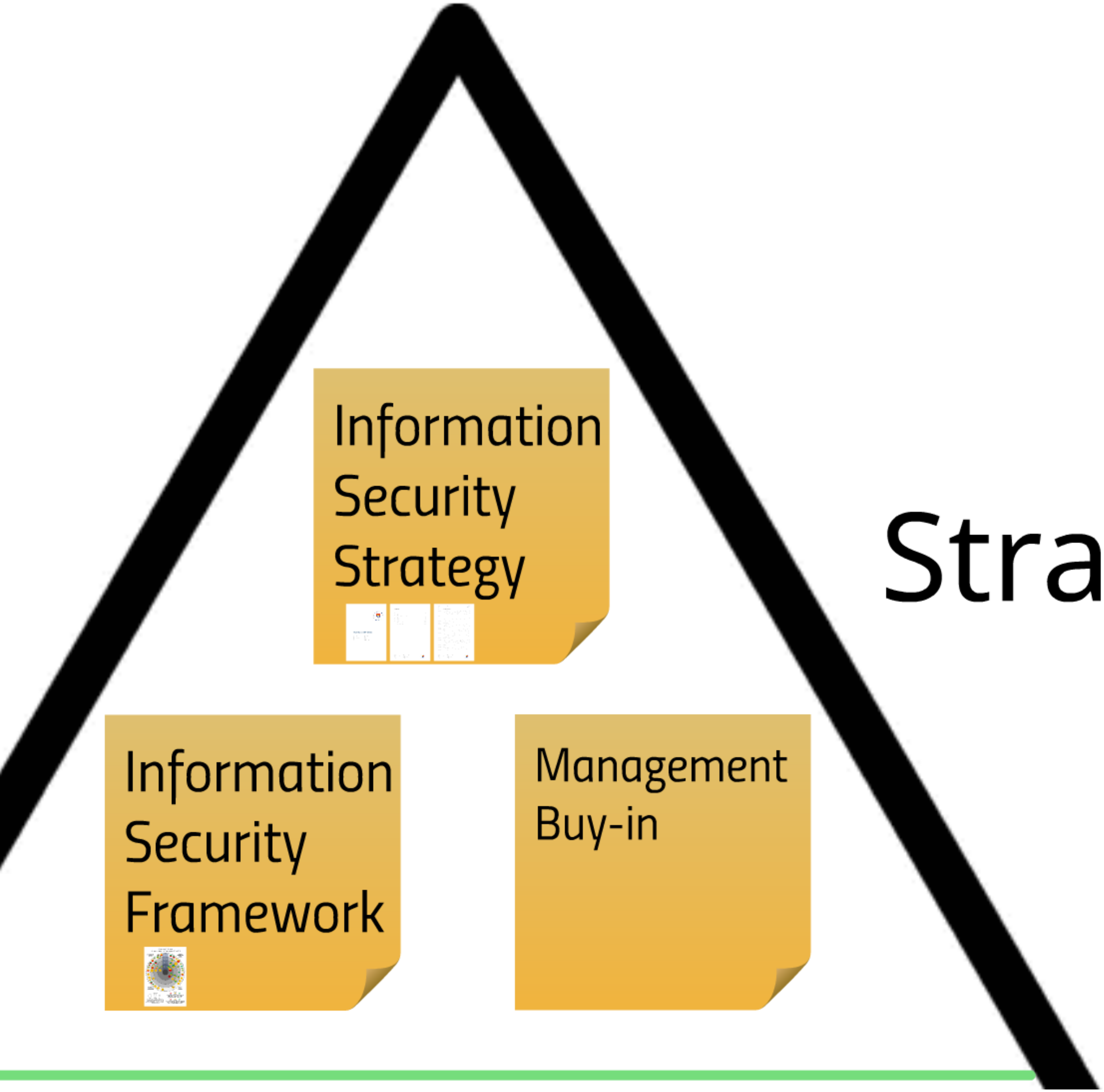
Technical Security Controls

Physical Security Controls

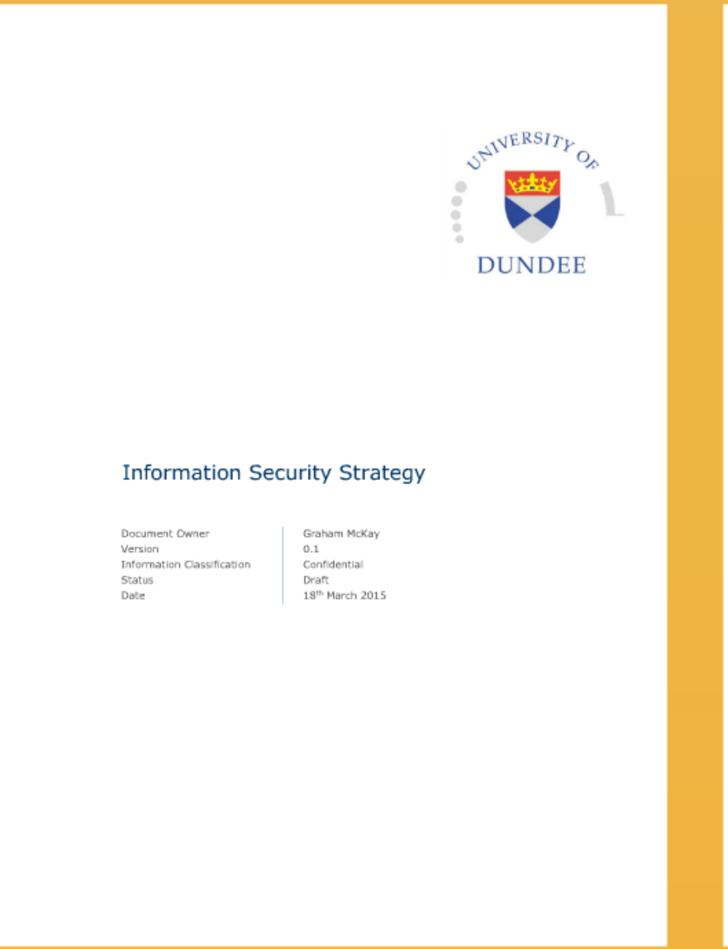
Risk Assessment

Monitoring & Measurement

Business Continuity


Information Security Strategy
Information Security Framework
Management Buy-in

Strategic



UNIVERSITY OF DUNDEE

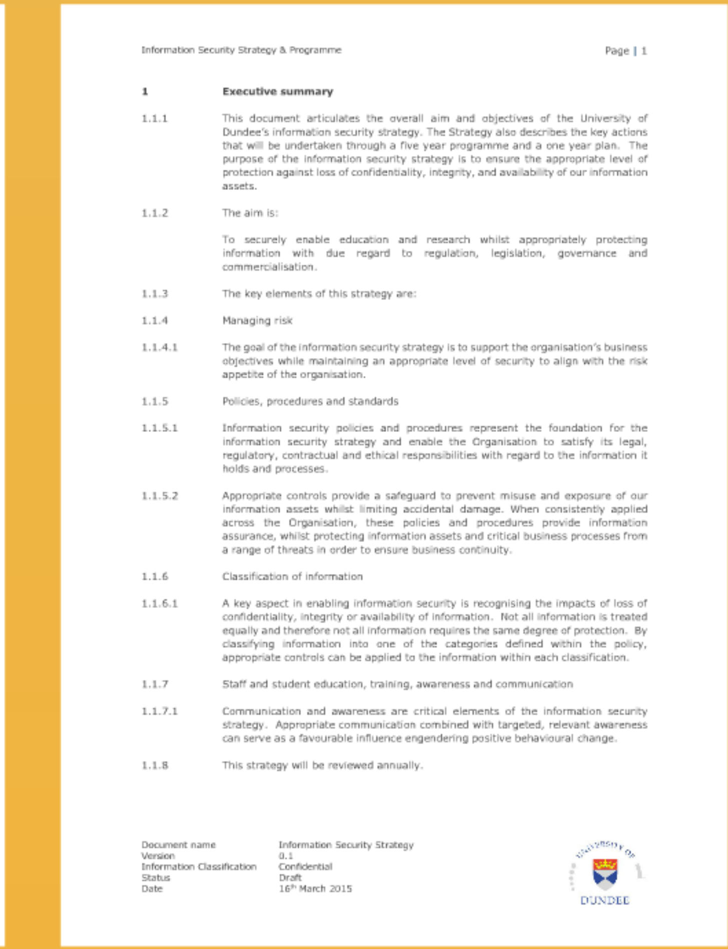
Information Security Strategy

Document Owner	Graham McKay
Version	0.1
Information Classification	Confidential
Status	Draft
Date	18th March 2015

Contents

Document name	Information Security Strategy
Version	0.1
Information Classification	Confidential
Status	Draft
Date	16th March 2015

DUNDEE



Information Security Strategy & Programme Page | 1

1 Executive summary

1.1.1 This document articulates the overall aim and objectives of the University of Dundee's information security strategy. The Strategy also describes the key actions that will be undertaken through a five year programme and a one year plan. The purpose of the information security strategy is to ensure the appropriate level of protection against loss of confidentiality, integrity, and availability of our information assets.

1.1.2 The aim is:

To securely enable education and research whilst appropriately protecting information with due regard to regulation, legislation, governance and commercialisation.

1.1.3 The key elements of this strategy are:

1.1.4 Managing risk

1.1.4.1 The goal of the information security strategy is to support the organisation's business objectives while maintaining an appropriate level of security to align with the risk appetite of the organisation.

1.1.5 Policies, procedures and standards

1.1.5.1 Information security policies and procedures represent the foundation for the information security strategy and enable the Organisation to satisfy its legal, regulatory, contractual and ethical responsibilities with regard to the information it holds and processes.

1.1.5.2 Appropriate controls provide a safeguard to prevent misuse and exposure of our information assets whilst limiting accidental damage. When consistently applied across the Organisation, these policies and procedures provide information assurance, whilst protecting information assets and critical business processes from a range of threats in order to ensure business continuity.

1.1.6 Classification of information

1.1.6.1 A key aspect in enabling information security is recognising the impacts of loss of confidentiality, integrity or availability of information. Not all information is treated equally and therefore not all information requires the same degree of protection. By classifying information into one of the categories defined within the policy, appropriate controls can be applied to the information within each classification.

1.1.7 Staff and student education, training, awareness and communication

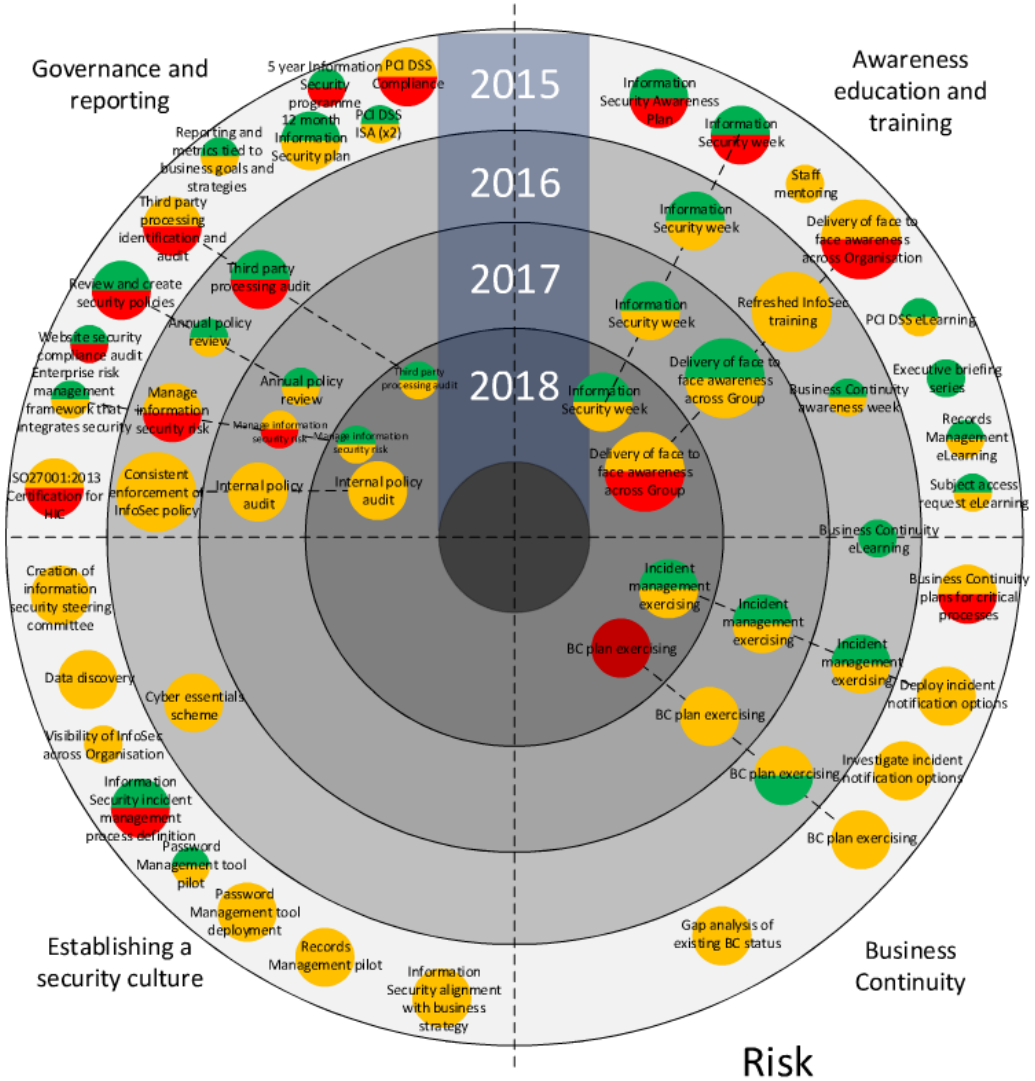
1.1.7.1 Communication and awareness are critical elements of the information security strategy. Appropriate communication combined with targeted, relevant awareness can serve as a favourable influence engendering positive behavioural change.

1.1.8 This strategy will be reviewed annually.

Document name	Information Security Strategy
Version	0.1
Information Classification	Confidential
Status	Draft
Date	16th March 2015

DUNDEE

University of Dundee
Information Security Programme 2015-2018


2015
2016
2017
2018
Governance and reporting
5 year Information Security programme
PCI DSS Compliance
PCI DSS ISA (x2)
12 month Information Security plan
Reporting and metrics tied to business goals and strategies
Third party processing identification and audit
Third party processing audit
Third party processing audit
Review and create security policies
Annual policy review
Annual policy review
Website security compliance audit
Enterprise risk management framework that integrates security
Manage information security risk
Manage information security risk
Manage information security risk
ISO27001:2013 Certification for HIC
Consistent enforcement of InfoSec policy
Internal policy audit
Internal policy audit
Awareness education and training
Information Security Awareness Plan
Information Security week
Staff mentoring
Information Security week
Delivery of face to face awareness across Organisation
Refreshed InfoSec training
PCI DSS eLearning
Information Security week
Delivery of face to face awareness across Group
Executive briefing series
Business Continuity awareness week
Information Security week
Delivery of face to face awareness across Group
Records Management eLearning
Subject access request eLearning
Business Continuity eLearning
Establishing a security culture
Creation of information security steering committee
Data discovery
Cyber essentials scheme
Visibility of InfoSec across Organisation
Information Security incident management process definition
Password Management tool pilot
Password Management tool deployment
Records Management pilot
Information Security alignment with business strategy
Business Continuity
Business Continuity plans for critical processes
Incident management exercising
Incident management exercising
Incident management exercising
BC plan exercising
Deploy incident notification options
BC plan exercising
BC plan exercising
Investigate incident notification options
BC plan exercising
Gap analysis of existing BC status

Value

High

Medium

Low

Value represents the potential benefits that can be derived and has been assessed by effect on cost, positive behaviour change, adherence to compliance and functional benefit.

Risk

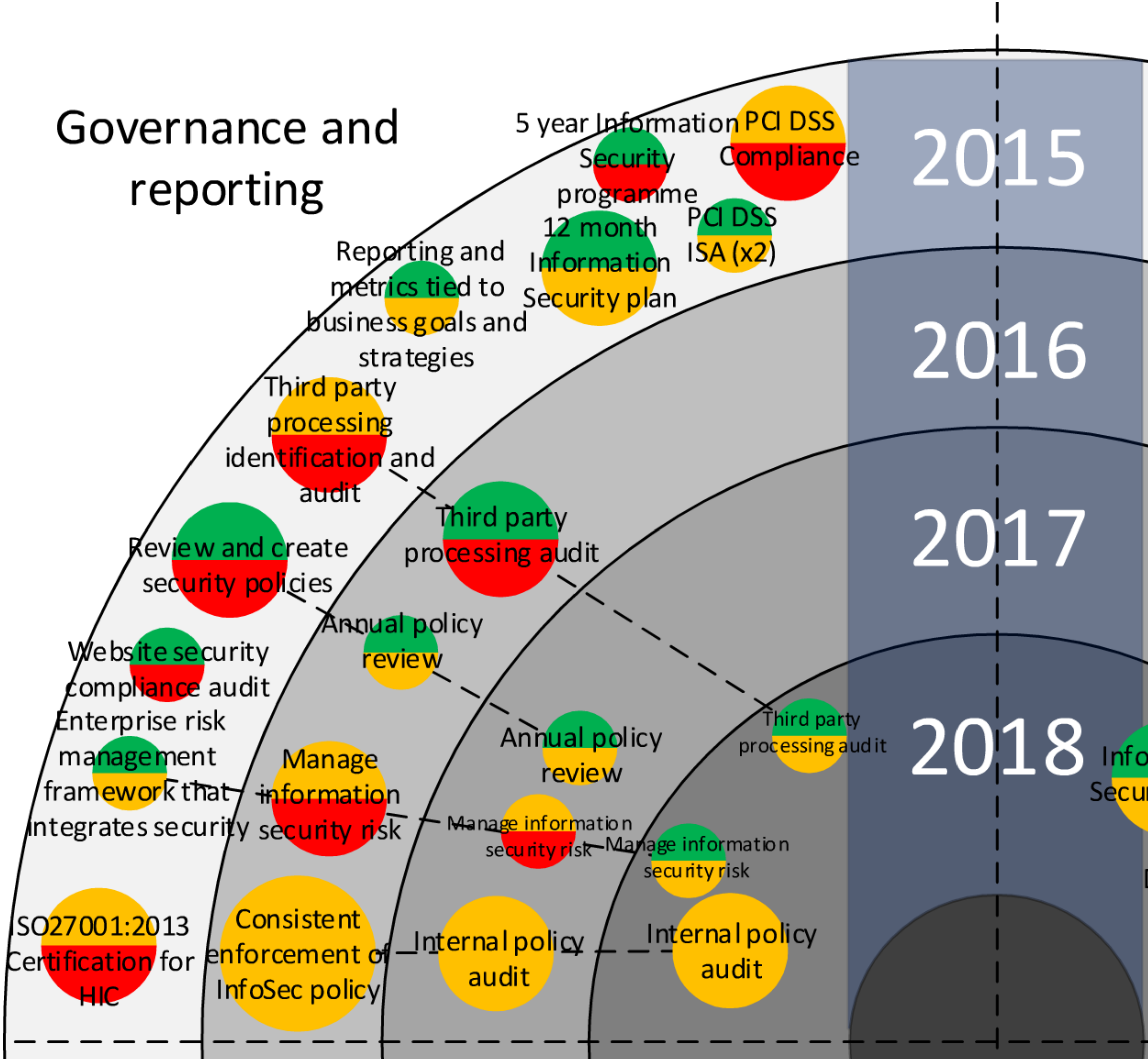
High Medium Low

The upper half of risk represents the likelihood of failure in terms of deployment, capability, organisational resistance or obsolescence.

High Medium Low

The lower half of risk represents the impact should the activity not be undertaken in terms of reputational damage, operational or financial exposure.

Governance and reporting



2015

2016

2017

2018

5 year Information Security programme

PCI DSS Compliance

12 month Information Security plan

PCI DSS ISA (x2)

Reporting and metrics tied to business goals and strategies

Third party processing identification and audit

Review and create security policies

Website security compliance audit

Enterprise risk management framework that integrates security

ISO27001:2013 Certification for HIC

Third party processing audit

Annual policy review

Manage information security risk

Consistent enforcement of InfoSec policy

Internal policy audit

Annual policy review

Manage information security risk

Internal policy audit

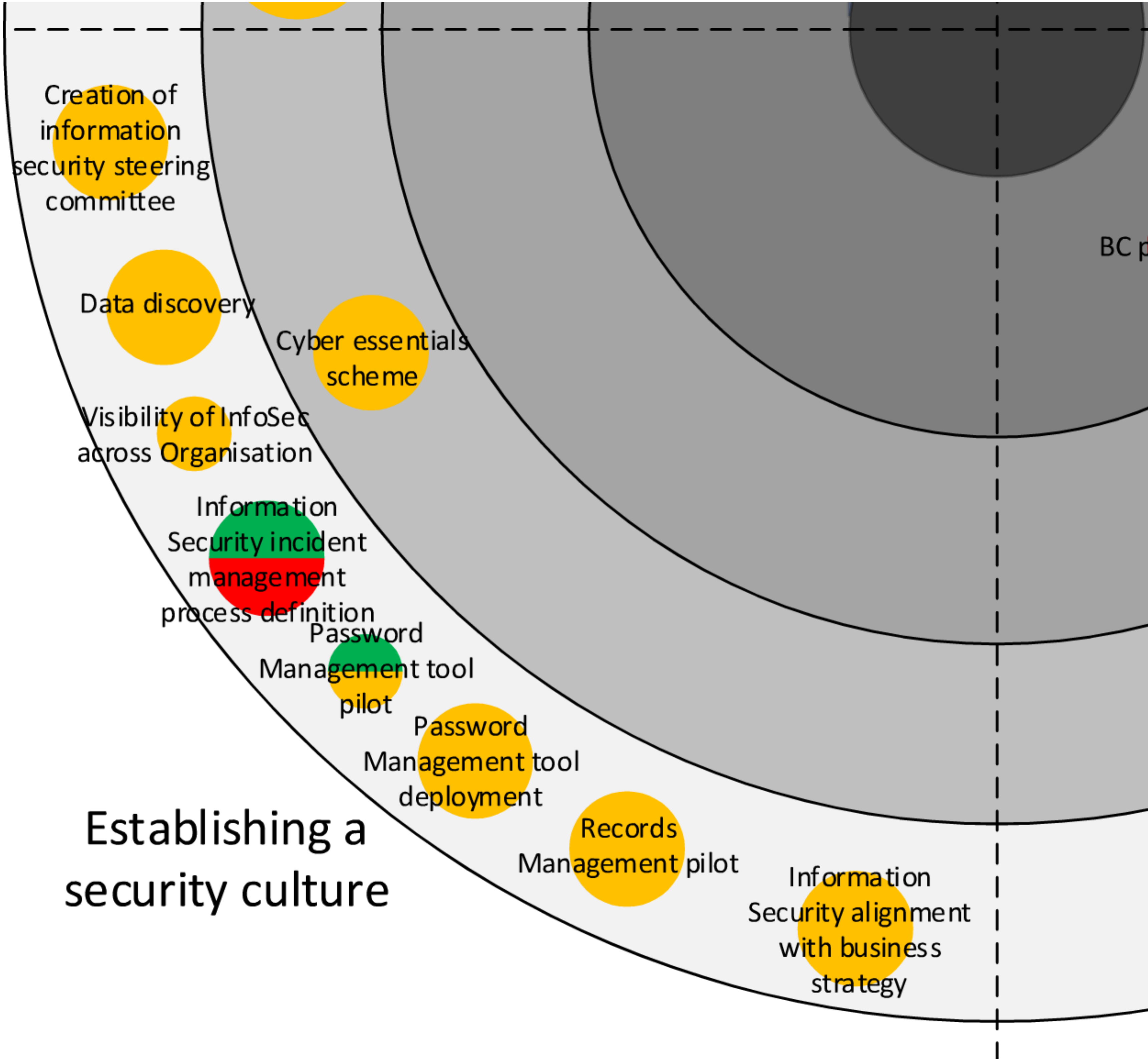
Third party processing audit

Manage information security risk

Internal policy audit

Info

Secu



Creation of information security steering committee

Data discovery

Cyber essentials scheme

Visibility of InfoSec across Organisation

Information Security incident management process definition

Password Management tool pilot

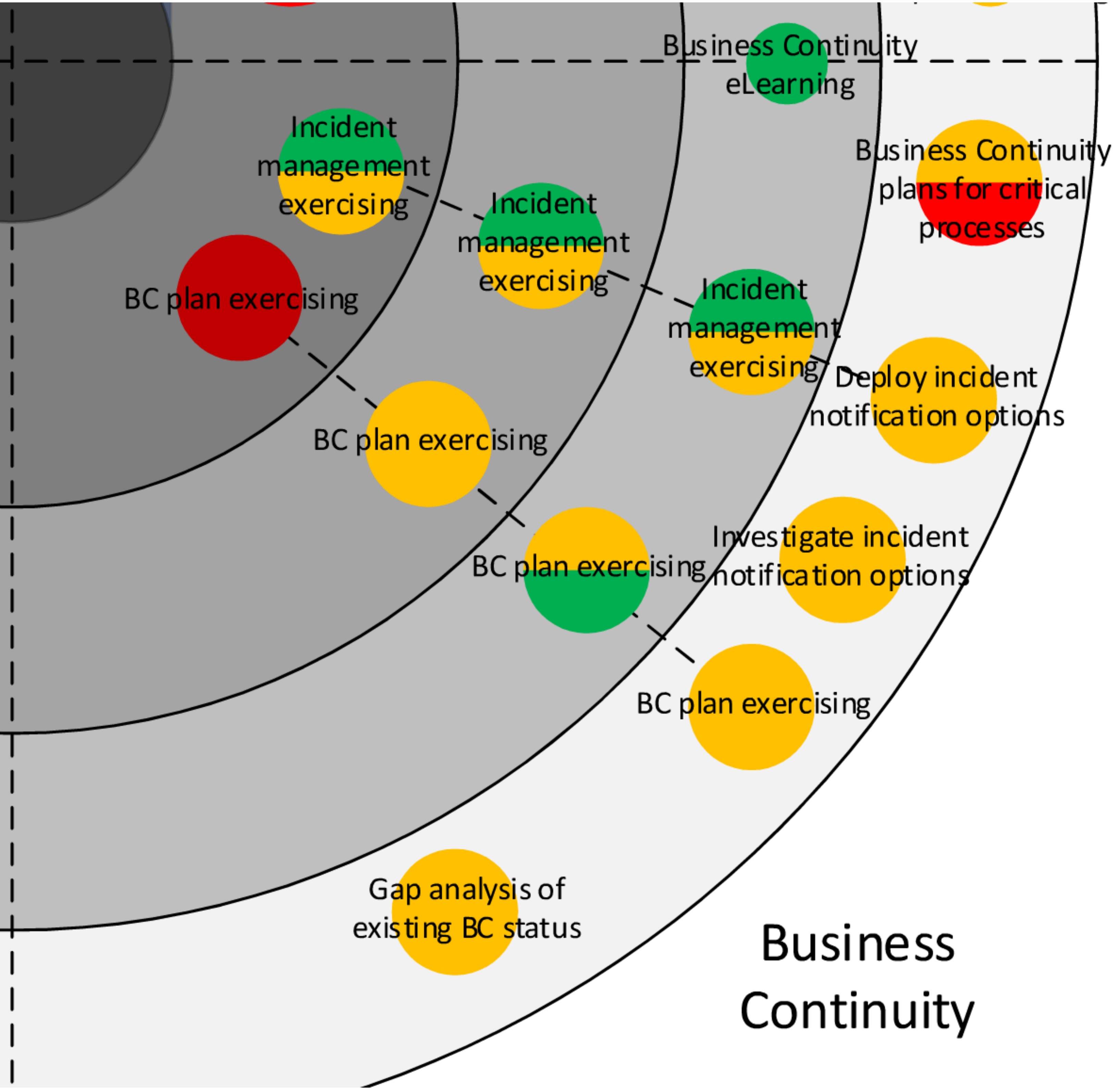
Password Management tool deployment

Records Management pilot

Information Security alignment with business strategy

BC p

Establishing a security culture



Business Continuity eLearning

Incident management exercising

Business Continuity plans for critical processes

Incident management exercising

BC plan exercising

Incident management exercising

Deploy incident notification options

BC plan exercising

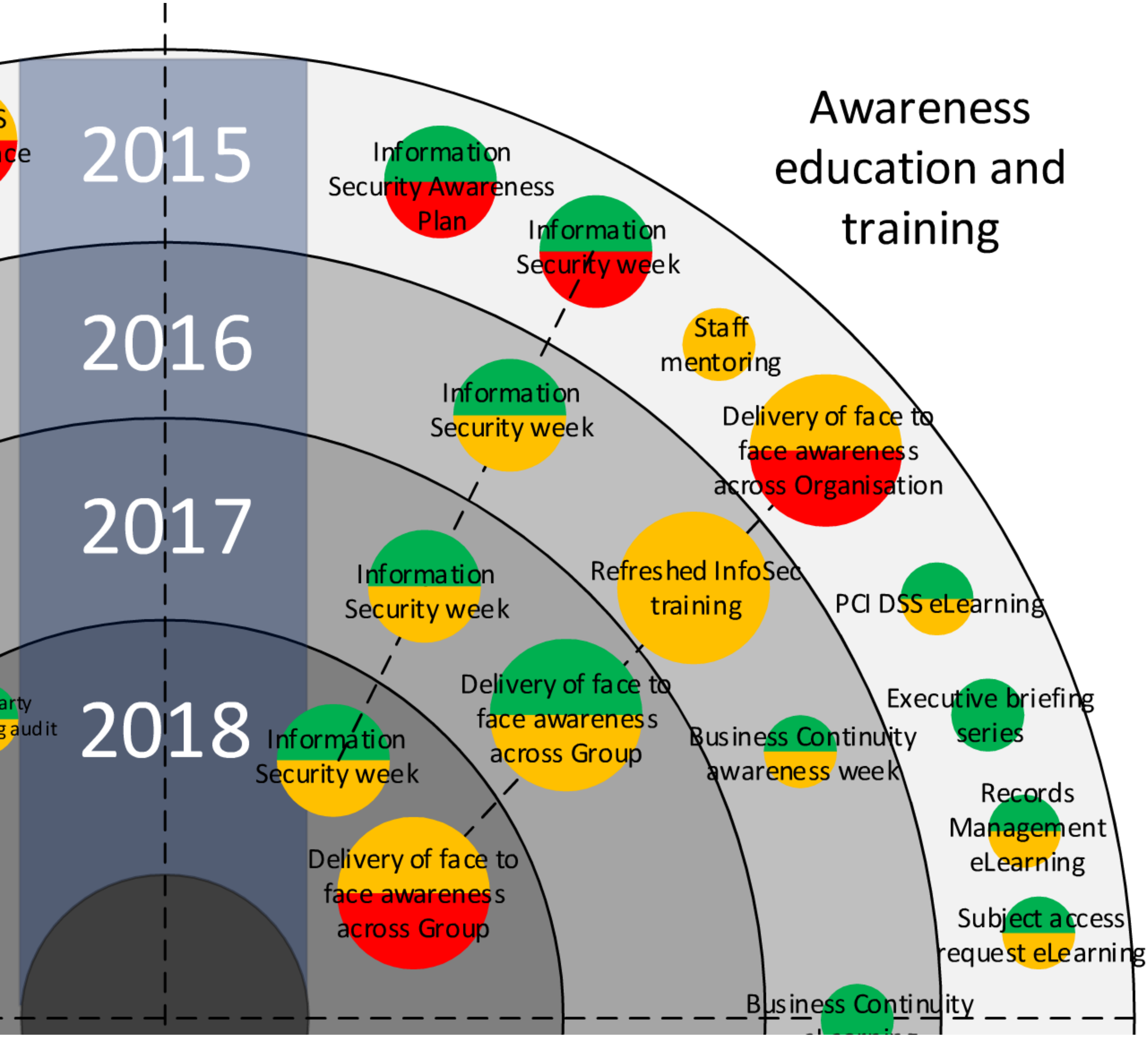
BC plan exercising

Investigate incident notification options

BC plan exercising

Gap analysis of existing BC status

Business Continuity



Awareness education and training

2015

2016

2017

2018

Information Security Awareness Plan

Information Security week

Staff mentoring

Delivery of face to face awareness across Organisation

Information Security week

Refreshed InfoSec training

PCI DSS eLearning

Information Security week

Delivery of face to face awareness across Group

Business Continuity awareness week

Executive briefing series

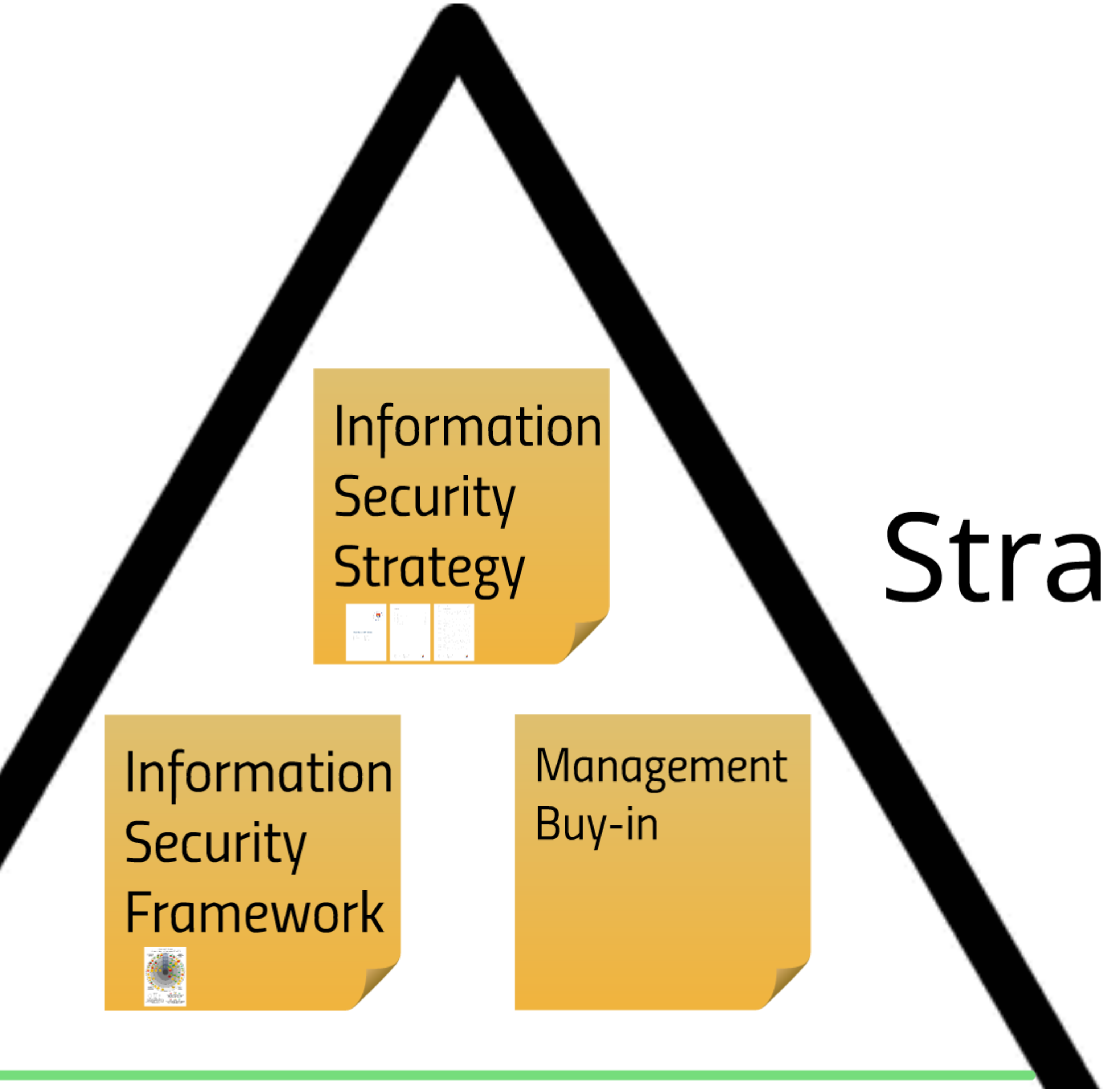
Information Security week

Delivery of face to face awareness across Group

Records Management eLearning

Subject access request eLearning

Business Continuity



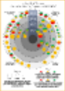
Information Security Strategy

Information Security Framework

Management Buy-in

Strategic

Framework



Policy

Audit & Compliance

Risk Management Framework

ISO 27005:2011
Establish context
Risk assessment
Risk treatment
Risk monitoring & review

Incident Management Framework

ISO 27035:2011
Plan and prepare
Detect and report
Assess
Respond
Improve

Awareness Education Training

Awareness methods
In person
Web based
Lunch and Learn
Posters
Emails
Website
Security Week

Timing
Annually - staff
Targeted - risk based
Induction - staff
Intake - students
Incidents - point of failure

Policy

Audit & Compliance

Risk Management Framework

ISO 27005:2011
Establish context
Risk assessment
Risk treatment
Risk monitoring & review

Incident Management Framework

ISO 27035:2011

Plan and prepare

Detect and report

Assess

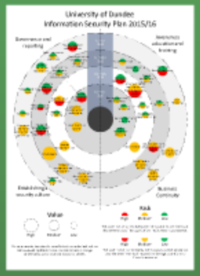
Respond

Improve

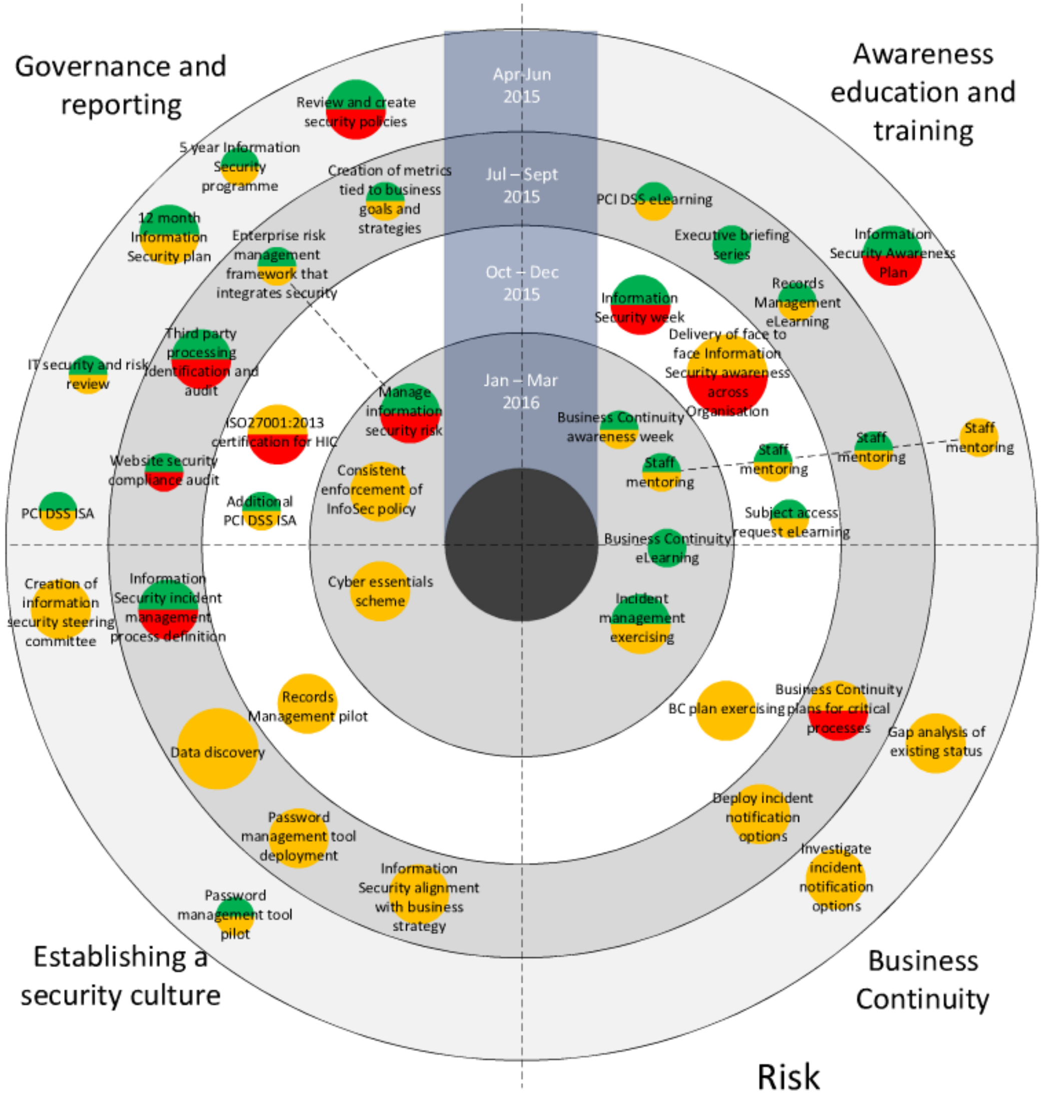
Awareness Education Training

Awareness methods
In person
Web based
Lunch and Learn
Posters
Emails
Website
Security Week

Timing
Annually - staff
Targeted - risk based
Induction - staff
Intake - students
Incidents - point of failure



University of Dundee
Information Security Plan 2015/16


Governance and reporting
Awareness education and training
Establishing a security culture
Business Continuity
Apr-Jun 2015
Jul – Sept 2015
Oct – Dec 2015
Jan – Mar 2016
Review and create security policies
5 year Information Security programme
Creation of metrics tied to business goals and strategies
12 month Information Security plan
Enterprise risk management framework that integrates security
Third party processing identification and audit
IT security and risk review
ISO27001:2013 certification for HIC
Manage information security risk
Website security compliance audit
Consistent enforcement of InfoSec policy
Additional PCI DSS ISA
PCI DSS ISA
Creation of information security steering committee
Information Security incident management process definition
Cyber essentials scheme
Records Management pilot
Data discovery
Password management tool deployment
Information Security alignment with business strategy
Password management tool pilot
PCI DSS eLearning
Executive briefing series
Information Security Awareness Plan
Records Management eLearning
Information Security week
Delivery of face to face Information Security awareness across Organisation
Business Continuity awareness week
Staff mentoring
Staff mentoring
Staff mentoring
Staff mentoring
Subject access request eLearning
Business Continuity eLearning
Incident management exercising
BC plan exercising
Business Continuity plans for critical processes
Gap analysis of existing status
Deploy incident notification options
Investigate incident notification options

Value

○ High ○ Medium ○ Low

Value represents the potential benefits that can be derived and has been assessed by effect on cost, positive behaviour change, adherence to compliance and functional benefit.

Risk

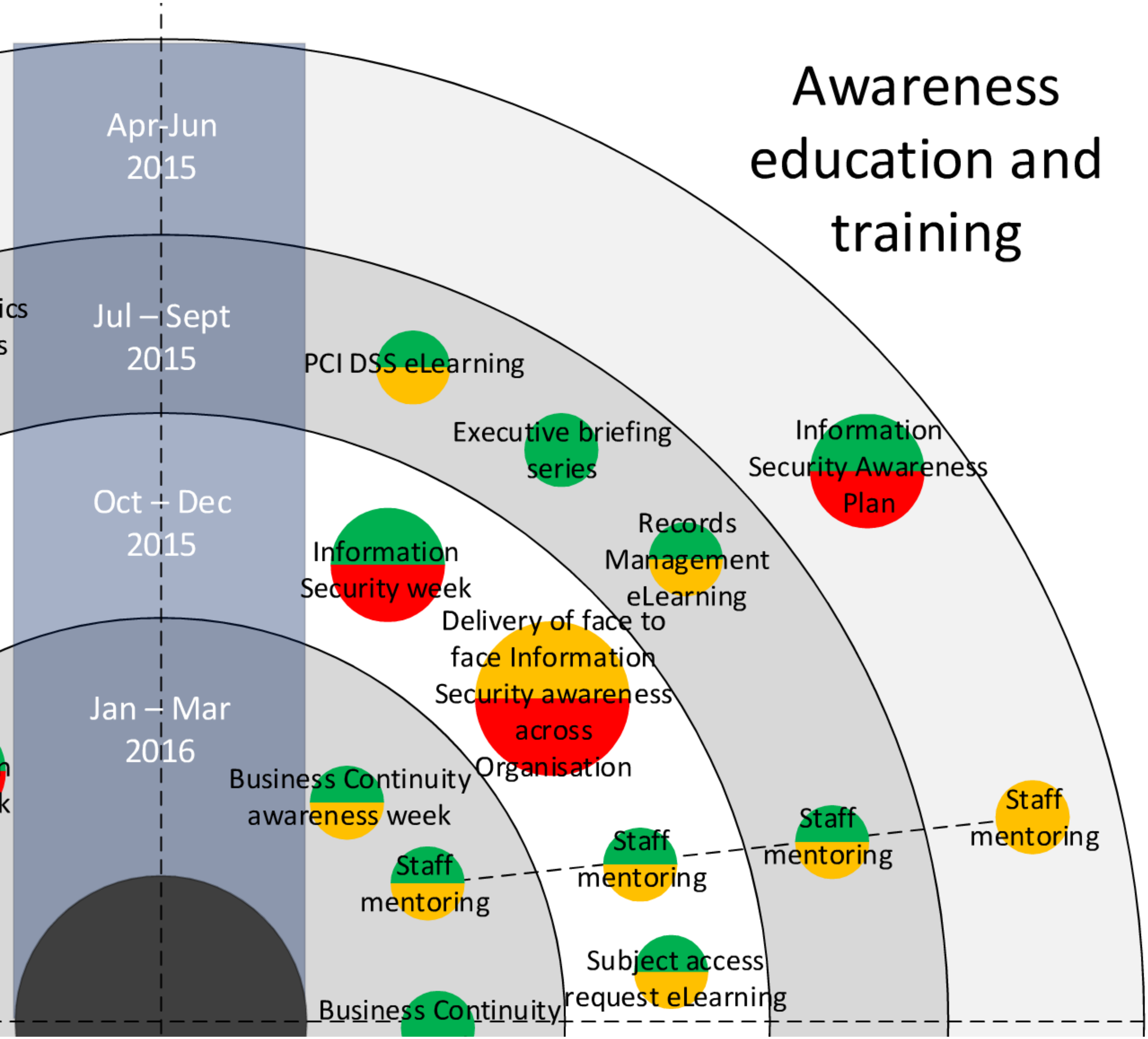
🟥 High 🟨 Medium 🟩 Low

The upper half of risk represents the likelihood of failure in terms of deployment, capability, organisational resistance or obsolescence.

🟥 High 🟨 Medium 🟩 Low

The lower half of risk represents the impact should the activity not be undertaken in terms of reputational damage, operational or financial exposure.

Awareness education and training



Apr-Jun 2015

Jul – Sept 2015

Oct – Dec 2015

Jan – Mar 2016

ics

s

n

k

PCI DSS eLearning

Executive briefing series

Information Security Awareness Plan

Records Management eLearning

Information Security week

Delivery of face to face Information Security awareness across Organisation

Business Continuity awareness week

Staff mentoring

Staff mentoring

Staff mentoring

Staff mentoring

Subject access request eLearning

Business Continuity

Data Discovery

Technical Security Controls

Physical Security Controls

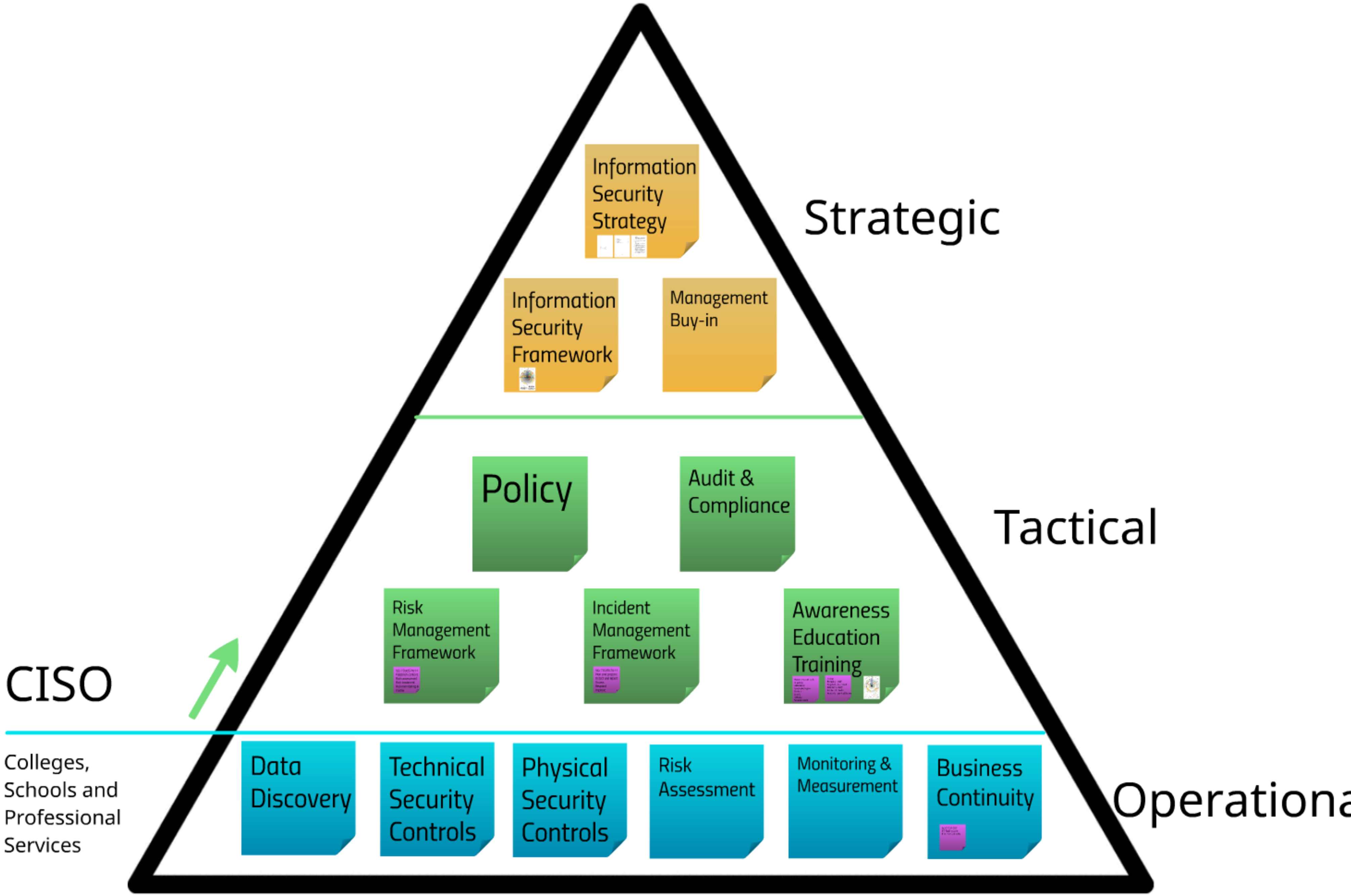
Risk Assessment

Monitoring & Measurement

Business Continuity

ISO 27031:2011 ICT Readiness for Business Continuity

Data Discovery



Information Security Strategy

Information Security Framework

Management Buy-in

Strategic

Policy

Audit & Compliance

Tactical

Risk Management Framework

Incident Management Framework

Awareness Education Training

CISO

Colleges, Schools and Professional Services

Data Discovery

Technical Security Controls

Physical Security Controls

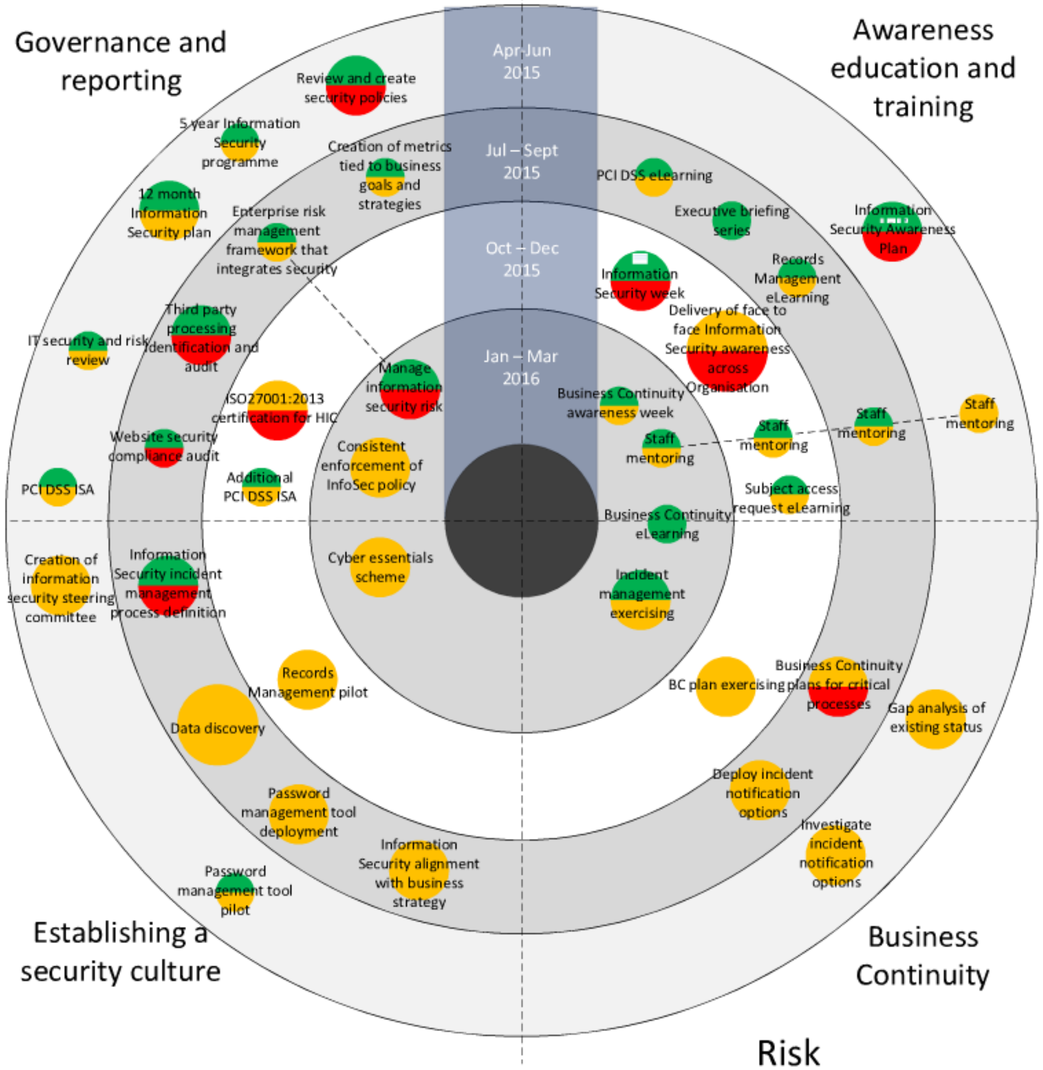
Risk Assessment

Monitoring & Measurement

Business Continuity

Operationa

University of Dundee
Information Security Plan 2015/16


Governance and reporting
Awareness education and training
Establishing a security culture
Business Continuity
Apr-Jun 2015
Jul – Sept 2015
Oct – Dec 2015
Jan – Mar 2016
Review and create security policies
5 year Information Security programme
Creation of metrics tied to business goals and strategies
12 month Information Security plan
Enterprise risk management framework that integrates security
Third party processing identification and audit
IT security and risk review
Manage information security risk
ISO27001:2013 certification for HIC
Website security compliance audit
Consistent enforcement of InfoSec policy
Additional PCI DSS ISA
PCI DSS ISA
Cyber essentials scheme
Creation of information security steering committee
Information Security incident management process definition
Records Management pilot
Data discovery
Password management tool deployment
Information Security alignment with business strategy
Password management tool pilot
PCI DSS eLearning
Executive briefing series
Information Security Awareness Plan
Records Management eLearning
Information Security week
Delivery of face to face Information Security awareness across Organisation
Business Continuity awareness week
Staff mentoring
Staff mentoring
Staff mentoring
Staff mentoring
Subject access request eLearning
Business Continuity eLearning
Incident management exercising
BC plan exercising
Business Continuity plans for critical processes
Gap analysis of existing status
Deploy incident notification options
Investigate incident notification options

Value

○ High ○ Medium ○ Low

Value represents the potential benefits that can be derived and has been assessed by effect on cost, positive behaviour change, adherence to compliance and functional benefit.

Risk

🔴 High 🟡 Medium 🟢 Low

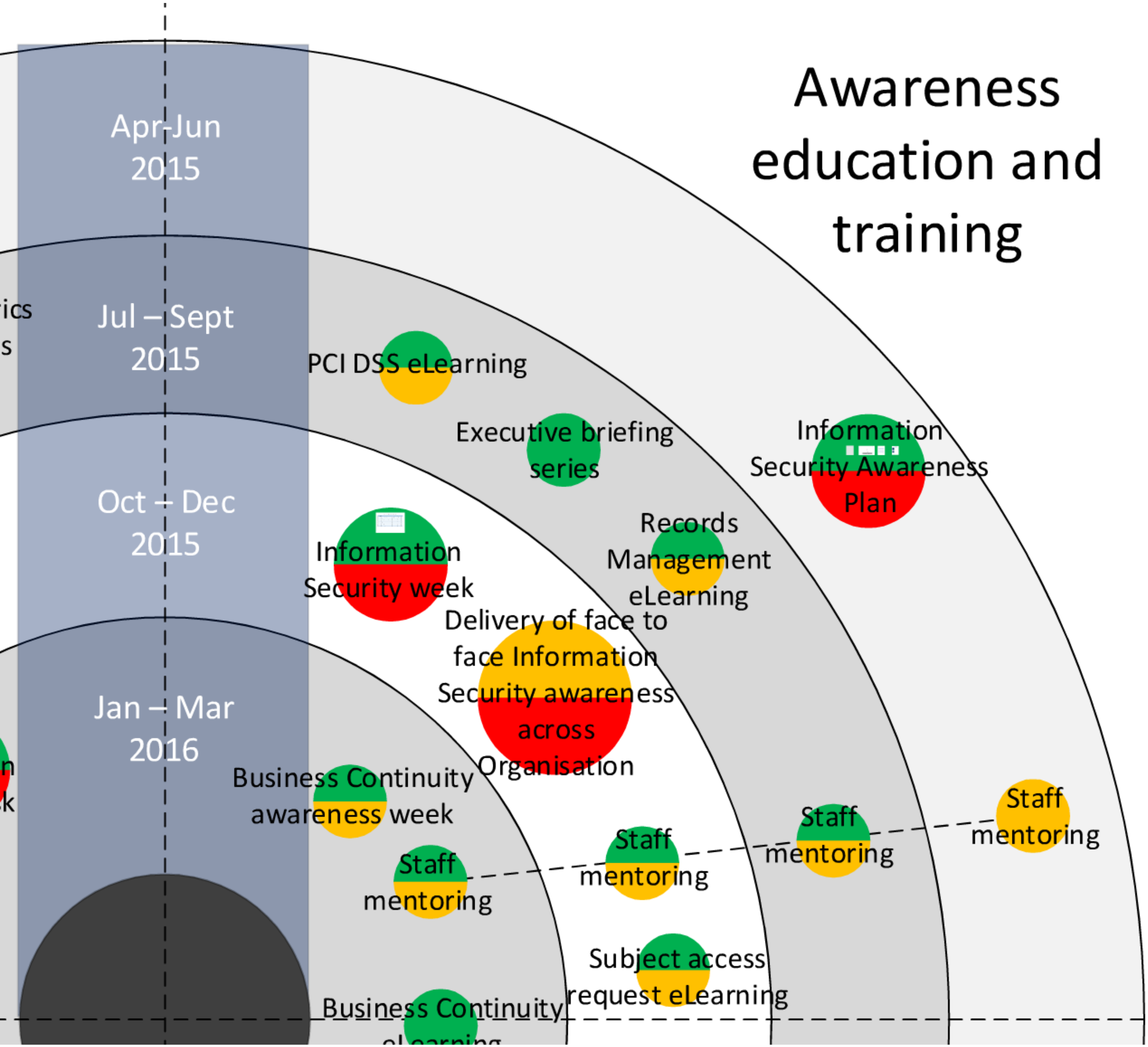
The upper half of risk represents the likelihood of failure in terms of deployment, capability, organisational resistance or obsolescence.

🔴 High 🟡 Medium 🟢 Low

The lower half of risk represents the impact should the activity not be undertaken in terms of reputational damage, operational or financial exposure.

al

Awareness education and training



Apr-Jun 2015

Jul – Sept 2015

Oct – Dec 2015

Jan – Mar 2016

PCI DSS eLearning

Executive briefing series

Information Security Awareness Plan

Information Security week

Records Management eLearning

Delivery of face to face Information Security awareness across Organisation

Business Continuity awareness week

Staff mentoring

Staff mentoring

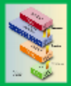
Staff mentoring

Staff mentoring

Subject access request eLearning

Business Continuity eLearning

Information



Security Awareness

Plan

ent

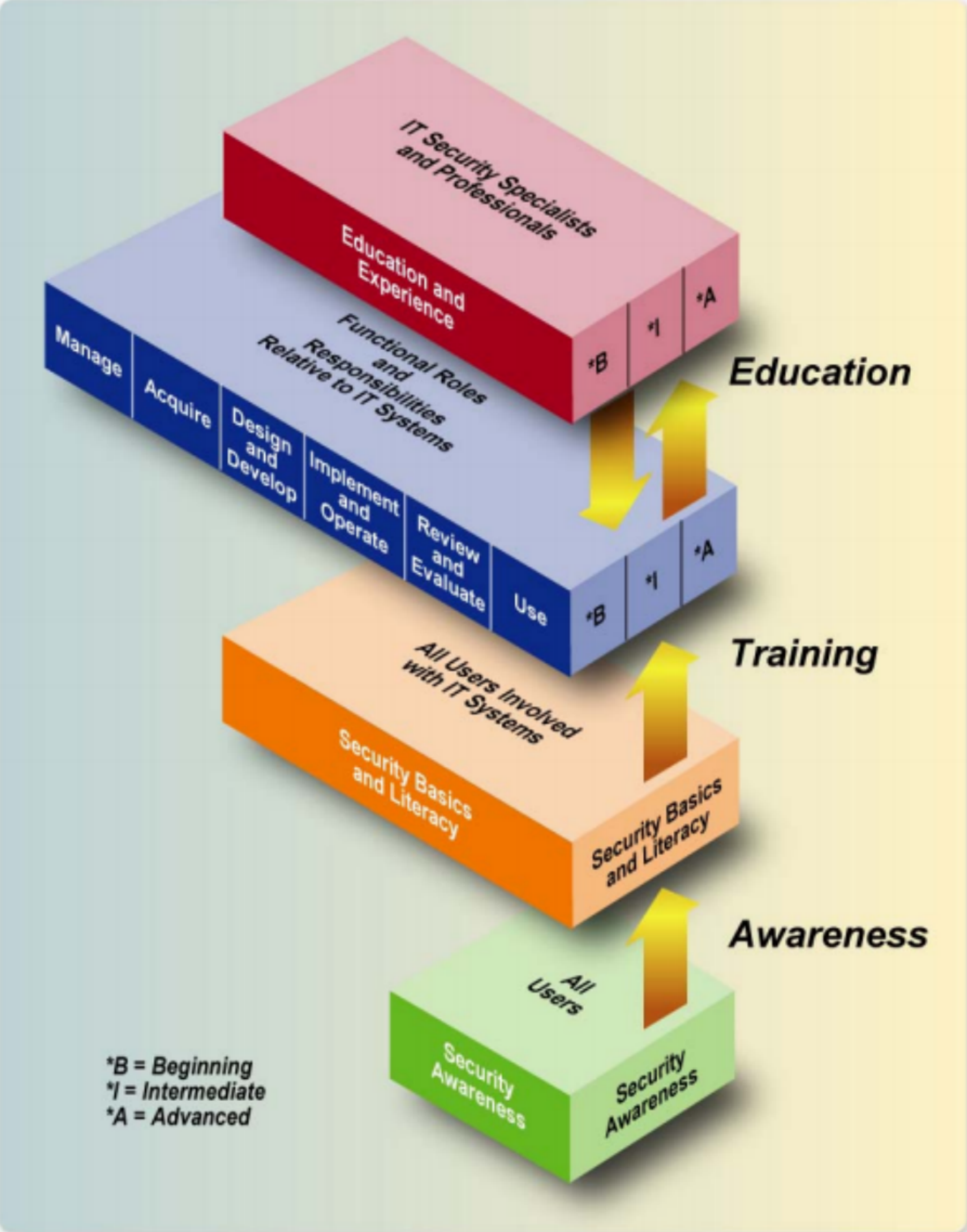
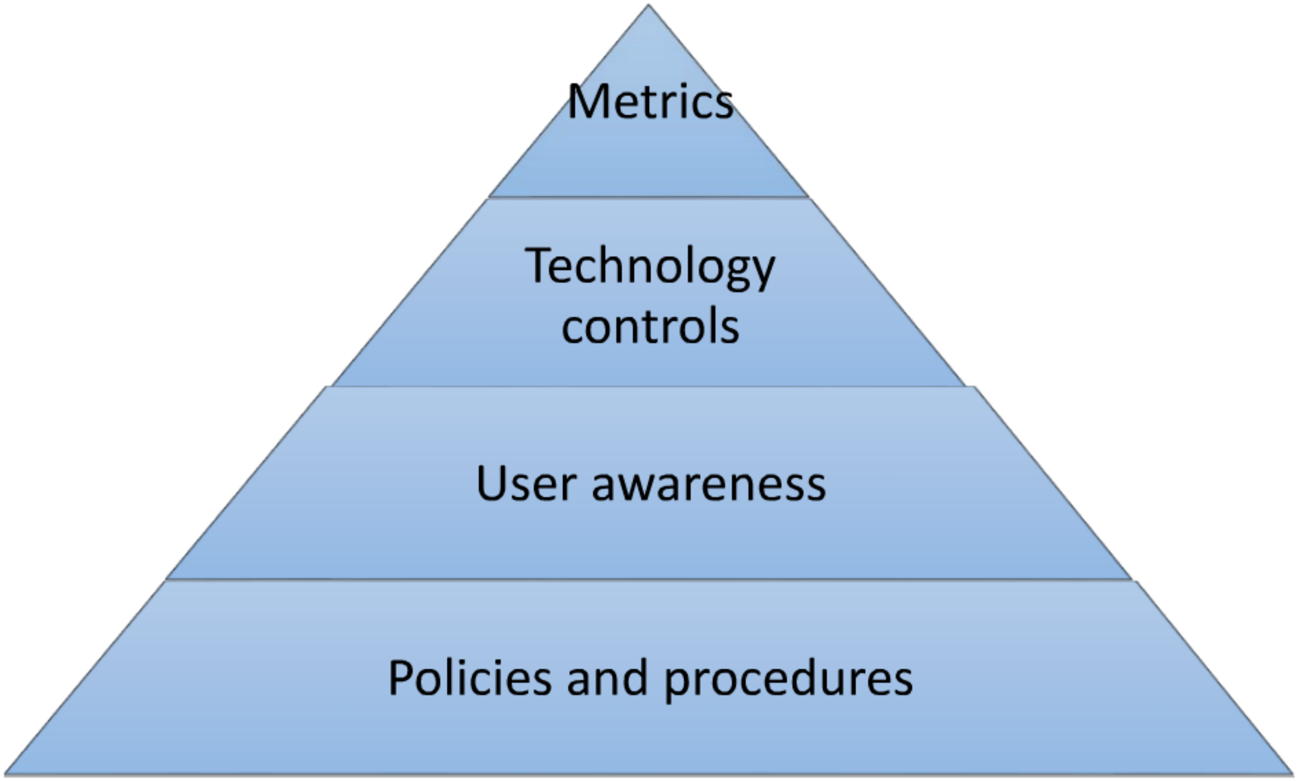

IT Security Specialists and Professionals
Education and Experience
*B
*I
*A
Education
Functional Roles and Responsibilities Relative to IT Systems
Manage
Acquire
Design and Develop
Implement and Operate
Review and Evaluate
Use
*B
*I
*A
Training
All Users Involved with IT Systems
Security Basics and Literacy
Security Basics and Literacy
Awareness
All Users
Security Awareness
Security Awareness
*B = Beginning
*I = Intermediate
*A = Advanced

Figure 1 - Elements of a mature information security programme

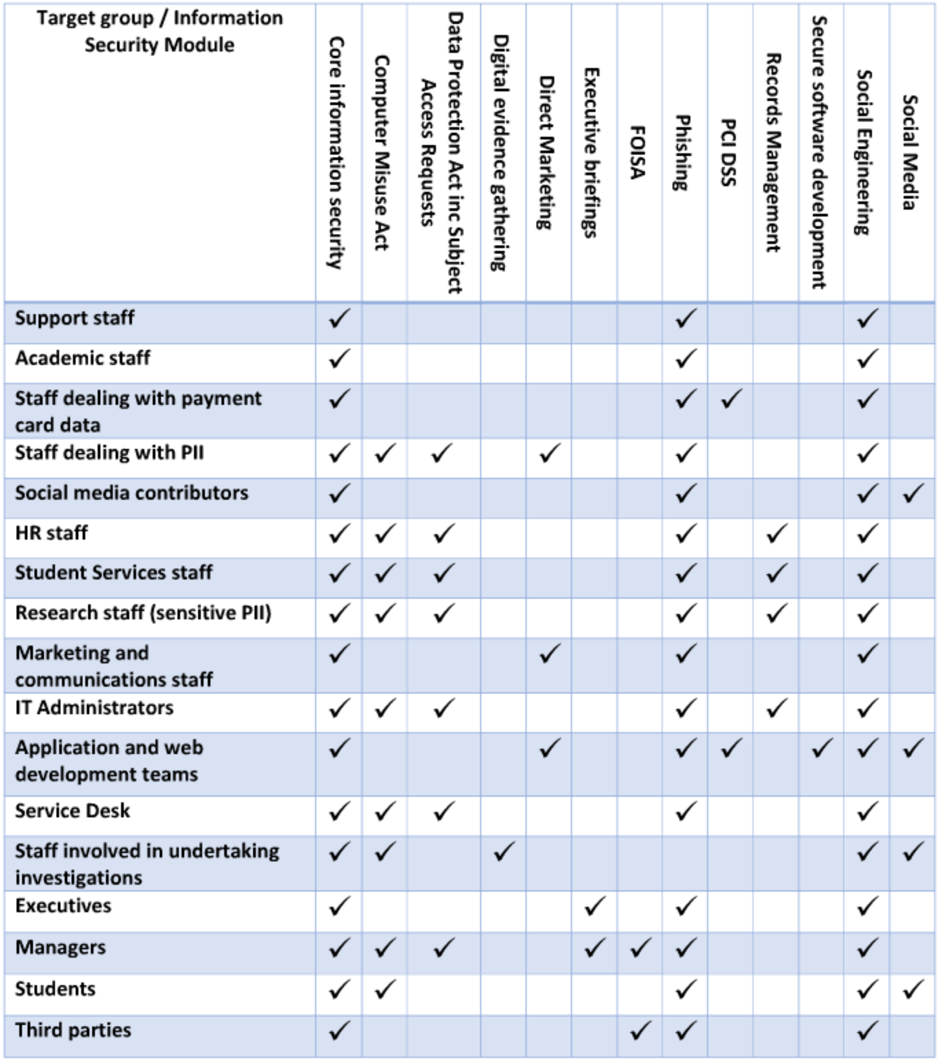


Metrics

Technology controls

User awareness

Policies and procedures



Target group / Information Security Module	Core information security	Computer Misuse Act	Data Protection Act inc Subject Access Requests	Digital evidence gathering	Direct Marketing	Executive briefings	FOISA	Phishing	PCI DSS	Records Management	Secure software development	Social Engineering	Social Media
Support staff	✓							✓				✓	
Academic staff	✓							✓				✓	
Staff dealing with payment card data	✓							✓	✓			✓	
Staff dealing with PII	✓	✓	✓		✓			✓				✓	
Social media contributors	✓							✓				✓	✓
HR staff	✓	✓	✓					✓		✓		✓	
Student Services staff	✓	✓	✓					✓		✓		✓	
Research staff (sensitive PII)	✓	✓	✓					✓		✓		✓	
Marketing and communications staff	✓				✓			✓				✓	
IT Administrators	✓	✓	✓					✓		✓		✓	
Application and web development teams	✓				✓			✓	✓		✓	✓	✓
Service Desk	✓	✓	✓					✓				✓	
Staff involved in undertaking investigations	✓	✓		✓								✓	✓
Executives	✓					✓		✓				✓	
Managers	✓	✓	✓			✓	✓	✓				✓	
Students	✓	✓						✓				✓	✓
Third parties	✓						✓	✓				✓	

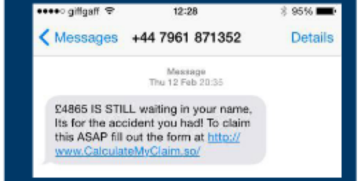
Nuisance calls and spam texts

RECENT NEWS

Nuisance calls and spam texts remain a continuing concern for consumers and a key area of action for the Information Commissioner's Office (ICO)

Top spam text topics[1]:

- Accident Claims
- Gambling (lottery)
- Payday Loans
- Banking
- PPI



+44 7961 871352

Message
Thu 12 Feb 20:35

£4865 IS STILL waiting in your name, Its for the accident you had! To claim this ASAP fill out the form at http://www.CalculateMyClaim.so/

Spam texts usually come from an 11-digit mobile number and the company isn't identified.

98% of texts are opened compared to 25% of emails[2]

Contact Us

Information Security
Computing Centre
Park Place
Infosec@dundee.ac.uk
www.dundee.ac.uk/infosec

WHAT ARE SPAM TEXTS AND NUISANCE CALLS?

A spam text is a text message sent to a mobile phone marketing a particular product or service. It is against the law for anyone to send you marketing texts unless you have previously given them permission. It's also against the law for companies to call consumers who are registered with the Telephone Preference Service (TPS**)** without their clear consent.

How to spot spam messages

Firstly you need to determine whether the text message is from a legitimate organization or just spam. If the text identifies a company name as the sender it could be a genuine marketing message but if it looks like a private mobile number then it's more likely to be spam. You can always type the number into a search engine to identify if it's likely to be genuine or not.

Q: How can I stop receiving spam calls and spam texts?
A: You can register your home and mobile numbers for free with the TPS (www.tpsonline.org.uk)- this should reduce calls from companies, unless you have requested them to call or text you.

Don't send the word "STOP" back to spam texts as then they will know you have a valid mobile phone number and this information may be sold on to other unscrupulous operators leading to you receiving more unsolicited messages.

> *"All of the UK's mobile operators worked together to deploy a tool which collates all the information from the 7726 short code in real time." - Which*

Q: Who can I complain to?
A: If you're receiving spam texts, you can forward these to your mobile operator's free spam reporting service by forwarding the text to 7726. For both nuisance calls and messages you can complain to the ICO by completing the details on their survey at https://ico.org.uk/for-the-public/texts/

Q: I have had fraud carried out on my account, where do I go?
A: If spam calls and texts have resulted in any fraudulent activity you can to report this to Action Fraud at www.actionfraud.police.uk or 0330 123 2040.

Malicious, abusive or threatening calls, whether from people you know or from strangers, are a criminal offence and should be reported to the Police.

[1] ICO, https://ico.org.uk/action-weve-taken/nuisance-calls-and-messages/ 27th April 2015
[2] WhizMobi http://www.slideshare.net/WhizMobi/10-mindblowing-mobile-marketing-stats-for-stronger-marketing-campaign 27th April 2015

Information Security Week - University of Dundee - October 2015

[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
Friday	[illegible]	Executive Breakfast	University senior managers	Briefing	TBC
TBC		[illegible]	[illegible]	[illegible]	TBC
TBC		Information asset identification	Information asset custodians	Workshop	TBC
TBC		Privacy impact assessment	[illegible]	Workshop	TBC
TBC		Risk management of data	Information asset custodians	Workshop	TBC
TBC		[illegible]	Staff and students	Demonstration	TBC
TBC		[illegible]	Staff	Presentation	TBC
TBC		[illegible]	Staff and students	[illegible]	TBC
TBC		[illegible]	Staff and students	Presentation	TBC
TBC		[illegible]	Staff and students	Demonstration	TBC
TBC		Incident response exercise	Incident management team	Workshop	TBC
TBC		[illegible]	Staff and students	[illegible]	TBC
TBC		[illegible]	Staff and students	Demonstration	TBC
TBC		[illegible]	Staff and students	Workshop	TBC
TBC		Phishing demo	Staff and students	Demonstration	TBC
TBC		[illegible]	Staff and students	Demonstration	TBC
TBC		[illegible]	Staff and students	Presentation	TBC
TBC		Online banking	Staff and students	Demonstration	TBC
TBC		Two factor authentication	Staff and students	[illegible]	TBC
TBC		[illegible]	Staff	Presentation	TBC
TBC		[illegible]	Staff and students	[illegible]	TBC

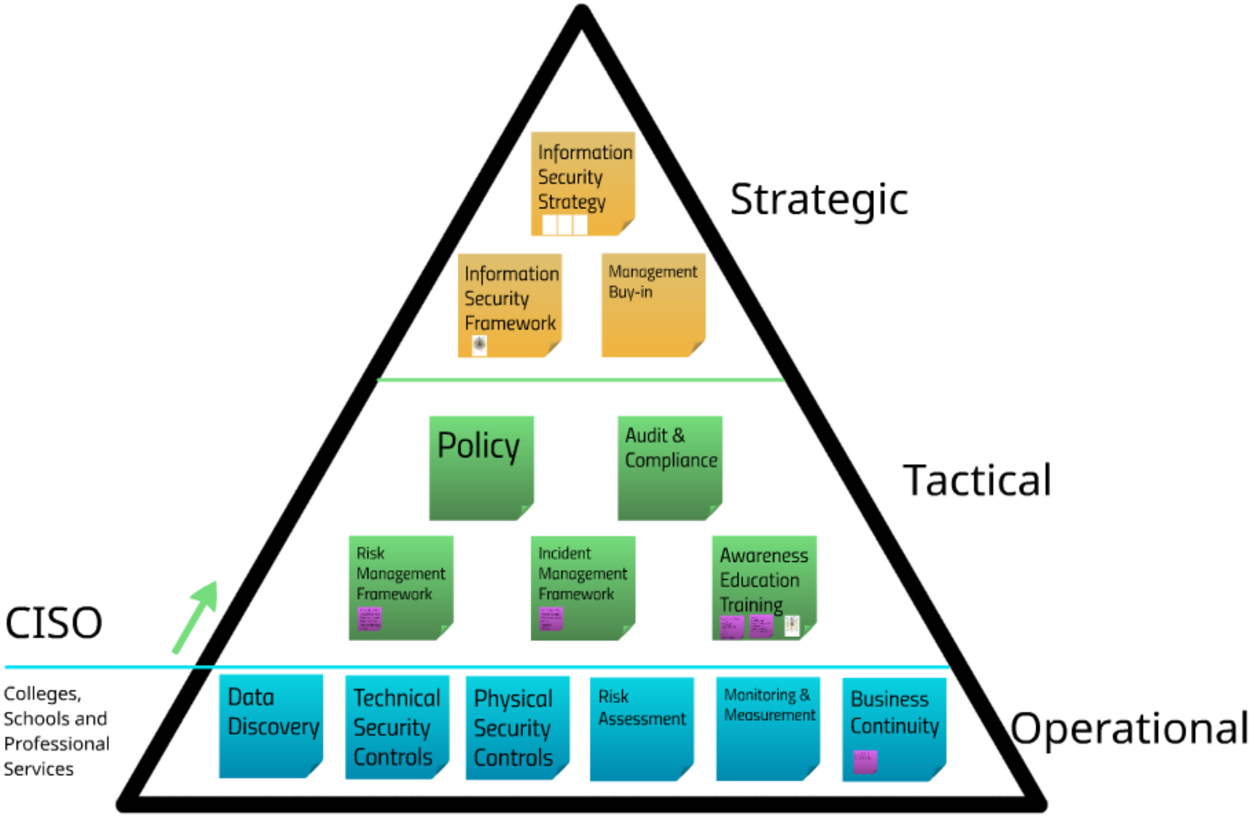
Information Security week

Del

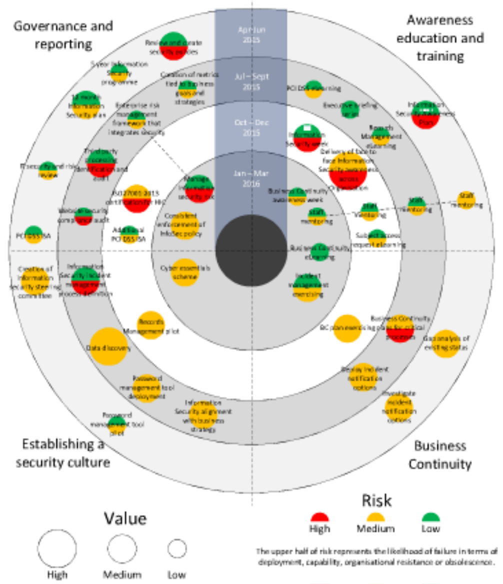
Information Security Week - Unversity of Dundee - October 2015

Day	Date	Topic	Attendees	Format	Location
Friday	01/10/2015	Executive breakfast	University senior managers	Briefing	TBD
TBD		Welcome to Information Security week	Recorded by Principal	Video/Social media	TBD
TBD		Information asset identification	Information owners, custodian	Workshop	TBD
TBD		Privacy impact assessment	Systems developers, outsourcers	Workshop	TBD
TBD		Risk management of data	Information owners, custodian	Workshop	TBD
TBD		I know all about you - social media breadcrumbs	Staff and student	Demonstration	TBD
TBD		Keeping your kids safe online	Staff	Presentation	TBD
TBD		You can access your personal information anywhere	Staff and students	Webinar	TBD
TBD		Using social networking sites safely	Staff and students	Presentation	TBD
TBD		Privacy on your mobile device	Staff and students	Demonstration	TBD
TBD		Incident response exercise	Incident management team	Workshop	TBD
TBD		Protect your personal information (including signposts to other resources)	Staff and students	WBT	TBD
TBD		LastPass launch	Staff and students	Demonstration	TBD
TBD		LastPass drop-in clinic	Staff and students	Workshop	TBD
TBD		Phishing demo	Staff and students	Demonstration	TBD
TBD		Honeypot Wi-Fi network	Staff and students	Demonstration	TBD
TBD		Women in cyber security	Staff and students	Presentation	TBD
TBD		Hands on hacking	Staff and students	Demonstration	TBD
TBD		Two factor authentication	Staff and students	WBT	TBD
TBD		Focussed on Information Security – the plan for the long term	Staff	Presentation	TBD
TBD		Hard drive destruction	Staff and students	Service offering	TBD

INFORMATION SECURITY ELEMENTS


Information Security Strategy
Information Security Framework
Management Buy-in
Strategic
Policy
Audit & Compliance
Risk Management Framework
Incident Management Framework
Awareness Education Training
Tactical
CISO
Colleges, Schools and Professional Services
Data Discovery
Technical Security Controls
Physical Security Controls
Risk Assessment
Monitoring & Measurement
Business Continuity
Operational

University of Dundee
Information Security Plan 2015/16


Governance and reporting
Awareness education and training
Establishing a security culture
Business Continuity
Apr-Jun 2015
Jul – Sept 2015
Oct – Dec 2015
Jan – Mar 2016
Review and create security policies
5 year Information Security programme
Creation of metrics tied to business goals and strategies
12 month Information Security plan
Enterprise risk management framework that integrates security
IT security and risk review
Third party processing identification and audit
ISO27001:2013 certification for HIC
Manage information security risk
Website security compliance audit
Additional PCI DSS SA
PCI DSS SA
Consistent enforcement of InfoSec policy
Cyber essentials scheme
Creation of Information security steering committee
Information Security incident management process definition
Records Management pilot
Data discovery
Password management tool deployment
Password management tool pilot
Information Security alignment with business strategy
PCI DSS eLearning
Executive briefing
Information Security Awareness Plan
Information Security week
Records Management eLearning
Delivery of face to face Information Security awareness across Organisation
Business Continuity awareness week
Staff mentoring
Subject access request eLearning
Business Continuity eLearning
Incident management exercising
BC plan exercising
Business Continuity plans for critical processes
Gap analysis of existing status
Deploy incident notification options
Investigate incident notification options
Value
High
Medium
Low
Risk
High
Medium
Low
High
Medium
Low

Value represents the potential benefits that can be derived and has been assessed by effect on cost, positive behaviour change, adherence to compliance and functional benefit.

The upper half of risk represents the likelihood of failure in terms of deployment, capability, organisational resistance or obsolescence.

The lower half of risk represents the impact should the activity not be undertaken in terms of reputational damage, operational or financial exposure.