Resources for Introduction

RESOURCES

- **Different elements of an Information Security Management System – Cardiff University**
- **Stages for implementing an Information Security Framework (ISF) programme – Cardiff University**

Different elements of an Information Security Management System – Cardiff University

Information Asset and Risk Ownership

- Ownership of risks
- Ownership of assets
- Risk assessment approach

User Education and Awareness

- Awareness raising campaign
- Information resources
- Training programme

Incident Management and Business Continuity

- Incident reporting and assessment framework
- Major Incident and Business continuity plans

Remote and Mobile Working

- Policy
- Processes
- Tools to enable secure remote and mobile working

Policy

- Overarching policy
- Information Classification and Handling Rules

Network Security

- Secure authentication
- Endpoint integrity
- Account and privileges management

Physical Security

- Secure areas
- Access management
- Secure disposal

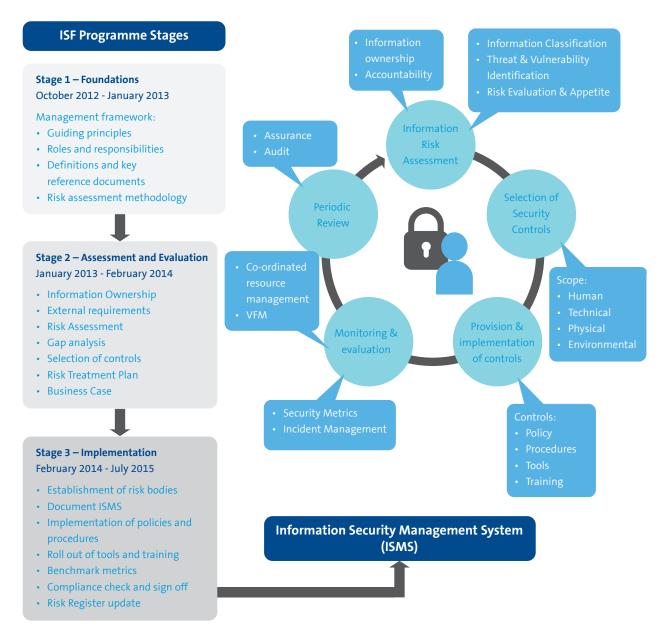## Testing, Monitoring and Continual Improvement

- Framework review
- Penetration and vulnerability tests
- Metrics gathering

External Assurance

- Baseline Personnel Security Standard
- ISO27001

Stages for implementing an Information Security Framework (ISF) programme – Cardiff University

Information Security Framework (ISF) Programme

ISF Programme Stages

Stage 1 – Foundations
October 2012 - January 2013

Management framework:
- Guiding principles
- Roles and responsibilities
- Definitions and key reference documents
- Risk assessment methodology

Stage 2 – Assessment and Evaluation
January 2013 - February 2014

- Information Ownership
- External requirements
- Risk Assessment
- Gap analysis
- Selection of controls
- Risk Treatment Plan
- Business Case

Stage 3 – Implementation
February 2014 - July 2015

- Establishment of risk bodies
- Document ISMS
- Implementation of policies and procedures
- Roll out of tools and training
- Benchmark metrics
- Compliance check and sign off
- Risk Register update

- Information ownership
- Accountability

- Information Classification
- Threat & Vulnerability Identification
- Risk Evaluation & Appetite

- Assurance
- Audit

Information Risk Assessment

Periodic Review

Selection of Security Controls

- Co-ordinated resource management
- VFM

Monitoring & evaluation

Provision & implementation of controls

Scope:
- Human
- Technical
- Physical
- Environmental

- Security Metrics
- Incident Management

Controls:
- Policy
- Procedures
- Tools
- Training

Information Security Management System (ISMS)