ISO 27001 & ISMS OVERVIEW & CASE STUDY

Neil Hare-Brown

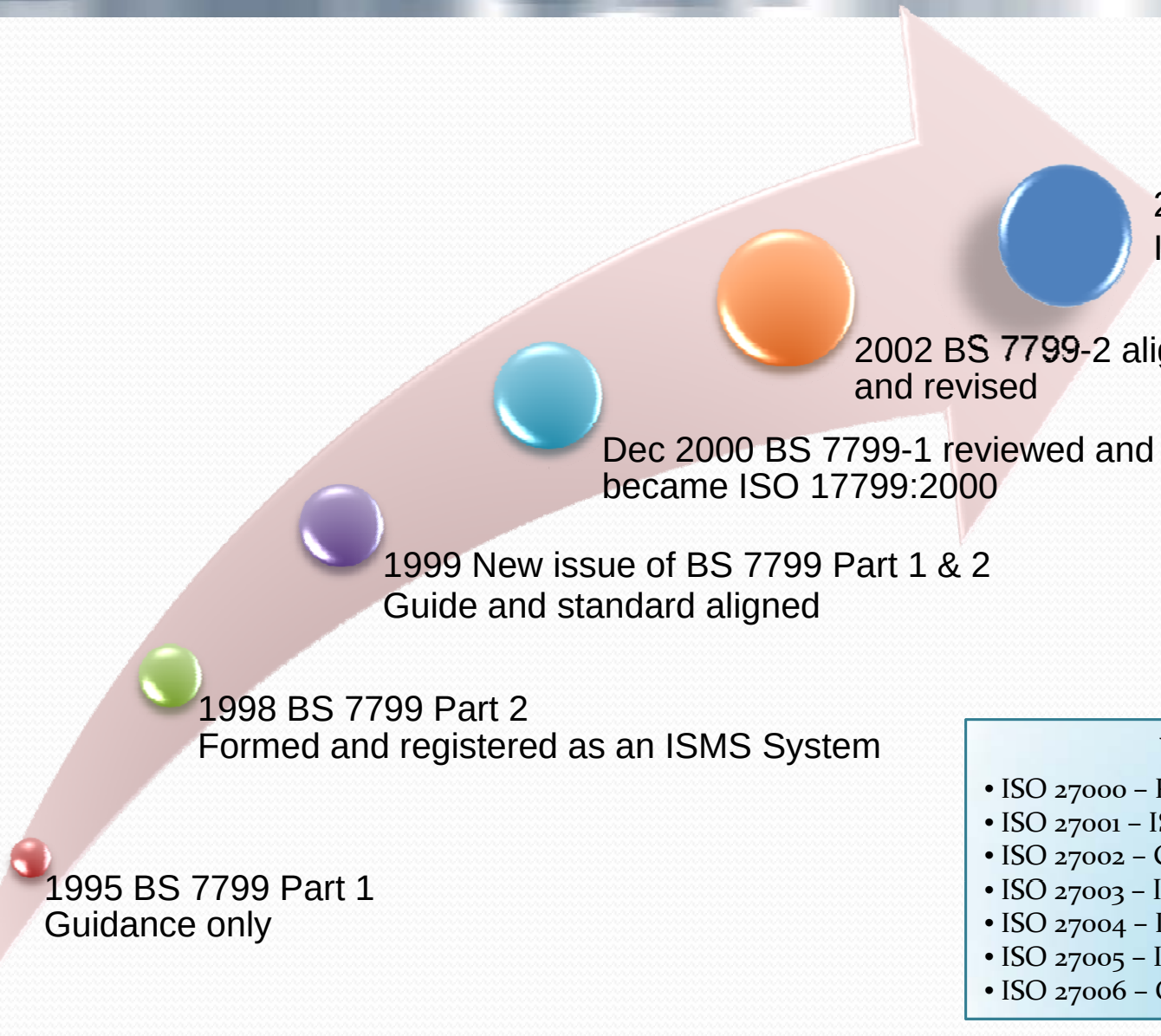
neilhb@qccis.com

+44 (0)207 353 9000

www.qccis.com

V1.0a dated 28 Jul 08

ISO 27001:2005 HISTORY



2005 New ISO 17799:2005 & ISO 27001:2005 released

ISO 17799:2005 renamed to ISO 27002:2005 in 2007 no change to document until next revision

2002 BS 7799-2 aligned and revised

Dec 2000 BS 7799-1 reviewed and became ISO 17799:2000

1999 New issue of BS 7799 Part 1 & 2 Guide and standard aligned

1998 BS 7799 Part 2 Formed and registered as an ISMS System

1995 BS 7799 Part 1 Guidance only

Where are we now?

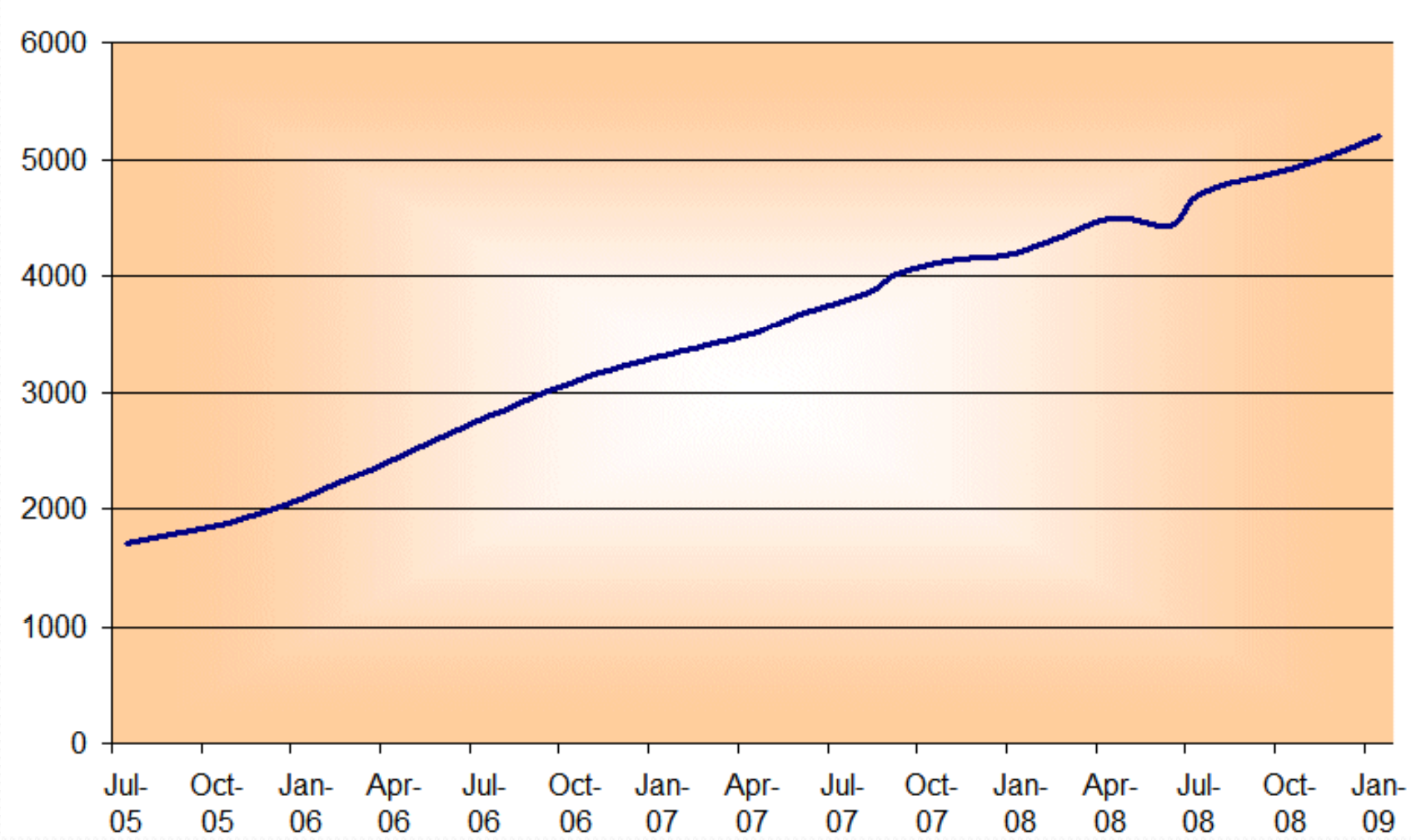
- ISO 27000 – Principles & Vocabulary
- ISO 27001 – ISMS Requirements (BS 7799 Part 2)
- ISO 27002 – Controls Guidance (ISO 17799:2005)
- ISO 27003 – ISMS Implementation Guidelines
- ISO 27004 – ISMS Measurements and Metrics (soon)
- ISO 27005 – ISMS Risk Management
- ISO 27006 – Guidelines for Accreditation

Standard started in 1992 when BSI had been approached by certain industry sectors with concerts over potential problems and security issues with ‘electronic systems’. Sept 1993 ‘Code of Practice’ published

STRATEGIC BENEFITS OF ISO 27001

- Improved effectiveness of Information Security
- Demonstrates Integrity and Trustworthiness
- Ownership by Senior Management
- Corporate Governance & Compliance
- Structured approach
- Global acceptance – International Standard
- Increased Risk Awareness and better Risk Treatment
- Gives an independent review of ISMS
- Improved marketing image and customer expectation

ISO 27001 Today (number of certificates)



Source: http://www.iso27001certificates.com

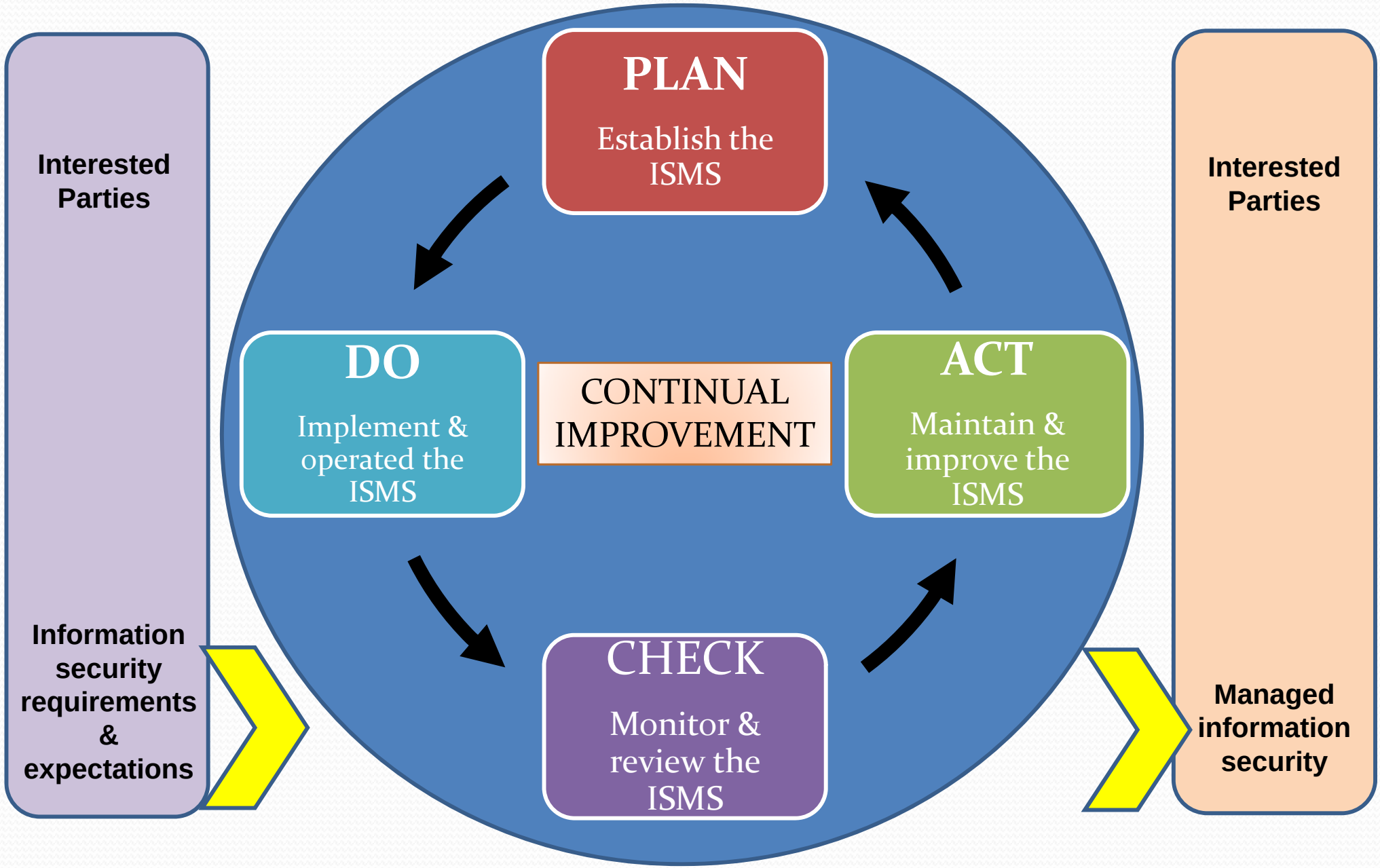
MEASUREMENT OF BUSINESS BENEFITS

- Manage risk down
- Provide tangible evidence to auditors
- Streamlined process of monitoring ISMS effectiveness
- Provides proactive toolset
- Reduction of security incidents over time
- Better root cause analysis of incidents / events
- Users see management support and buy-in
- Increased awareness of information security throughout the organisation
- Improvement in accountability

What is ISO 27001

- Based on an ISMS that establishes adequate and correct controls are put place to protect information assets so the business has confidence in its operations
- Utilises the PLAN, DO, CHECK, ACT cycle of:
  - Establishing
  - Implementing
  - Operating
  - Monitoring
  - Maintaining
  - Improving
- Uses a comprehensive set of controls applicable to all industry sectors
- The emphasis is on prevention

PDCA model applied to the ISMS process



PDCA OVERVIEW

- **Plan (establish the ISMS)**
  - Establish ISMS policy, objectives, processes and procedures relevant to managing risk and improving information security to deliver results in accordance with an organization's overall policies and objectives.
- **Do (implement and operate the ISMS)**
  - Implement and operate the ISMS policy, controls, processes and procedures.
- **Check (monitor and review the ISMS)**
  - Assess and, where applicable, measure process performance against ISMS policy, objectives and practical experience and report the results to management for review.
- **Act (maintain and improve the ISMS)**
  - Take corrective and preventive actions, based on the results of the internal ISMS audit and management review or other relevant information, to achieve continual improvement of the ISMS.

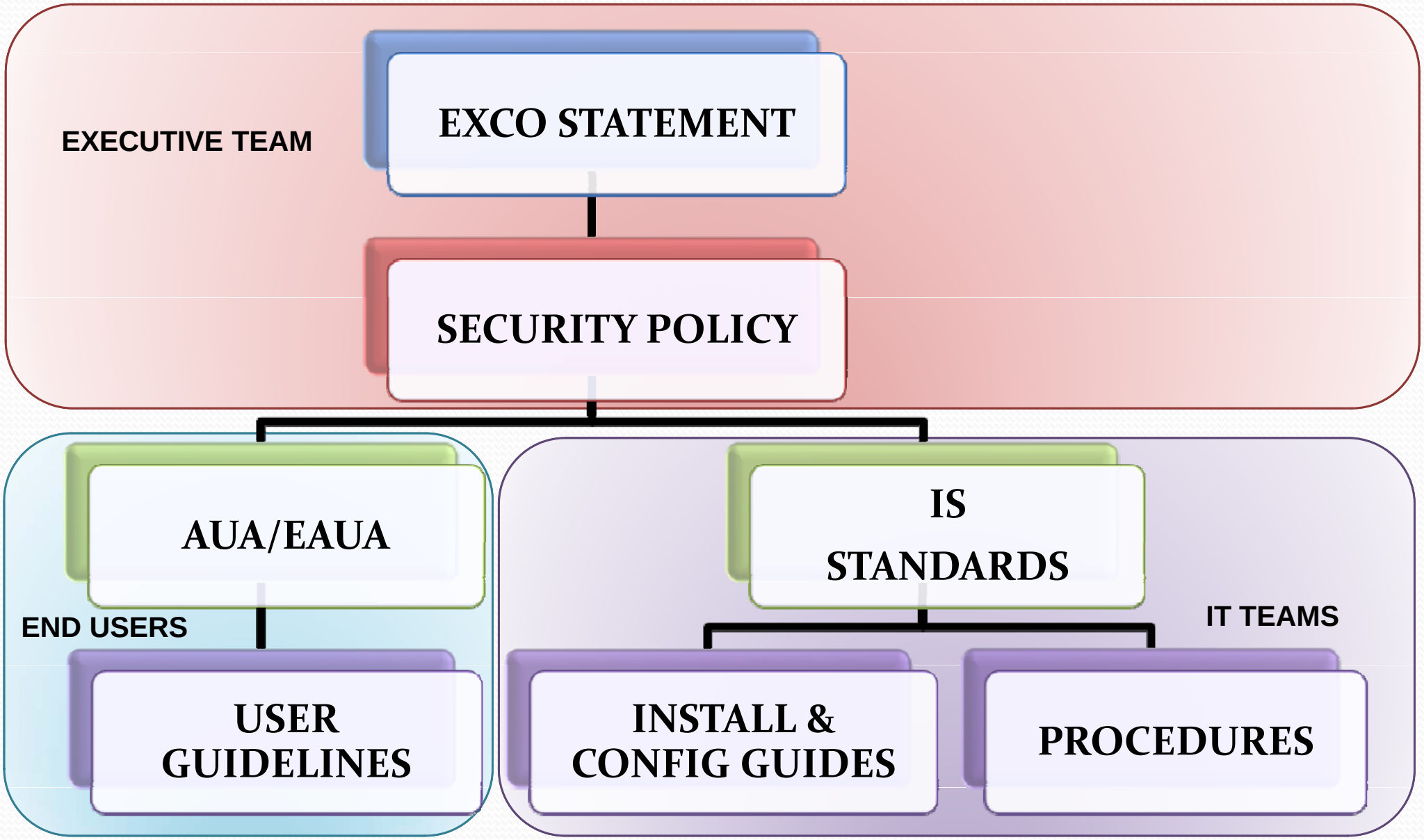
PDCA - KEY AREAS

- The PDCA cycle is an **ongoing process**, management must **continue to support** the ISMS through the following key areas of the cycle:
  - Monitor
  - Review
  - Improve
- To achieve compliance on a yearly basis **evidence** of the above process must be shown

What does the ISMS include?

- Policies and Standards
- Organisation Structure
- Planning Activities
- Responsibilities
- Practices
- Procedures
- Process
- Resources
- Guidelines

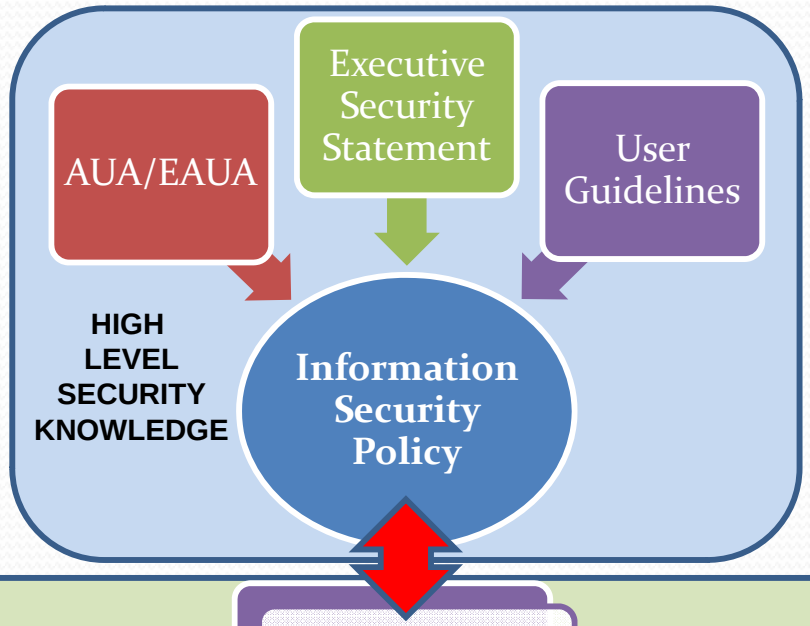
ISMS OVERVIEW



ISMS DETAILED VIEW / IMPLEMENTATION

AUA / EAUA 3-5 Pages
Sign-off statements for users to ensure they comply to specific company security requirements

IS Policy 3-5 Pages
Summary of the security standards. This is the main document staff will read and sign



Exec Statement – 1 Pager
High level security statement defining the Company's security ethic and posture, will include a statement of support from the CEO

Guidelines 3-5 Pages
Descriptive advisories to improve end user behaviour, e.g. password guides

Guiding Principles 50-100+ Pages
This is the core and comprehensive security document based on ISO27001. The document will follow the ISO standard to define all key security requirements

Standards 7-15 Pages
Expand specific security requirements and controls to what is expected in a specific area

Procedures / Baselines 5-10 Pages
Define specific steps that must be taken to implement a control. Baselines define the minimum Requirement for a system or component

ISO 27001 STANDARD OVERVIEW

The ISO Standard has:

- 11 Sections (A5 – A15)
- 39 Control Objectives
- 133 Controls

- **Clauses 4 – 8**

  These are the most important as they are mandatory

CLAUSES 4 -8

- The five mandatory requirements of the Standard
  - **Information Security Management System (ISMS)**
    - General requirements
    - Establishing and maintaining the ISMS (e.g. Risk Assessment)
    - Documentation requirements (e.g. Policy, Records, Statements, Plans, Controls)
  - **Management Responsibility**
    - Management Commitment (e.g. Chairman's Statement)
    - Resource Management (e.g. Training, Awareness)
  - **Internal ISMS Audits**
  - **Management Review of the ISMS**
    - Review Input (.e.g. Audits, Measurement, Meetings, Recommendations)
    - Review Output (e.g. Update Risk, Treatment Plan, Action Plan)
  - **ISMS Improvement**
    - Continual Improvement
    - Corrective Action
    - Preventive Action

This is the most important clause

CONTROLS

- Annex A of the Standard lists the Control Objectives and Controls
  - 11 Sections – A5 – A15
  - 29 Control Objectives – Each has a detailed summary of the objective of the control
  - 133 Controls – Each control has a summary of implementation advice
    - ISO 27002:2007 give guidance notes for each control
- The list is not exhaustive and additional controls can be added
- The ISMS process allows you to define which controls are applicable – Controls that are not applicable have to be justified.

A PERSPECTIVE ON CONTROLS

Management Controls

Security Policy, IT Policies, Security Procedures, Business Continuity Plans, Security Improvement Plans, Business Objectives, Management Reviews

Business Processes

Risk Assessment & Risk Treatment Management Process, Human Resource Process, SOA, Selection Process, Media Handling Process

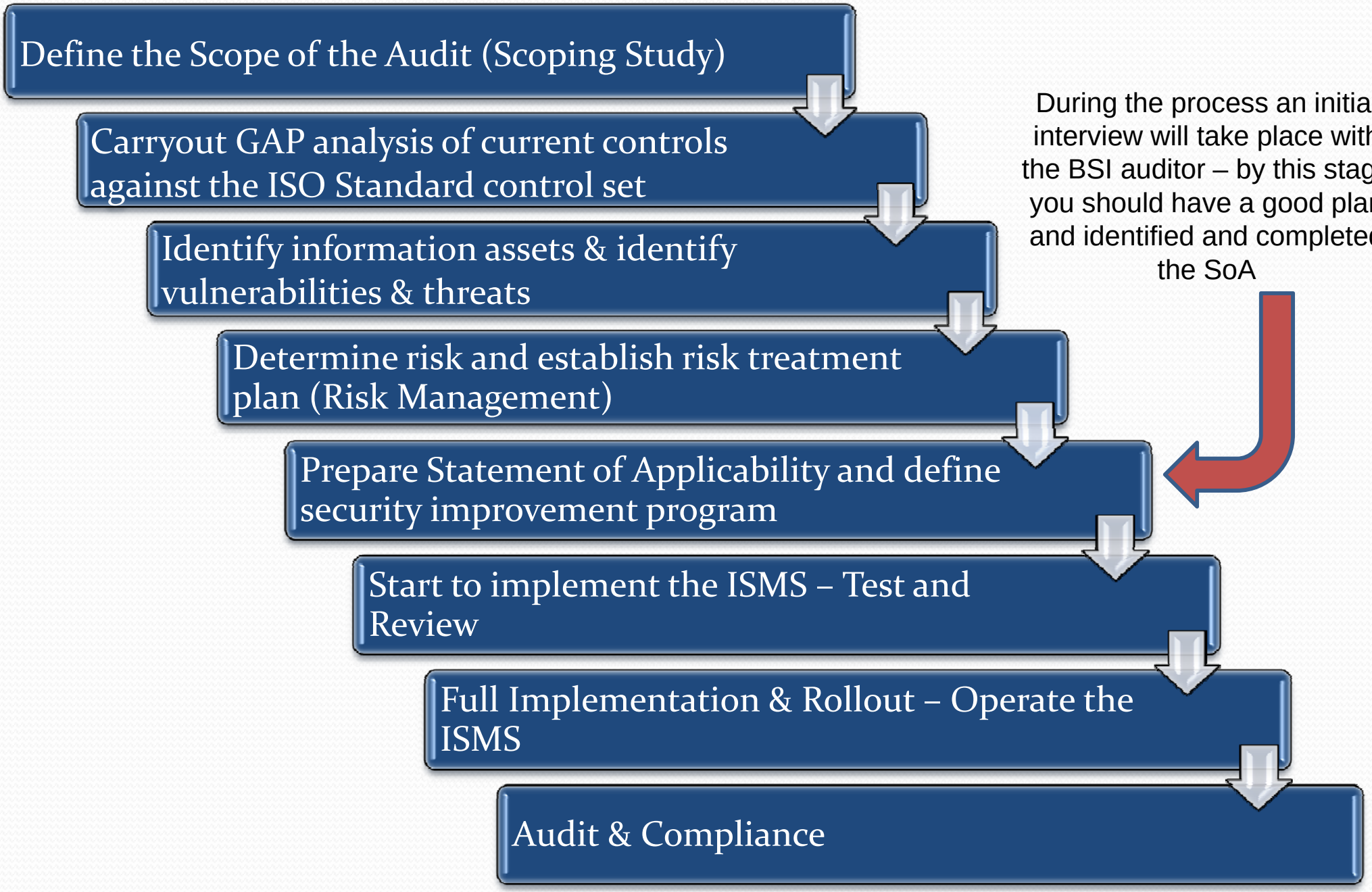
Operational Controls

Operational Procedures, Change Control, Problem Management, Capacity Management, Release Management, Back-up, Secure Disposal, Equipment off site

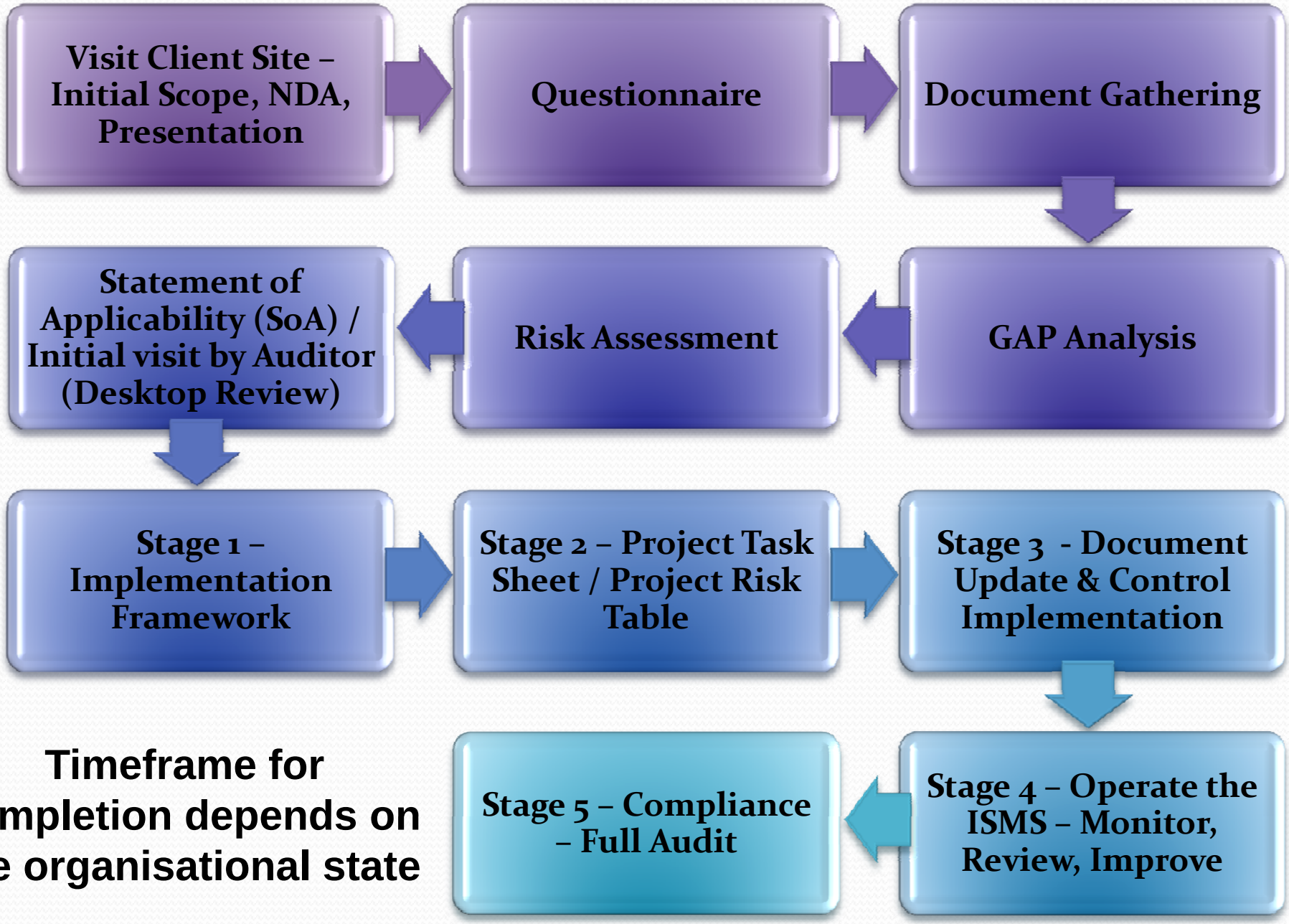
Technical Controls

Patch Management, Malware Control, IDS / IPS Monitoring & Handling, Firewalls, Content Filtering

ACHIEVING COMPLIANCE (OVERVIEW)



QCC PROCESS TO COMPLIANCE



Timeframe for completion depends on the organisational state

IMPLEMENTATION ISSUES

- Documentation development
  - Approval
  - Dissemination
  - Hosting
- On-going Risk Management Plan
  - Identification of critical assets / network diagrams
  - Risk Assessment / Risk Treatment
- On-going Training, Awareness and Development
- Policy enforcement
  - Internal / External assessments
- Continual management support and commitment
- Resources

BSI COMPLIANCE ROUTE

Stage 1
- Establish an Information Security Management System as identified in ISO 27001.

Stage 2
- Upon contacting BSI, we will provide an estimate of costs and timescales for formal assessment.

Stage 3
- Submit a formal application to BSI.

Stage 4
- BSI will undertake a desk top review of the Risk Assessment, Policy, Scope, Statement of Applicability and Procedures. This will then identify any weaknesses and omissions in your management system that need to be resolved.

Stage 5
- BSI will then conduct an on-site assessment and make recommendations.

Stage 6
- On successful completion of the audit, a certificate of registration is issued which clearly identifies the Scope of the Information Security Management System. This certificate remains valid for three years and is supported by routine assessment visits throughout.

CASE STUDY

- Leading UK Law Firm
  - Wanted ISO 27001 to:
    - More easily respond to client questionnaires on InfoSec/PII
    - Distinguish themselves from the competition
- 30-day QCC Resource to support initiative
  - Project Management
  - Applying Perspective and some Coal-Face work
- Client Resource: IT Manager and 2 IT Security staff
- Scope: IT Function
  - Two UK locations
  - Statement of Applicability to reflect appropriately

CASE STUDY - PROBLEMS

- Resources
  - Missing an Information Security Officer
  - Found it hard to dedicate some time to the project
- Documentation development
  - Very few IT processes (related to security) documented.
  - Too much in the heads of key staff rather than on paper
- Gap vs Risk Analysis
  - Need to be two distinct sets: no prob with Gap but why then Risk???
  - Identification of critical assets
- Policies
  - Very basic Policies in-place, no structure, no awareness no enforcement

CASE STUDY - SOLUTIONS

- Resources
  - QCC provided virtual Information Security Officer
  - Project Management booked solid days out
- Documentation development
  - We assisted with considerable library BUT still had to integrate properly.
  - Facilitated meetings to get knowledge written down
- Gap vs Risk Analysis
  - QCC undertook Gap Analysis
  - Facilitated a Workshop for Risk Analysis (used OCTAVE)
- Policies
  - Arranged meetings with HR to get the Policies on track and officially adopted, disseminated and enforced

OVERVIEW OF EACH CONTROL

Control A5 – Security Policy

To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.

Control A6 – Internal Organisation

To manage and plan information security within the organisation, taking into account the needs of both internal and external parties.

Control A7 – Asset Management

To deliver appropriate levels of protection and ensure that information receives a level of protection that is appropriate to its needs.

Control A8 – Human Resource Security

To ensure that staff, during employment, after termination and during change of employment, are part of the information security process.

OVERVIEW OF EACH CONTROL

Control A9 – Physical & Environmental Security

To secure buildings, locations and equipment in such a way as to prevent unauthorised physical access, damage and interference to the organisation's assets, premises and information.

Control A10 – Communications & Operations Management

To ensure that information is treated properly, backed up correctly and handled securely to the highest standards available..

Control A11 – Asset Control

To control access to information, networks, and applications. Preventing unauthorised access, interference, damage and theft.

Control A12 – Information Systems Acquisition & Development

To ensure that security is an integral part of the information system. Securing applications, files and reducing vulnerabilities.

OVERVIEW OF EACH CONTROL

Control A13 – Information Security Incident Management

To ensure information security events and weaknesses are communicated consistently in a manner allowing timely corrective action to be taken.

Control A14 – Business Continuity Management

To counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.

Control A15 - Compliance

To avoid breaches of any law, regulation or contractual obligations. To ensure compliance without adverse affects on Information Security.

Thank You

Neil Hare-Brown

MSc CISSP CISA CITP MBCS

neilhb@qccis.com

+44 (0)207 353 9000

www.qccis.com