BSI Group headquarters
389 Chiswick High Road
London W4 4AL
Tel: +44 (0)20 8996 9000
Fax: +44 (0)20 8996 7400
www.bsigroup.com

Responsible Committee:	IST/033 IT - Security Techniques
Title:	Controls Panel (IST/033/4) Summary of Work on Security Architecture Frameworks
Version:	0.A DRAFT
Date:	15 December 2011
Prepared by:	Ian Bryant – Study Period Rapporteur
Distribution:	IST/033/4 Consultative Group on Architecture
Information:	IST/033/4

References:

A. ISO/IEC JTC 1/SC 27/WG 4 N49942
B. ISO/IEC JTC 1/SC 27/WG 4 N49989

Issue

ISO/IEC JTC1 SC27 WG4 has adopted the UK suggestion of investigating the topic of Security Architecture Frameworks as a Study Period [A,B], with the Rapporteur being Mr I Bryant (UK). An initial report was provided for the SC27 meeting in Nairobi (October 2011), but the Study Period is now extended to the May 2012 SC27 meeting. This note summarises the current thoughts, as a basis for any further UK contributions to this Study Period.

Current Situation

At present the work on formalising Systems and Software Engineering is carried out under ISO/IEC JTC1 SC7, and work on Information Security is carried out in ISO/IEC JTC1 SC27, but there is no direct mapping between these activities, as illustrated at Figure 1, with the possible exception of the Verification phase.

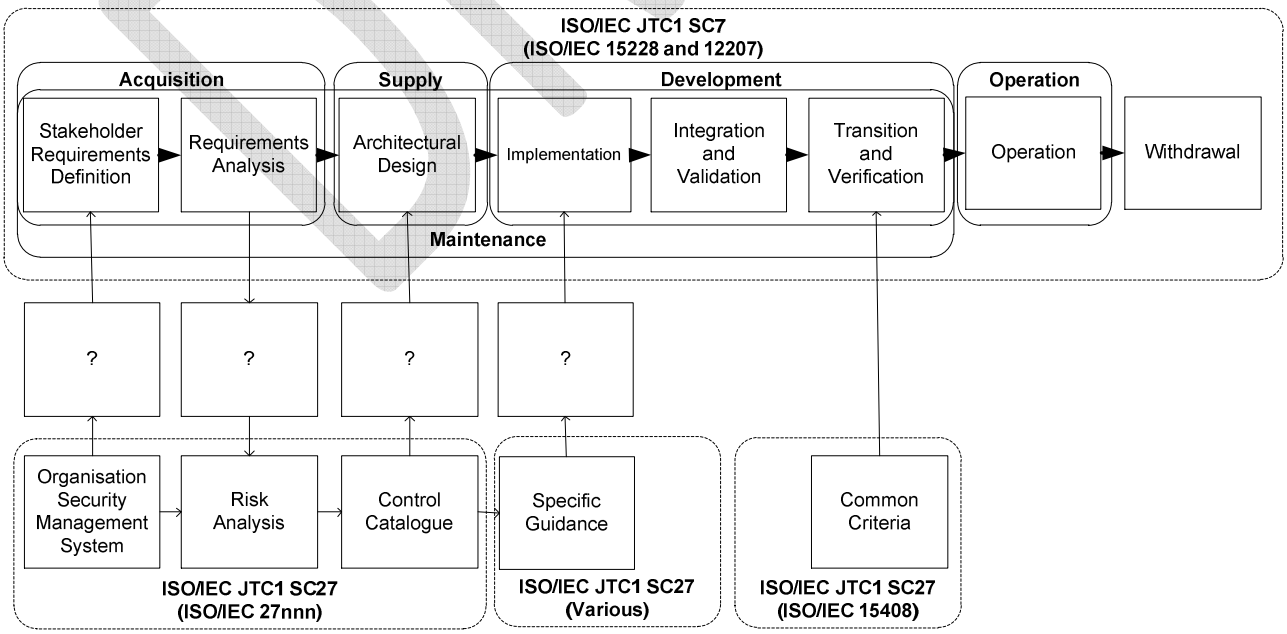

Figure 1

Possible Approach

This mapping deficiency can be express as a need for "*the conceptual structure and logical organization of a computer or computer-based system*", which is itself also a recognised definition of an Architectural approach.

The discipline of Architecture, according to Marcus Vitruvius Pollio (~75 BCE - ~15 BCE) is intended produce Artefacts that are:

- Dependable - in good condition and resilient
- Usable - should function well
- Agreeable - should address needs of users

These would appear to also be valid goals for an Information Security Architecture.

In terms of ICT, high level architecture is generally accepted to first introduced as the Zachman Framework[1], and has gone through many iterations since[2].

At the most abstract, such Frameworks decompose an architecture into a number of Levels, covering both Requirements and Implementation, which have been interpreted for Information Security at Figure 2.

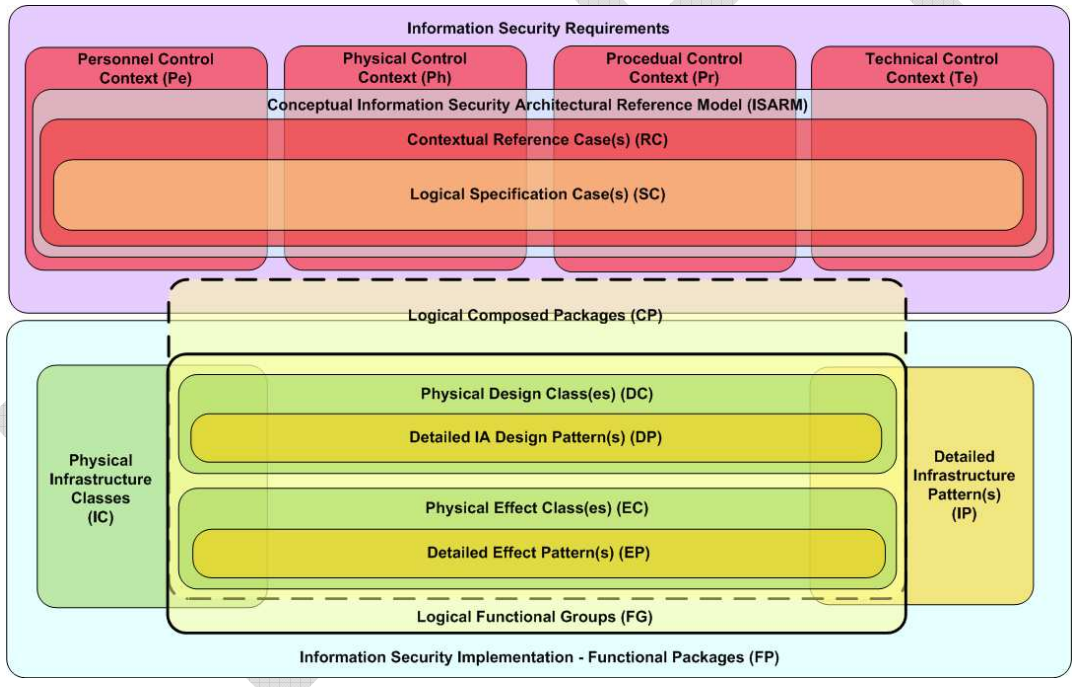

Figure 2

[1] John A. Zachman "A Framework for Information Systems Architecture", IBM Systems Journal 1987 (G321-5298), Vol 26, No 3

[2] Including, but not limited, to:

- US DOD Technical Architecture Framework for Information Management (TAFIM), 1991, later Command, Control, Communications, Computers, and Intelligence, Surveillance, and Reconnaissance (C4ISR), Jun-1996, and Department of Defense Architecture Framework (DoDAF), Aug-2003
- IFAC/IFIP Generalised Enterprise Reference Architecture and Methodology (GERAM), 1994
- The Open Group Architecture Framework (TOGAF), v1.0, 1995
- Reference Model of Open Distributed Processing (RM-ODP) (ITU-T Rec. X.901-X.904 & ISO/IEC 10746), 1998
- Enterprise Architecture Planning (EAP), 1998
- US ANSI/IEEE 1471 Recommended practice for architectural description of software-intensive systems, September 2000, now ISO/IEC 42010:2007
- UK Ministry of Defence Architecture Framework (MODAF), Aug-2005
- NATO Architecture Framework (NAF), a fusion of DODAF and MODAF

It will be noted that the Logical level provides the interface between Requirements and Implementation views of architecture.

In this model Generic functional specifications are defined as a CLASS and detailed implementations defined as PATTERNS. A collection of Patterns is referred to as a Composed Package.

- An import distinction in this model is between DESIGN and EFFECT:
- DESIGNS define requirements for components provide architectural Security Enforcing Functions (SEF), with Designs Classes / Patterns for Infrastructure (IC/ IP) being a special case which define SEFs for use as common Enterprise Architecture (EA) infrastructure components
- EFFECTS define Information Security requirements for components where security is a Non-Functional Requirement (NFR)

Approach Alignment

Recalling that the deficiency in mapping between ISO/IEC JTC1 Systems and Software Engineering and Information Security approaches (Figure 1) is a primary driver for considering Information Security Architecture, Figure 3 illustrates how the introduction of these concepts does seem to address the deficiency.

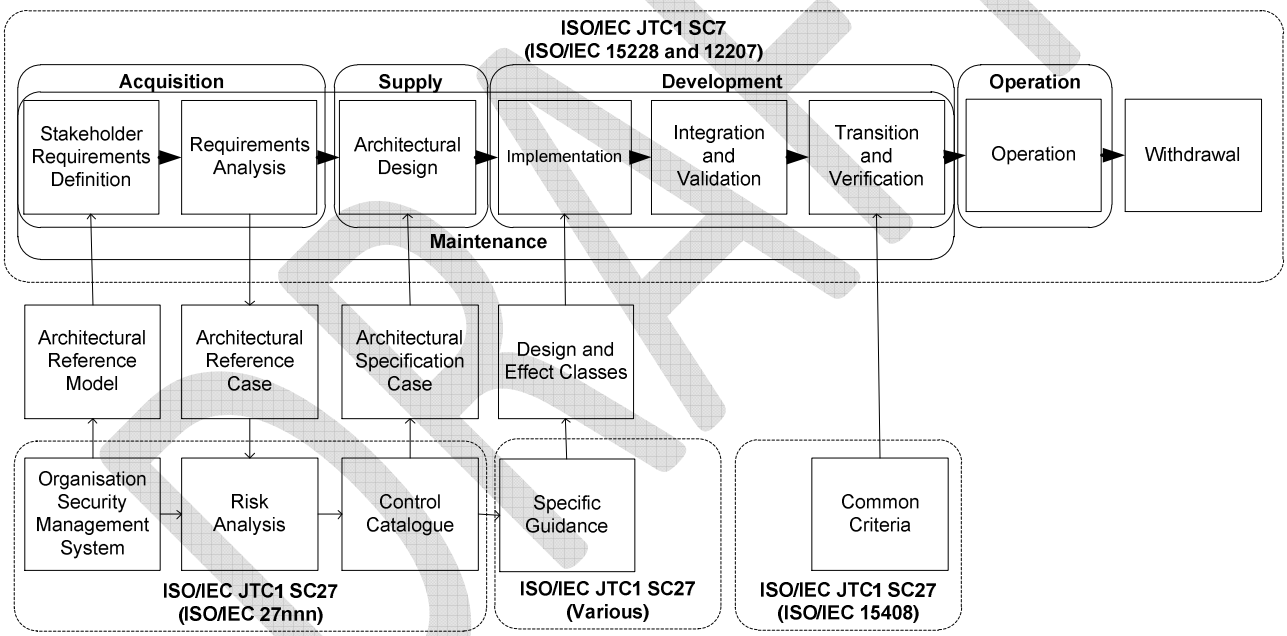

Figure 3

Benefits of Information Security Architecture Framework

As well as addressing the deficiency in mapping between ISO/IEC JTC1 Systems and Software Engineering and Information Security approaches, a major benefit of a common approach to Information Security Architecture, and in particular *de facto* recognition of Design and Effects Classes and Patterns, is the scope for re-use which will tend to minimise both nugatory effort and costs.

Standardisation Approach

An International Standard in Information Security Architecture should:

- Explain the value proposition, in particular in terms of re-use

- Draw the distinction between the Requirements and Implementation modes of use of architecture
- Clearly define the terminology that is required to be standardised
- For the Requirements mode, define the Concepts of Reference Model, Requirements Case and Specification Cases
- For the Implementation mode, define the concepts of Functional Groups and the subordinate Classes, explain the use of Composed Packages and Patterns, and draw the distinction between Designs and Effects
- Have a normative Annex that defines the Generic Effects Class, which is derived from ISO/IEC 27001/27002
- Have an informative Annex that itemises the Functional Groups (FG) and Classes (with the Strawman lists for FG and Classes, based on the work of the UK Government Chief Technology Officers' (CTO) Council, Information Assurance (IA) Domain on "IA Enterprise Architecture Framework" (© Crown Copyright) being provided at Annexes A and B to this document respectively)
- Have an informative Annex that itemises the Classes that are best delivered as Infrastructure components
- Have an informative Annex that shows an example of a defined Design Class
- Have an informative Annex that shows an example of a defined Pattern

Unresolved Issues

The following issues were identified in the Study Period, but will need further consideration should a New Work Item be pursued:

- A need for elements of the Catalogue to be independently validated
- An understanding as how Composability and Traceability is achieved and documented, as failures in integration could lead to weaknesses and vulnerabilities

Conclusions

An International Standard on Information Security Architecture would provide the means to addressing lack of mapping between ISO/IEC JTC1 Systems and Software Engineering and Information Security approaches, and, with the adoption of Design and Effects Classes and Patterns, provide a means of reuse of activity, which minimises both nugatory effort and costs.

DRAFT

Reference: UK Government Chief Technology Officers' (CTO) Council, Information Assurance (IA) Domain, IA Enterprise Architecture Framework (© Crown Copyright)

Most abstract – Logical Level – decomposition is into Functional Groups (FG)

1. Technical Functions (8)
   - Connectivity Protection (Te - Conn)
   - Cryptography (Te - Cryp)
   - Entity Authorisation (Te - EntA)
   - Media & Device Protection & Disposals (Te - MDPD)
   - Monitoring and Surveillance (Te - MonS)
   - Information Integrity Preservation & Protection (Te - IIPP)
   - Media and Information Authentication (Te MIAu)
   - Intrinsic ICT Functions (Te - IICT)

2. Non-Technical("P^3") Functions (3)
   - Personnel Security Functions (Pers)
   - Physical Security Functions (Phys)
   - Procedural Functions (Proc)

3. Data Management Functions (1)
   - Security Labels

DRAFT

Reference: UK Government Chief Technology Officers' (CTO) Council, Information Assurance (IA) Domain, IA Enterprise Architecture Framework (© Crown Copyright)

1. Connectivity Protection (Te – Conn (6))
    - Perimeter Control Design Class
    - Virtual Connection Design Class
    - Wireless Protection Design Class
    - Port Protection Effects Class
    - WAN/MAN Protection Effects Class
    - LAN/PAN Protection Effects Class

2. Cryptography (Te – Cryp (7))
    - Credential Generation Design Class
    - Credential Management Design Class
    - Credential Storage Design Class
    - Network Encryption Design Class
    - File Encryption Design Class
    - Internal Media Encryption Design Class
    - Removable Media Encryption Design Class

3. Entity Authorisation (Te – EntA (8))
    - User Authentication Design Class
    - Multifactor Authentication Design Class
    - Privilege Management Design Class
    - Biometrics Design Class
    - ID Management Design Class
    - Federation Design Class
    - Session Authentication Design Class
    - User Registration Design Class

4. Media & Device Protection & Disposals (Te – MDPD (4))
    - Media Erasure Design Class
    - Object Erasure Design Class
    - Mobile device remote disable/erase Design Class
    - Hard Copy Protection Design Class

5. Monitoring and Surveillance (Te – MonS (8))
    - Intrusion Detection Design Class
    - Intrusion Protection Design Class
    - Protective Monitoring Design Class

DRAFT

- Content Scanning (Malware / SpyWare) Design Class
- Forensic Capture Design Class
- Network Devices Design Class
- Network Management Design Class
- Mobile device tracking Design Class

6. Information Integrity Preservation & Protection (Te – IIPP (11))

- Device / Executable Control Design Class
- Technical Vulnerability Management Design Class
- Information Management Design Class
- Code Management Design Class
- Pre Boot controls Design Class
- System Virtualisation Design Class
- Time synchronisation Design Class
- Software licensing Design Class
- Offline Backup Design Class
- Remote Backup Design Class
- BCP / DR Facilities Design Class

7. Media and Information Authentication (Te – MIAu (2[3]))

- Media Authentication Design Class
- Realtime Policy Advice / Enforcement Design Class

8. Intrinsic ICT Functions (Te – IICT (12))

- Generic Effects Class
- Server Effects Class
- Workstation Effects Class
- Web Browser Effects Class
- Web Server Effects Class
- Email Server Effects Class
- DNS Server Effects Class
- PED Effects Class
- Service Bus Effect Class
- Audio Device Effect Class
- Video Device Effect Class
- Database Effect Class

9. Personnel Security Functions (Pers (3))

- Awareness Effect Class

[3] Logically also includes 3rd Class, Information Labelling, but this is now broken out as own Functional Group – Security Labelling – as part of Data Management not Information Security

- Training Effect Class
- Education Effect Class

10. Physical Security Functions (Phys (3))

- Data Centre Security Effect Class
- Static UAD[4] Security Effect Class
- Mobile UAD Security Effect Class

11. Procedural Security Functions (Proc (5))

- Audit Analysis Effect Class
- Forensic Analysis Effect Class
- Assurance Testing Effect Class
- Supply Chain Trust Effect Class
- BCP/DR testing Effect Class

12. Data Management Functions (1)

- Security Labels Design Class

DRAFT

[4] User Access Device