Annex – SCOPE and Outline of structure of the deliverable

Title	Security and resilience - Protective security architecture, framework and guidelines
Forward and Introduction	This will be an outline of the intent, purpose and content of the standard that, at a glance, will provide a view of its value to the reader.
Scope	The new international standard will detail the enterprise architecture[2], management framework and guidelines necessary to implement a principles-based approach to mitigating and managing protective security risk. The international standard will be helpful to any organisation in implementing and defining a structure for the range of protective security measures (security governance, information security, personnel security and physical security) in a way that is strategically aligned and cost effective.
Normative References	To include, but not necessarily be limited to: ▪ ISO 31000:2009, Risk management – Principles and guidelines ▪ ISO 28001:2007, Security management systems for the supply chain ▪ The ISO/IEC 27000 series – the ISMS Family of Standards ▪ AS4811:2006 Employment screening – in terms of personnel security elements, particularly regarding background screening (in the absence of an International Standard). Referencing a range of national standards that reflect current good international practice, will be beneficial. Such references will include, but not be limited to, AS4811:2006 (above).
Terms and Definitions	To include, but not necessarily be limited to: ▪ Risk and the risk-related terms as defined in ISO 31000:2009, Risk management – Principles and guidelines, such as likelihood, consequence, intent, capability, vulnerability, criticality, impact etc. ▪ Other protective security-related terms that require additional definition such as – Security governance and related terms – Information security and related terms, including cyber security and – Personnel security and related terms – Physical security and related terms.
Clauses	See attached base draft.
Tables and Figures	To be determined.

Formulae	While reflecting the commonly accepted principle that security risk is largely qualitative, this section may reference risk-related formulae.
Annexes	Key annexes will provide additional detail on the detail and implementation of Tier 3 controls, with high-level guidelines. Importantly, the relationship between the Tier 1 principles, the Tier 2 outcomes and the Tier 3 controls will be demonstrated in necessary detail, and visually represented.
Bibliography	As indicated, the recently completed 'Review of Protective Security' included a comprehensive analysis of current protective security and security risk literature, international policy thinking and terminology. This new work item is the culmination of substantial research and analysis of protective security approaches and practices around the world. This has enabled mapping of the contemporary protective security lexicon (attached to the 'Review of Protective Security Frameworks' referenced at Annex 2), encapsulating protective security policy frameworks of various jurisdictions and the thinking that many in the international security community share in relation to protective security. This informs the need for this proposed new international standard, and provides the analytical point of departure in its initial formulation.

[2] Enterprise architecture (EA) is a well-defined practice for conducting organisational enterprise analysis, design, planning, and implementation, using a holistic approach at all times, for the successful development and execution of strategy.

Annex 1

Base draft of the proposed new international standard

The attached base draft was presented, discussed and, with a range of inclusions, accepted at ISO/TC292 Working Group 6 meeting, 24-28 April 2017. These inclusions have been integrated into the current text.

Annex 2

Review of protective security frameworks

Presented and accepted at ISO/TC292 Working Group 6 meeting, 5-8 September 2016, Edinburgh.

Annex 3

Report on the rationale for an ISO standard for a protective security architecture

A study into why the global security community needs an international Protective Security Standard and why the timing is right.

Fifteen years after the terrorist attacks on September 11, 2001 (9/11) threats at the international level have continued to evolve from the traditional, conventional inter-state conflicts to attacks perpetrated by de-structured, networked non-state actors (McConnell 2007, p.50), particularly terrorists and transnational criminals. This changing environment has been driven by a range of factors, such as globalisation, increased economic and democratic liberalism and advances in technology.

In this new environment, private sector defence organisations have increased, as has the number of democratic states and both groups are taking on a greater role within the international security community. In order to manage this new diversity, the international security community, in partnership with the International Organisation for Standardization (ISO 2016, paragraph 1), is developing an ISO Standard to provide guidance for the management of Protective Security across multiple industries in both the public and private sectors (Brown 2016a, p.2). At its heart, the main objective in developing the Protective Security Standard is to support nations, societies, industry and people, in remaining free from danger (ISO Review 2016, p.2). The new standard seeks to build on existing Risk Management Standards, but with a focus on the security aspect of human intent and the threat of malicious actors (ISO Review 2016, p.7).

Divided into four sections, this discussion will seek to understand why there is a need for a Protective Security Standard, how the changing international structure and the range of threats have contributed to that need and how the evolving security environment has meant the timing is right for a Protective Security Standard. It will also outline the benefits that standardization can provide to the security industry and finally it will consider future implications for international security should the standard fail to be adopted and implemented.

The Need for a Protective Security Standard

At first glance, a model for standardizing protective security may not seem necessary. Information management and sharing between nations, governments and organisations in the current era of sharing information has increased dramatically since 9/11 (Sepper 2010, p.153). There are many unofficial agreements and mechanisms in place that allow for intelligence sharing, as well as more formal bilateral and multilateral agreements between nations. What is different today is the number of non-state actors, on both sides of spectrum, which have entered the security environment.

The security environment of today requires a quick and agile response (Jones 2007, p.384) for dealing with international threats that are often fluid and difficult to detect. Terrorist non-state actors and transnational criminals no longer operate within traditional state boundaries and states can no longer defeat or contain these threats in isolation (Drabot 2013, p.1). Many of the security organisations, in place since World War II, are no longer capable of dealing with the current security environment (Anderson 2012, p.27). A more robust and standardized system for facilitating the management and sharing of information at the international level is required.

Globalisation is a significant contributor to the current security environment. The free movement of peoples across fluid state borders (Walsh 2006, p.627) has posed significant challenges for security in monitoring terrorist activities, transnational crime, people smuggling and drug trafficking (Walsh 2006, p.627). In this environment, the immediacy of information sharing is vital to facilitate practical decision-making.

Increased economic liberalization and the growing number of democratic states have altered the structure of the international state-based system. In 1973 democracies equated to 27% of the state system and by 2006 the number of democracies had grown to 63% (Anderson 2012, p.29). At the same time, the global economy has increased exponentially from $2.9 trillion in 1970 to $63.1 trillion in 2012 (Anderson 2012, p.29 cited World Bank 2012). This global growth has liberalized the political system and with the growing number of democratic states, has increased the need for a standardized system with which to manage protective security information. This increased number of democracies also provides an opportunity to

broaden the information sharing alliances and collaborations, but a more standardized approach is required to facilitate this.

There is an urgent need for a common approach and increased standardization towards protective security management in order to support cooperation at the international level (Kosanke 2006, p.55). The development and implementation of a best practice Protective Security Standard would improve collaboration and interoperability between private and public sectors as well as states, by providing a common language, streamlined processes, guidelines and objectives for managing important information, assets and people (Kajava et al 2006, p.2093).

The Protective Security Standard seeks to build on the ISO 31000 Risk Management Standard, but it will apply a narrower view to security threats, with a focus on malicious actors and their intent to cause harm and disruption (ISO Review 2016, p.2). Over the past decade the security brief to governments has become very broad, paradoxically one of the limitations with the 'all hazards' view is that it seeks to apply a one-size-fits-all approach to national security. Non-traditional threats are important to states, but they can be managed through a risk management approach, which ISO 31000 is designed to facilitate (ISO 31000 2016, p.12). Protecting against malicious acts and actors requires a different understanding of managing risk, one that is separate from the broader 'all hazards' approach.

Malicious acts involve intent, which is a key difference in understanding this approach. This differs from preventing a natural disaster, pandemic or climate change, as those events can be predicted to a certain degree. Malicious acts are connected to the intentions and capabilities of humans to do harm, which are less predictable. Security threats can no longer be defined in terms of just the nation state; individuals must now be factored into security thinking. Modeled in a similar vein to threat management strategies (Harding 2014, p.484), Protective Security management seeks to identify the actor and to prevent the actor's negative behaviour. It focuses on understanding the target of the malicious actor, the areas of vulnerability for an organisation and reducing the likelihood of an attack.

The 2012 attack on the United States (US) Embassy in Benghazi, Libya is an example of why there is a need for a Protective Security framework and how standardization may add value to the current risk assessment system. In 2014 the US Senate Select Committee on Intelligence reviewed the attack and found that while there were security protection and risk management procedures in place designed to protect the complex, what the risk assessments failed to understand was that the embassy was an intended target (Harding 2014, p.484). The Committee concluded that the US State Department should have been aware of the threat level to the embassy and increased security accordingly (Harding 2014, p.484). A Protective Security framework would have provided an assessment of the malicious actors and their intentions within the environment, not just the risk factors associated with the collateral damage of being located within a hostile environment.

The benefits of a standardized approach

ISO Standards are primarily about ensuring quality; they are the most widely used and are recognized as the global benchmark (Susanto et al 2011, p.28). The Protective Security Standard will provide a unified approach for organisations collaborating on intelligence and security. The World Trade Organisation (WTO) requires member states to adhere to ISO Standards because they create a level playing field (ISO Central Secretariat 2012,p.2). In this way, an international Protective Security Standard will provide unity and smooth out any cultural, language or regional differences that are a barrier to successful collaboration (Tsohou 2010, p.351).

ISO Standards certifications provide organisations with credibility and a level of recognition worldwide (Bizmanualz 2016, 3rd paragraph). They also provide customers with a level of confidence in the quality of the organisation (Saint-Germain 2005, p.60), which can lead to business opportunities, deliver long-term sustainability through improved business processes which can reduce the risk of security breaches (Saint-Germain 2005, p.64). A standardized approach can facilitate a level of transparency that is necessary across the security industry in order to build trust between organisations (Fomin et al p.1). States that have high levels of compliance and security may be reluctant to share information with states that are known to have weaker processes in place. Trust is one of the key issues around successful information sharing and an ISO Standard can provide a level of assurance, consistency and reliability (Purdy 2010, p.881) for organisations, which leads to more confident decision-making. As the threats and malicious actors have evolved and diversified, so too has the security industry that seeks to combat them. Globalisation and new technologies have broadened the range of threats, but it has also increased the means with which to combat them. It is this new security environment that has determined the need for a standardized approach to Protective Security. The role of the private sector in national security is steadily increasing, with national

governments outsourcing more of the intelligence process to the private sector. The framework of the Protective Security Standard is designed to work with the current and evolving risk and threat environment. By implementing the framework, organisations will produce a better understanding of their capabilities, the assessed risks and threats to their environments. There is a particular focus on malicious acts and the measures organisations need for protection. In order to achieve a high level of integrity, there needs to be an international-led unified approach that enables a range of stakeholders to adopt common practices (Brown 2016a, p.2).

Adopting a Protective Security framework will also increase resilience. Organisational resilience is an important aspect of security because it is a measure of the sustainability of the system and determines how well an organisation or state can recover from shocks (Ayyub 2014, p.341). Resilience is also an indication of how well the organisation may manage or reduce risks and failures (Ayyub 2014, p.341). The benefits of the framework to states and organisations can also be financial. Resilience can be measured in terms of savings and losses as well as a cost-benefit analysis gained from implementing operational improvements through standards (Ayyub 2014, p.352). Examples of direct financial gains from resilience are difficult to quantify, but the French government has reported 2.5% of GDP growth can be attributed to standardization (ISO Central Secretariat 2012, p.3), and in the UK, standardization reportedly contributes GBP 2.5billion annually to the economy (ISO Central Secretariat 2012, p.4). ISO Standards have also become a strategic means of achieving a competitive advantage (Hung-Chung et al 2015, p.31).

Why the Standard could fail to achieve its objectives

There are a number of reasons why a standard could fail to achieve the objectives for which it has been designed. These include; low levels of implementation due to complexity or cost, a lack of trust across the industry, and the threat of defections by organisations and states. One of the most challenging aspects of developing a new standard is striking the right balance between complexity and simplicity (Brown 2016b). To give a standard meaning, it needs to be universally applied across large, medium and small organisations. If the is too complicated then the rate of adoption may be low. For example, when the standard for Quality Management ISO 9000 (ISO Standards, paragraph 1), was published in 1987 (ASQ, paragraph 2), one of the difficulties was interpreting exactly what the standard required, which resulted in inconsistencies between consultants (Fomin et al, p.8). Popularity for ISO standards has grown since the 2000s (ISO Surveys 2015), but overall, implementation of ISO Standards remains quite low.

The cost of implementing a standard, which requires technical resources and capabilities, can be an impediment. This is particularly true for developing nations and of the 162 ISO member states more than three-quarters are classified as developing countries (ISO Action Plan 2016, p.2). In addition, developing countries tend to have a lower ability to build and implement the required technology (Shaaban et al 2012, p.517). The 2015 ISO Annual Survey indicates the regional areas of Africa, Central and South America, Central and South Asia and the Middle East account for only 13.8% of 27,536 organisations that have implemented the standard for Information Security Management ISO 27001 (ISO Surveys 2015, 27001). Developing countries generally have weaker laws and legislation with regards to security issues (Shaaban et al 2012, p.519) and are more likely to have the conditions that encourage terrorists and transnational criminals to operate within their borders. The low adoption of standards is a crucial issue for global security and future collaboration between nations, a particular focus and assistance should be given to the developing world.

One of the most significant impediments to the success of the Protective Security Standard is a lack of trust between states. Despite their joint common market and the lack of physical borders, the European Union (EU) states have not yet developed practices to overcome their cooperation issues (Walsh 2006, p.626). All the while terrorist and transnational criminal activities continue to rise (Drabot 2013, p.1), threatening the safety of EU citizens. A significant aspect that prevents the development of a trust dynamic between states is the fear of defection (Walsh 2007, p.158). While common interests can be a contributing factor to overcoming defection and encouraging cooperation, historically shared threats have not guaranteed cooperation (Lefebvre 2003, p.529). However, the current threat environment is not one that has been faced before and states may be more incentivized towards cooperation to combat against malicious acts and actors. A Protective Security Standard will be a key element towards encouraging collaboration between states and organisations because it can provide a high level of compliance and transparency, enhancing the credibility and reliability of information management at the international level.

Implications for the international community

Since World War II there have been a number of security alliances and organisations that have formed to facilitate information and intelligence sharing across borders, these include the UKUSA Agreement and The

Five Eyes (Sepper 2010, p.157), The Club of Berne (Lefebvre 2003, p.530), NATO (Lefebvre 2003, p.531), and Europol just to name a handful. These organisations have common intelligence databases and information sharing arrangements, but with restricted memberships there are limitations to what these security alliances can achieve. Despite working together with common practices, these organisations do not have mandated guidelines for sharing information, the same quality controls or security standards (Drabot 2013, p.18).

Bilateral arrangements remain the most prevalent security arrangements, but a Protective Security Standard is now required in order to broaden the existing network of countries and organisations that contribute intelligence. Without standardization, information sharing will continue, but it will not develop much further than its existing functionality. The increase of private and public sector actors operating in the current security environment allows for the potential of a much larger net from which to draw information. If the standard is not widely accepted or adopted, information sharing will more than likely continue to be restricted only to the top tier intelligence nations. The success of the Protective Security Standard will depend on how motivated states and organisations are to work together. The fear of consequences of defection, of not collaborating, or the threat of a major terrorist attack, may play a significant role in driving adoption and compliance.

Conclusions

Globalisation and technology have created a faster world where information is generated and dispersed instantly and people move between nations with more ease than ever before. This has brought significant advances, such as increased trade activity, as demonstrated by the unification of the EU; but that experiment has also demonstrated the same advantages are available to malicious actors. Security threats continue to evolve and the traditional structures formed in the post World War II era are no longer sufficient to protect today's systems, assets and people. Global security infrastructures and processes need to reflect and respond to current developments.

The complexities of the international environment, with increased players on both sides and advancements in technology, have elevated the importance of guidelines and processes at the international level. This environment has not developed overnight, but it has taken the past fifteen years for the international security community to accept they must now work together, across states and organisations, if they are to successfully combat the increasing threats posed by malicious acts and actors. The timing is now right for the development and acceptance of a Protective Security Standard.

The ISO Protective Security Standard is designed to be the bridge that links (Susanto et al 2011, p.27) the private and public sectors, states and organisations with the aim of keeping people free from threats. It is also aimed at facilitating best practice for sharing of information between states and organisations. Developing the ISO Standard is an exercise in international collaboration in itself involving large numbers of stakeholders and the end result is yet known. There are risks that the standard will not achieve the objectives to which it has been designed, or that it will not be adopted in the areas that need it most. If the standard is not well received and adopted then the status quo will remain much as it is today, but the threats posed by malicious actors will continue to increase.

Further research and analysis will be required to assess the success or failure of the standard in the years following its publication. Despite the current decline of the traditional nation-state threats, which may turn out to be only temporary, the role of intelligence is not diminishing (Sepper 2010, p.153). The environment is evolving, but it appears certain that in the coming decades the importance of intelligence and information sharing for protecting assets, systems and people, will only increase which is why the standard for Protective Security is an essential development.

References

Anderson, ND 2012, '"Re-redefining" International Securing: Bringing Intent Back in', Josef Korbel Journal of Advanced International Studies, 4, Summer, pp.27-47

Ayyub, BM, 2014, 'Systems Resilience for Mulithazard Environments: Definition, Metrics, and Valuation for Decision-Making', Risk Analysis, Vol.34, Issue 2, pp.340-355

Bizmanualz.com, 2016, 'What are the 10 Reasons Why you need ISO9001 Certification?' viewed 28 September 2016, http://www.bizmanualz.com/obtain-iso-certification/what-are-10-reasons-why-you-need-iso-9001-certification.html

Brown, J, 2016a, 'Draft of the Roadmap for ISO/TC 292 WG6', ISO Protective Security, 10 May, pp.1-7

Brown, J, 2016b, 'Interview with L. Wray', 28 September 2016

Diesing, G, 2011, 'The Future of Quality ISO Standards', Quality, May, Vol.50, Issue 5, pp. 36-39

Drabot, AL, 2013, 'Transatlantic Intelligence Sharing and the Fight Against Terrorism', ProQuest Dissertations Publishing, pp.1-39

Fomin, VV, de Vries, HJ, Barlette, Y, 'ISO/IEC 27001 Information Systems Security Management Standard: Exploring the Reasons for Low Adoption', Rotterdam School of Management, Erasmus University, Rotterdam, pp.1- 13, https://static.aminer.org/pdf/PDF/000/249/641/an_empirical_exploration_of_how_process_standardization_reduces_outsourcing_risks.pdf

Harding, D, 2014, 'Threat Management: The Coordinated Focus on the Threat Actor, Their Intentions, and Attack Cycle', Journal of Applied Security Research, Vol.9, No.4, pp.478-494.

Hung-Chung, S, Dhanorkar, S, Linderman, K, 2015, 'A Competitive Advantage from the implementation timing of ISO management standards', Journal of Operations Management, Vol.37, pp.31-44

ISO Central Secretariat, 2016, 'ISO Action Plan for Developing Countries 2016-2020', ISO, pp.1-16 http://www.iso.org/iso/iso_action_plan_2016-2020_en_ld.pdf

ISO Central Secretariat, 2012, 'ISO Standards – What's the Bottom Line?', ISO, pp.1-12, http://www.iso.org/iso/bottom_line.pdf

ISO, International Organisation for Standardization, viewed 25 October 2016 http://www.iso.org/iso/home.html

ISO/TC292, 2016,'ISO/CD 31000 Risk Management – Framework and process – Guidelines', 1 June, pp.1-39

ISO, 2015, 'ISO Survey's', viewed 18 October 2016, http://www.iso.org/iso/iso-survey

ISO, 'Benefits of Standards', viewed 28 September 2016, http://www.iso.org/iso/home/standards/benefitsofstandards.htm

ISO, 2016, 'Review of Protective Security Material', 10 May, pp.1-9

Jones, C, 2007, 'Intelligence Reform: The Logic of Information Sharing', Intelligence and National Security, Vol.22, No.3, June, pp.384-401

Kajava, J., Anttila, J., Varonen, R., Savola, R. and Roning, J., 2006, December. 'Information security standards and global business', Industrial Technology, 2006. ICIT 2006. IEEE International Conference on, pp. 2091-2095

Kosanke, K., 2006. 'ISO Standards for Interoperability: a comparison' *Interoperability of Enterprise Software and Applications*, pp.55-64

Lefebvre, S, 2003, 'The difficulties and dilemmas of International Intelligence Cooperation', International Journal of Intelligence and CounterIntelligence, Vol.16, No.4, pp.527-542

McConnell, M, 2007, 'Overhauling Intelligence', *Foreign Affairs*, Vol.86, No.4 p.50

McCormack, T, 2015, 'The British National Security Strategy: Security after Representation', The British Journal of Politics and International Relations, Vol.17, pp.494-511

Purdy, G, 2010, 'ISO31000: 2009 – Setting a New Standard for Risk Management', Risk Analysis, Vol.30, No.6, pp.881-886

Saint-Germain, R, 2005, 'Information Security Best Practice Based on ISO/IEC 17799', The Information Management Journal, July/August, pp.60-66

Sepper, E, 2010, 'Democracy, Human Rights, and Intelligence sharing', Texas International Law Journal, Vol.46, issue 151, pp.151-207

Shaaban, H, Conrad, M, French, T, 2012, 'Towards a Framework for Managing Information Security in Zanzibar's Public Organisations: A Developing Country's View', IADIS International Conference e-Society, pp.516-520

Susanto, H, Almunaware, MN, Tuan, TC, 2011, 'Information Security Management Systems Standards: A Comparative Study of the Big Five', International Journal of Electrical & Computer Science, Vol.11, No.5, pp.23-29

Tsohou, A, Kokolakis, S, Lambrinoudakis, C, Gritzalis, S, 2010, 'A Security Standards' framework to facilitate best practices awareness and conformity', Information Management & Computer Security, Vol.18 Issue 5, pp.350-365

Walsh, JI, 2007, 'Defection and Hierarchy in International Intelligence Sharing', Journal of Public Policy, Vol.27, Issue 2, pp.151-181

Walsh, JI, 2006,'Intelligence-Sharing in the European Union: Institutions are not enough', JCMS: Journal of Common Market Studies, Vol.44, No.3, pp.625-643

Protective Security Bibliography (as at 25th August 2016)

C. Alberts, A. Dorofee – 'Managing Information Security Risks: The OCTAVE sm Approach', Addison Wesley, 9 July 2002, pp.1-466
http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.461.7807&rep=rep1&type=pdf

AlertBoot, viewed 17th August 2016,
http://www.alertboot.com/blog/blogs/endpoint_security/archive/2009/03/13/what-is-data-at-rest-encryption.aspx

ASIS (Europe) –'Global Competency Model for Security Professionals- Physical Security', pp.1-37

ASIS International, Protection of Assets, October 2012
https://www.asisonline.org/Pages/default.aspx

Australian Government: ASIO Business Liaison Unit – 'Critical Infrastructure Guide: Develop and review security plans', 11th February 2016, pp.1-20

Australian Government: ASIO Business Liaison Unit – 'Critical Infrastructure Guide: Selecting Security Systems and Hardware', 11 February 2016, p.1-33

Australian Government – 'Protective Security Policy Framework: Australian Government Security Classification System', viewed 16th August 2016
https://www.protectivesecurity.gov.au/informationsecurity/Pages/AustralianGovernmentSecurityClassificationSystem.aspx

Australian Government – 'Protective Security Policy Framework: Information Security Management Guidelines', 1 November 2014, pp.1-21, viewed 16th August 2016
https://www.protectivesecurity.gov.au/informationsecurity/Documents/INFOSECGuidelinesAustralianGovernmentSecurityClassificationSystem.pdf

Australian Government – 'Protective Security Policy Framework: Physical Security', viewed 10th August 2016
https://www.protectivesecurity.gov.au/physicalsecurity/Pages/default.aspx

Australian Government – Protective Security Policy Framework: Security Risk Management, viewed 17th August 2016
https://www.protectivesecurity.gov.au/governance/security-risk-management/Pages/Security-risk-management.aspx

Australian National Audit Office – 'Management of Personnel Security: Follow up Audit', 2008, pp.1-94, viewed 11th August 2016
https://www.anao.gov.au/sites/g/files/net616/f/ANAO_Report_2007-2008_41.pdf

A. Banerjee, R. Hanna, J. Kyle, B.A. Olken, S. Sumarto – 'Tangible Information and Citizen Empowerment – Identification Cards and Food Subsidy Programs in Indonesia', November 2015, pp.1-38
http://economics.mit.edu/files/11175

Business Economics – A Library of Information, viewed 16th August 2016
http://businessecon.org/2014/11/tangible-and-intangible-business-definitions-and-use/

Cisco – 'Secure Data Center Architecture: Protecting Data in Transit and at Rest', 2008, pp.1-2
http://www.cisco.com/c/dam/en_us/solutions/industries/docs/gov/nwsltr0708SecureDC.pdf

CPNI – Centre for the Protection of National Infrastructure (UK), viewed 10th August 2016.
http://www.cpni.gov.uk/advice/Physical-security/

Defence in Depth – 'Trusted Information Sharing Network for Critical Infrastructure Protection', June 2008, pp.1-102

E.S Elliott, F.Fons, A. Randell – 'Business Architecture and Agile Methodologies – A Business Architecture Guild Whitepaper'. Business Architecture Guild, February 2015, pp.1-16
http://c.ymcdn.com/sites/www.businessarchitectureguild.org/resource/resmgr/BA__AgileMethodologis.pdf

ENISA – European Union Agency for Network and Information Security – 'Risk Management & Information Security Management Systems', viewed 9th August 2016
https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-isms

E. Ganesan, R. Paturi – 'Building Blocks for Enterprise Business Architecture', SETLabs Briefings, Vol.6 No.4 2008, pp.3-14
https://www.infosys.com/consulting/architecture-services/white-papers/Documents/enterprise-business-architecture.pdf

J. Gerakos, J.T Linnainmaa – 'Market Reactions to Tangible and Intangible Information Revisited', Critical Finance Review, 2016, Vol.5, pp.135-163
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2358513

ISO – Business Architecture: Framework. Survey of Architecture Frameworks, viewed 25th August 2016
http://www.iso-architecture.org/ieee-1471/afs/frameworks-table.html

ISO/IEC/IEEE 42010 – 'Systems and Software Engineering – Architecture Description', International Standard, 1 December 2011, pp.1-47
http://www.iso-architecture.org/ieee-1471/afs/

E. Lewis – 'Enhancing Enterprise Architecture Practices in the Department of Defence', Layrib PTY Limited, 22nd December 2010, pp.1-112

N. Lord – 'Data Protection: Data in Transit V Data at Rest', Digital Guardian, Monday 13th June 2016, viewed 16th August 2016
https://digitalguardian.com/blog/data-protection-data-in-transit-vs-data-at-rest

D.W McDavid – 'A Standard for Business Architecture Description', IBM Systems Journal, 12th October 1998, Version 3.3, pp.228-2728

NCSIP – National CIO Council Subcommittee for Information Protection (Canada) – 'Public Sector Security Classification Guideline', 7th September 2004, pp.1-10
http://www.iccs-isac.org/en/pubs/Security%20Classification%20Guideline%20-%20Final%20Verison%202004-09-07.pdf

New Zealand Government – 'Agency Personnel Security', viewed 11th August 2016,
https://protectivesecurity.govt.nz/home/personnel-security-management-protocol/agency-personnel-security/

New Zealand Government – 'Protective Security Requirements', viewed 11th August 2016
https://www.protectivesecurity.govt.nz/home/physical-security-management-protocol/physical-security-management-protocol-2/introduction-3/definition-of-physical-security/https://www.protectivesecurity.gov.au/governance/security-risk-management/Pages/Security-risk-management.aspx

Object Management Group – 'Business Architecture Overview', viewed 9th August 2016
http://bawg.omg.org/business_architecture_overview.htm

The Open Group – 'Introduction to Architecture Development Method', viewed 11th August 2016,
www.opengroup.org/architecture/togaf9-doc/arch/index.html

Oracle – 'The Oracle Enterprise Architecture Framework', October 2009, pp.1-13
http://www.oracle.com/technetwork/articles/entarch/oea-framework-133702.pdf

Orica Group Standard– 'Physical Security', (Draft) June 2016, pp.1-5

Parliament of Australia – 'Private Review of Agency Security Arrangements', 13 October 2003, viewed 12th August 2016
http://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Former_Committees/pjcaad/securityreview/securityreviewindex

Parliament of Australia – 'Private Review of Agency Security Arrangements – Personnel Security', 13 October 2003, pp.11-26
http://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Former_Committees/pjcaad/securityreview/securityreviewindex

C.M Pereira, P. Sousa – 'A Method to Define an Enterprise Architecture using the Zachman Framework', SAC, 2004, pp.1-2

T. Rains – 'Cloud Security Controls Series: Encrypting Data at Rest', Sept 10 2015, viewed 15th August 2016
https://blogs.microsoft.com/microsoftsecure/2015/09/10/cloud-security-controls-series-encrypting-data-at-rest/

J.W Ross, P. Weill, D.C Robertson – 'Enterprise Architecture as Strategy – Creating a Foundation for Business Execution', Harvard Business School Press, 2006, pp.1-10

M. Rossi – 'Is Computer Data "Tangible Property" or Subject to "Physical Loss or Damage"? – Part 1', IRMI International Risk Management Institution, August 2001, viewed 15th August 2016
https://www.irmi.com/articles/expert-commentary/is-computer-data-tangible-property-or-subject-to-physical-loss-or-damage-part-1

D. Shackleton – 'Regulations and Standards: Where Encryption Applies', SAN Institute InfoSec Reading Room, November 2007, p.4, viewed 16th August 2016
https://www.sans.org/reading-room/whitepapers/analyst/regulations-standards-encryption-applies-34675

STA Group – 'What is Business Architecture', viewed 9th August 2016
http://www.stagrp.com/architecture/business-architecture/what-is-business-architecture/

Stilgherrian – 'Encrypting Data at Rest is vital, but it's just not happening', ZDNet, 18 June 2015
http://www.zdnet.com/article/encrypting-data-at-rest-is-vital-but-its-just-not-happening/

J. Talbot, M. Jakeman – 'Security Risk Management Body of Knowledge', Wiley, July 2009, pp.1-472

Talk Tech to Me, viewed 15th August 2016
http://www.gfi.com/blog/protecting-data-with-encryption/

Tech Republic, viewed 14th August 2016
http://www.techrepublic.com/article/encryption-is-front-line-defense-for-data-at-rest/

Tech Target, viewed 16th August 2016
http://searchstorage.techtarget.com/tip/Securing-data-at-rest-vs-data-in-transit

U.K Government – 'Government Security Classifications – April 2014', Cabinet Office, V.1 October 2013, pp.1-35, viewed 17th August 2016
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/251480/Government-Security-Classifications-April-2014.pdf

US Dept of Commerce – 'Managing Information Security Risk', NIST Special Publication 800-39, March 2011, pp.1-88, viewed 17th August 2016
http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf

US Department of Defense – 'Manual', Number 5200.01, Vol.2, February 24, 2012, pp.1-117
http://www.dtic.mil/whs/directives/corres/pdf/520001_vol2.pdf

USGS – US Geological Survey Manual – Physical Security Handbook, August 2005, viewed 10th August 2016
https://www2.usgs.gov/usgs-manual/handbook/hb/440-2-h/440-2-h.html

J. Versperman – 'Introduction to Securing Data in Transit', 24th February 2002, p.6, viewed 16th August 2016, http://www.tldp.org/REF/INTRO/SecuringData-INTRO.pdf

G. Versteeg, H. Bouwman – 'Business Architecture: A new paradigm to relate business strategy to ICT', Inf Syst Front, 2006, Vol.8, pp.91-102

Waytek, viewed 16th August 2016
http://waytek.com/q-what-meant-terms-data-rest-and-data-motion

R. Whittle – 'Enterprise Business Architecture', January 2013, p.20, viewed 10th August 2016
www.enterprisebusinessarchiteture.com

Wikipedia – 'Business Architecture'
https://en.wikipedia.org/wiki/Business_architecture

Wikipedia – 'ISO/IEC 27000'
https://en.wikipedia.org/wiki/ISO/IEC_27000

Wikipedia – 'Physical Security'
https://en.wikipedia.org/wiki/Physical_security