Sub 013

ISACA®
Trust in, and value from, information systems
Perth Chapter

11 September 2015

Public Accounts Committee
Legislative Assembly
Parliament House
PERTH WA 6000

Via email: lapac@parliament.wa.gov.au

Subject: **ISACA's submission in response to the inquiry into Information and Communications Technology (ICT) Procurement and Contract Management**

To: The Chairman

Thank you for the opportunity to respond to the Inquiry into Information and Communications Technology (**ICT**) Procurement and Contract Management. ISACA is extremely supportive of your inquiry and your objectives.

ICT is a critical business service for managing information which is a key resource for all public sector organisations. There are significant pressures for both business and ICT to be more effective, efficient, innovative and demonstrate value for money in a fast-paced and ever-changing environment. This is compounded by the need to maintain or surpass current levels of transparency, accountability and conformance (with standards, frameworks, policy and legislation). Managing ICT in the current environment is complicated and challenging and the road ahead only appears to be uphill. The success of any knowledge-based organisation relies on the ability of the senior executive to govern ICT. By govern we mean evaluate, direct and monitor.

The objective of governance is to create value. Value creation is generated by: benefits realisation, risk minimisation and resource optimisation. One of the largest challenges to generating value is unclear lines of responsibility. Ideally public sector organisations should be clearly and purposefully structured to address the policy functions that they are required to execute. In reality the situation is often far from ideal. The impacts of unclear lines of responsibility and reporting is often that those charged with governing the organisation are presented with, and required to make decisions on, information that is highly technical and does not clearly relate to their area of expertise.

ISACA applauds the appointment of the state's first Government Chief Information Officer (**GCIO**). This is an important step to improving the way services are delivered in WA. Strong and effective leadership lays the foundation for accountability, change, and diligent stewardship. Likewise, giving that GCIO the right tools to be successful is also important. Placing ICT governance at the pinnacle of government, from which can stem embedded systems of risk and control, is the type of better practice ISACA has been championing through its frameworks and credentials.

ISACA's core message is about generating trust and value with the business, which must be done through effective planning for, and acquisition and alignment of, technology with the right professionals

Should the committee wish to discuss this response or any of ISACA's frameworks or certifications please contact me.

Respectfully submitted,

Mike Nisbet
President – ISACA Perth Chapter
president@isaca-perth.org.au

ABOUT ISACA

With more than 140,000 constituents in 180 countries (and more than 3,000 in Australia), ISACA members have developed, implemented, managed and assessed security controls in leading critical infrastructure organisations and governments on a global basis. ISACA is a leading global provider of knowledge, certifications, community, advocacy and education on information and systems assurance and security, enterprise governance and management of IT and IT-related risk and compliance.

ISACA also continually updates COBIT®, which helps IT professionals and enterprise leaders deliver their governance and management of IT responsibilities, particularly in the areas of security, risk and assurance to deliver value to the enterprise. COBIT is used within many governmental departments and regulatory bodies around the world. ISACA also participates in the development of international security and governance standards through its global liaison status with the International Organisation of Standardisation (ISO).

Founded in 1969 ISACA is an independent non-profit organisation which hosts international conferences, develops frameworks, publishes the ISACA® Journal, and develops international IS auditing and control standards, which help its constituents ensure trust in, and value from, information systems. It also advances and attests IT skills and knowledge through the globally respected Certified Information Systems Auditor® (CISA®), Certified Information Security Manager® (CISM®), Certified in the Governance of Enterprise IT® (CGEIT®) and Certified in Risk and Information Systems Control™ (CRISC™) designations.

Pertinent to ISACA is a significant global shortage of skilled cybersecurity professionals. The Enterprise Strategy Group reports that 83 percent of enterprises lack the necessary skills to protect their IT assets. ISACA makes a firm commitment to address the skills crisis and do for cybersecurity professionals what we have done (and will continue to do) for audit, control and governance professionals over the past 45 years and deliver the frameworks, certifications and knowledge sharing for professionals to continue to make an impact.

SUBMISSION OBJECTIVES

Our understanding is it the Public Accounts Committee (**Committee**) has recognised potential for improvement in the governance of and management of ICT and is exploring possible solutions by concentrating on identifying models of better practice which can be incorporated into the public sector.

Consequently, in this submission ISACA will illustrate effective frameworks and practices which could be pragmatically adopted by the WA Government in order to address identified issues and enable sustainable change for future ICT investments and delivery ensuring that value is realised.

BACKGROUND

Defining success for ICT delivery is the moving away from just recognising on-time, on-budget delivery and towards recognising the business value from those ICT investments. This major shift comes from an understanding that ICT exists to enable business change and support the delivery of services. In the case of government this is the delivery of services to citizens and the creation of public value. This shift is fundamental and requires changes in the dynamic of governance and management of ICT. ICT should not govern itself, but rather must be oversighted, monitored and guided by the business and delivery areas it serves. This shift has been long recognised by ISACA and is reflected in the thinking and approaches outlined in COBIT 5.

Investing in a successful Governance of Enterprise IT (**GEIT**) system can result in a myriad of benefits. These often include: lower costs, greater control, and overall increased efficiency and effectiveness. The primary purpose of using a GEIT system, however, is to deliver value to stakeholders. If that value cannot be delivered, or if its delivery is not well understood, the resources consumed to implement GEIT are wasted. Consequently, using a proven GEIT framework to reduce the risks of implementation is prudent. ISACA has many guidelines on pragmatic approaches to implementing and measuring the impact and ongoing effectiveness of GEIT systems that perform, and add value.

QUESTION AND ANSWER MAP

This table is provided as a map of available resources, in this document, for the Committee to explore.

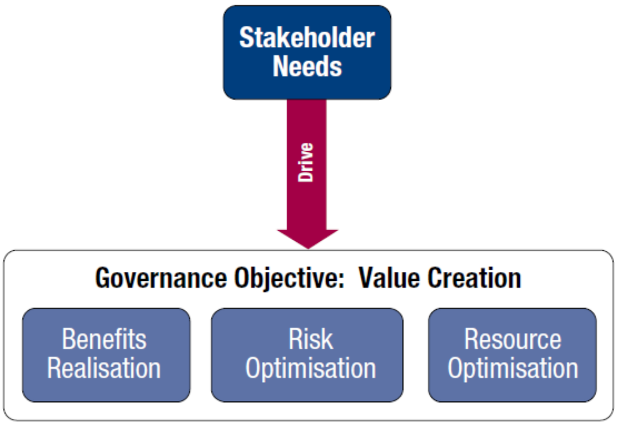
QUESTIONS	ANSWER SUMMARY	ADDITIONAL RESOURCES
1. What are the common problems witnessed in public sector delivery of IT goods and services?	A failure to realise benefits and value, and a loss of trust. The root cause is most often from insufficient or unsuitable governance.	APPENDIX B: ISACA IN ACTION
2. What elements represent best practice in IT delivery? IT delivery includes: Project Planning, Contract Management, Project Management, Project Status Reporting and Reviews.	ISACA's COBIT framework takes a more holistic view – reaching beyond just ICT delivery to focus on business value.	COBIT 5: A Business Framework for the Governance and Management of Enterprise IT
3. How do we best measure or define success in IT delivery?	ICT exists to deliver business value. It is through effective governance that these stakeholder needs are articulated.	COBIT 5: A Business Framework for the Governance and Management of Enterprise IT
4. What are the latest developments (domestic and/or international), in the area of government IT systems?	There is an emerging understanding and awareness that the Governance of Enterprise IT is fundamental to value realisation. Increasingly the importance of digital leadership and people capability to deliver on Enterprise goals is being revisited and promoted.	COBIT 5: A Business Framework for the Governance and Management of Enterprise IT and APPENDIX A: CERTIFICATION AND PROFESSIONAL DEVELOPMENT
5. What jurisdictions (domestic and/or international) have adopted the latest developments in government IT systems that have demonstrably reduced the cost, and improved the delivery, of government services?	ISACA has global case studies from the implementation of our world class international frameworks. Case studies are available in Appendix B.	APPENDIX B: ISACA IN ACTION
5.1 Could such systems be incorporated into Western Australia?	Examples of successful implementations are provided in Appendix B. This includes E-health governance. Our independent study demonstrates the link between better E-health governance, better health care strategic alignment and better health care outcomes.	APPENDIX B: ISACA IN ACTION
5.2 If so, what factors need to be taken into account to ensure successful implementation?	Please find guidance and advice on our website, through our chapter volunteers and from our professionally certified members.	APPENDIX B: ISACA IN ACTION

COBIT 5: A BUSINESS FRAMEWORK FOR THE GOVERNANCE AND MANAGEMENT OF ENTERPRISE IT

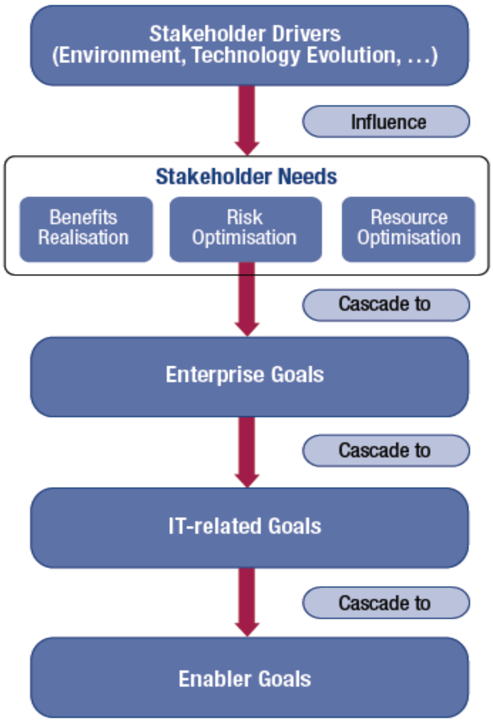
COBIT 5 provides a comprehensive framework that assists enterprises in achieving their objectives for the governance and management of enterprise ICT. Simply stated, it helps enterprises create optimal value from ICT by maintaining a balance between realising benefits and optimising risk levels and resource use. COBIT 5 enables ICT to be governed and managed in a holistic manner for the entire enterprise, taking in the full end-to-end business and ICT functional areas of responsibility, considering the ICT-related interests of internal and external stakeholders. COBIT 5 is generic and useful for enterprises of all sizes, whether commercial, not-for-profit or in the public sector.

The specific components of COBIT 5 which relate to the focus of the committee are the management processes of aligning, planning and organising (**APO**) ICT systems. These processes do not operate alone and are integrated into and supported by the holistic approach COBIT 5 takes to the governance and management of ICT. This section introduces the fundamental principles, and the following sections on the process reference model and assurance framework provide an overview of how COBIT 5 operates.

COBIT5’s first and foremost principle is meeting stakeholder needs. The main purpose of GEIT is to achieve strategic alignment of information and related technology in order to meet stakeholder needs and create value. Simply stated, it helps enterprises create optimal value from IT by maintaining a balance between realising benefits and optimising risk levels and resource use. ICT procurement and contract management is an activity which must be governed and managed effectively in order for stakeholder needs to be met.



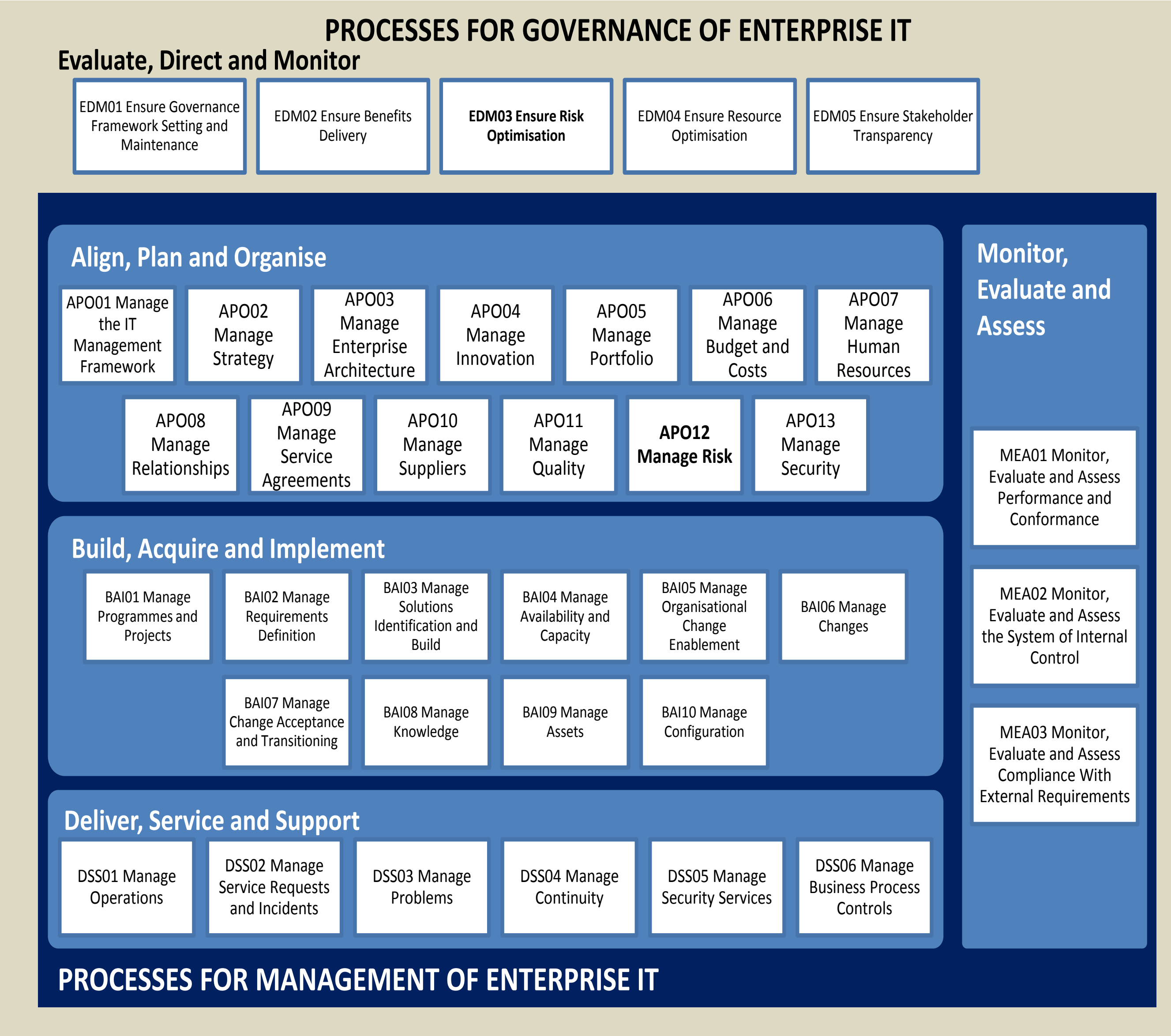
As noted above one of the largest challenges to generating value is unclear lines of responsibility. Ideally public sector organisations should be clearly and purposefully structured to address the policy functions that they are required to execute as stakeholder needs have to be transformed into an enterprise's actionable strategy for them to be successful. The COBIT 5 goals cascade is a model for translating stakeholder needs into specific, actionable and customised enterprise goals, ICT-related goals and enabler goals. This translation allows setting specific goals at every level and in every area of the enterprise in support of the overall goals and stakeholder requirements, and thus effectively supports alignment between enterprise needs and ICT solutions and services.



COBIT 5 PROCESS REFERENCE MODEL

COBIT 5 has a process reference model, which defines and describes in detail a number of governance and management processes. This includes processes for governing Enterprise ICT which should be distinct and separate from processes for managing ICT. This framework represents all of the processes found in an enterprise relating to ICT activities, and therefore provides a common reference model which can be understood by both operational ICT and business managers. Of course each enterprise must define its own process set, taking into account their specific situation.

Incorporating an operational model and a common language for all parts of the enterprise involved in IT activities is another critical step towards good governance. It also provides a framework for measuring and monitoring ICT performance, providing ICT assurance, communicating with service providers, and integrating best management practices. ISACA has all the tools, training and knowledge sharing to deliver these.



PROCESSES FOR GOVERNANCE OF ENTERPRISE IT

Evaluate, Direct and Monitor

- EDM01 Ensure Governance Framework Setting and Maintenance
- EDM02 Ensure Benefits Delivery
- **EDM03 Ensure Risk Optimisation**
- EDM04 Ensure Resource Optimisation
- EDM05 Ensure Stakeholder Transparency

Align, Plan and Organise

- APO01 Manage the IT Management Framework
- APO02 Manage Strategy
- APO03 Manage Enterprise Architecture
- APO04 Manage Innovation
- APO05 Manage Portfolio
- APO06 Manage Budget and Costs
- APO07 Manage Human Resources
- APO08 Manage Relationships
- APO09 Manage Service Agreements
- APO10 Manage Suppliers
- APO11 Manage Quality
- **APO12 Manage Risk**
- APO13 Manage Security

Build, Acquire and Implement

- BAI01 Manage Programmes and Projects
- BAI02 Manage Requirements Definition
- BAI03 Manage Solutions Identification and Build
- BAI04 Manage Availability and Capacity
- BAI05 Manage Organisational Change Enablement
- BAI06 Manage Changes
- BAI07 Manage Change Acceptance and Transitioning
- BAI08 Manage Knowledge
- BAI09 Manage Assets
- BAI10 Manage Configuration

Deliver, Service and Support

- DSS01 Manage Operations
- DSS02 Manage Service Requests and Incidents
- DSS03 Manage Problems
- DSS04 Manage Continuity
- DSS05 Manage Security Services
- DSS06 Manage Business Process Controls

Monitor, Evaluate and Assess

- MEA01 Monitor, Evaluate and Assess Performance and Conformance
- MEA02 Monitor, Evaluate and Assess the System of Internal Control
- MEA03 Monitor, Evaluate and Assess Compliance With External Requirements

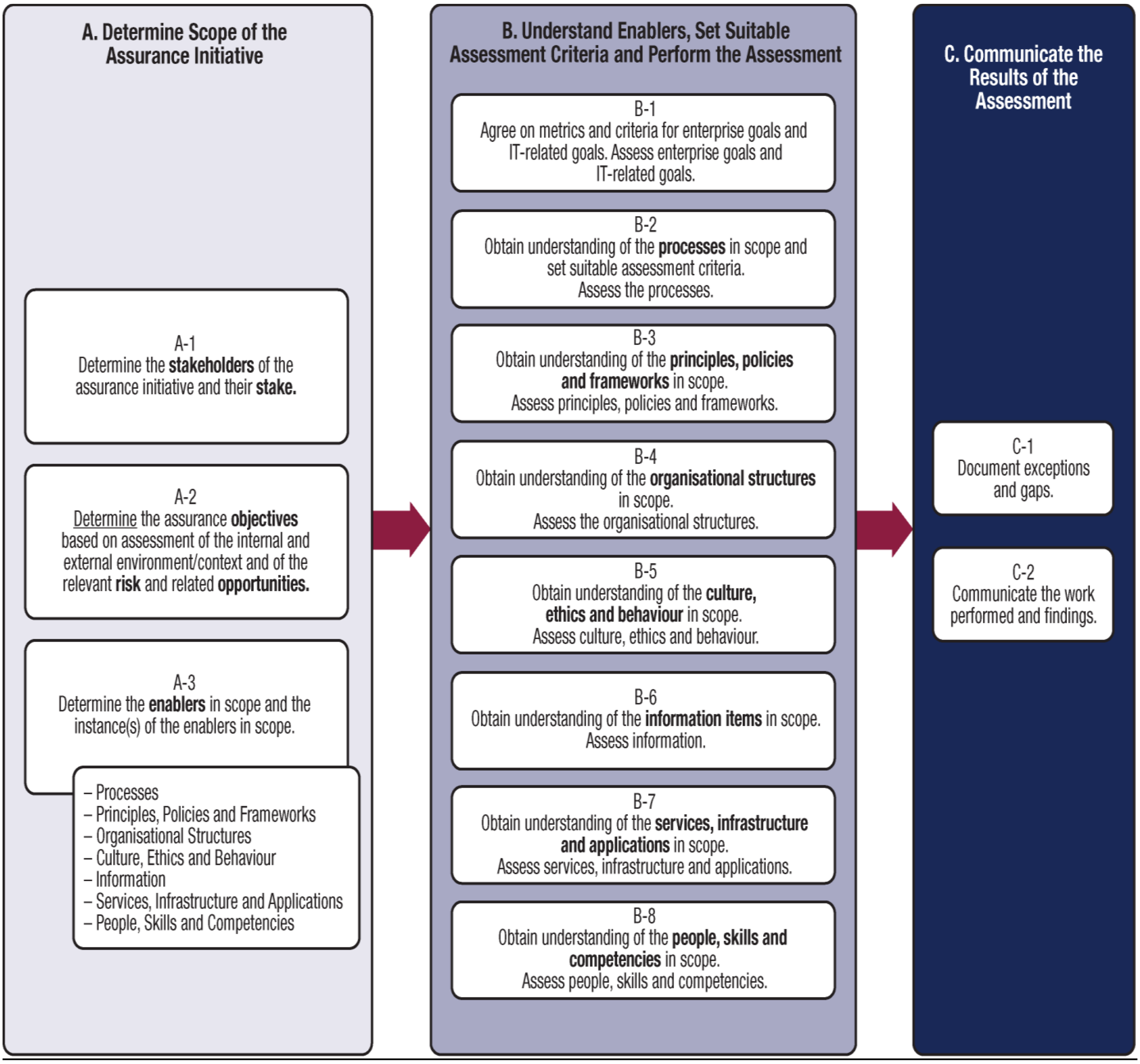
PROCESSES FOR MANAGEMENT OF ENTERPRISE IT

COBIT 5 ASSURANCE FRAMEWORK

A key component of value creation and ensuring the successful delivery of ICT is assurance. The main drivers for assurance include:

- Providing interested parties substantiated opinions on governance and management of enterprise IT according to assurance objectives
- Defining assurance objectives in line with enterprise objectives, thus maximising the value of assurance initiatives
- Satisfying regulatory or contractual requirements for enterprises to provide assurance over their IT arrangements

To these ends COBIT 5 and its related assurance guide allow enterprises to form a view of the extent to which the value objectives of the enterprise—delivering benefits while optimising risk and resource use—are achieved. The diagram below shows the generic assurance approach.



A. Determine Scope of the Assurance Initiative

A-1
Determine the **stakeholders** of the assurance initiative and their **stake.**

A-2
Determine the assurance **objectives** based on assessment of the internal and external environment/context and of the relevant **risk** and related **opportunities.**

A-3
Determine the **enablers** in scope and the instance(s) of the enablers in scope.

– Processes
– Principles, Policies and Frameworks
– Organisational Structures
– Culture, Ethics and Behaviour
– Information
– Services, Infrastructure and Applications
– People, Skills and Competencies

B. Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment

B-1
Agree on metrics and criteria for enterprise goals and IT-related goals. Assess enterprise goals and IT-related goals.

B-2
Obtain understanding of the **processes** in scope and set suitable assessment criteria.
Assess the processes.

B-3
Obtain understanding of the **principles, policies and frameworks** in scope.
Assess principles, policies and frameworks.

B-4
Obtain understanding of the **organisational structures** in scope.
Assess the organisational structures.

B-5
Obtain understanding of the **culture, ethics and behaviour** in scope.
Assess culture, ethics and behaviour.

B-6
Obtain understanding of the **information items** in scope.
Assess information.

B-7
Obtain understanding of the **services, infrastructure and applications** in scope.
Assess services, infrastructure and applications.

B-8
Obtain understanding of the **people, skills and competencies** in scope.
Assess people, skills and competencies.

C. Communicate the Results of the Assessment

C-1
Document exceptions and gaps.

C-2
Communicate the work performed and findings.

SUMMARY

ISACA Perth sees this inquiry as a key step in the journey by the WA Parliament to strengthen trust in and value from public sector information systems. We would like to offer our support using our global network of highly experienced and certified volunteers–backed by professional staff–in an ongoing capacity to assist the Committee with continuing their journey to deliver value to Western Australian citizens.

The aim of this submission is to highlight the strength of ISACA's frameworks, the experience and knowledge of the Organisation and the continuing drive to empower ICT professionals to deliver the best for their organisations. If you have any questions or would like to discuss this submission or any other ISACA document or activity please contact me

Mike Nisbet, ACCA, CISA
President – ISACA Perth Chapter

Mike Nisbet.

APPENDIX A: CERTIFICATION AND PROFESSIONAL DEVELOPMENT

ISACA's four professional certifications are outlined as follows.

CRISC (pronounced "see-risk") is the most current and rigorous assessment available to evaluate the risk management proficiency of IT professionals or other employees within an enterprise or financial institution. Introduced in 2010, the CRISC certification is for IT and business professionals — including risk and compliance professionals, business analysts and project managers — who identify and manage risk through the development, implementation and maintenance of appropriate information systems (IS) controls. More than 18,000 professionals have earned the CRISC designation since inception. CRISC retention rates are more than 93 percent.

CRISC won the 2013 Best Professional Certification Award from SC Magazine. CRISC is the highest earning certification on the 2015 IT Skills and Salary Survey.

The uniquely management-focused CISM certification (pronounced "sis-im") promotes international security practices and recognises the individual who manages, designs, oversees and assesses an enterprise's information security. Sought after by experienced information security managers, the CISM certification is a ground breaking credential earned by more than 26,000 professionals since 2002. The management focused CISM is the globally accepted achievement for individuals, who develop, build and manage enterprise information security programs. CISM retention rates are more than 95 percent.

CISM is the second highest earning certification on the 2015 IT Skills and Salary Survey.

The CISA designation (pronounced "sigh-sa") is a globally recognised certification for IS audit control, assurance and security professionals. Being CISA certified showcase audit experience, skills and knowledge, and demonstrates capabilities to assess vulnerabilities, report on compliance and institute controls within the enterprise. Since 1978, the CISA certification has been a globally accepted standard of achievement among information systems (IS) audit, control and security professionals. More than 114,000 professionals have earned the CISA designation since inception. CISA retention rates consistently remain more than 90 percent.

The CISA certification is sought by those who audit, control, monitor and assess an enterprise's information technology and business systems. CISAs are recognised internationally as professionals with the assurance knowledge, skills, experience and credibility to leverage standards, manage vulnerabilities, ensure compliance, offer solutions, institute controls and deliver value to the enterprise. CISA is often a mandatory qualification for employment as an information systems auditor.

CISA is the fifth highest earning certification on the 2015 IT Skills and Salary Survey.

Introduced in 2007, the CGEIT credential (pronounced "see-get") is for professionals who manage, provide advisory and/or assurance services related to, and/or otherwise support the governance of an enterprise's IT. CGEIT certified professionals deliver on the focus areas of IT governance and approach it holistically, enhancing value to enterprises. More than 6,000 professionals have earned the CGEIT credential to date. CGEIT retention is more than 95 percent.

APPENDIX B: ISACA IN ACTION

This table has references to external websites. Printed copies are available upon request.

ISACA EXAMPLE	DESCRIPTION	RELATED QUESTION	LINK
Strategic Alignment and eHealth Governance	Research demonstrating the link between governance and strategic alignment in eHealth systems	4. What are the latest developments in the area of government IT systems?	http://www.isaca.org/knowledge-center/research/documents/monitoring-progress-on-ehealth-strategic-alignment-and-ehealth-governance_mis_eng_0115.pdf
Value Governance – Police Case Study	A case study relevant to illustrating the importance and relevance of COBIT 5 and Val IT for a state agency	4. What are the latest developments in the area of government ICT systems?	http://www.isaca.org/Knowledge-Center/cobit/Pages/Val-IT-Case-Study-Value-Governance-Police-Case-Study.aspx
COBIT Recognition Articles	The COBIT website which has key success stories from across the Globe	5. What jurisdictions (domestic and/or international) have adopted the latest developments in government IT systems	http://www.isaca.org/COBIT/focus/Pages/archive.aspx
COBIT 5 – A Framework for the Governance and Management of Enterprise IT	ISACA's Governance framework	5.2 What factors need to be taken into account to ensure successful implementation?	http://www.isaca.org/cobit/pages/cobit-5-framework-product-page.aspx A printed copy will also be provided
VAL IT 2.0 – The Val IT Framework 2.0 – Enterprise Value: Governance of IT Investments	Complementary to COBIT 5 in detailing the specifics of practices of Value Governance and Management	5.2 What factors need to be taken into account to ensure successful implementation?	http://www.isaca.org/Knowledge-Center/Val-IT-IT-Value-Delivery-/Pages/Val-IT-Publications.aspx
Vendor Management using COBIT 5	Practical steps for managing vendors in IT	2.0 What elements represent best practice in IT delivery?	A printed copy will be provided