26 March 2015

Ms. Michelle Price, Senior Adviser Cyber Policy Branch
The Department of Prime Minister and Cabinet

Via email: michelle.price@pmc.gov.au

RE: Cybersecurity 2015 Review

Dear Ms. Price,

Thank you for the opportunity to respond to the Department of Prime Minister and Cabinet’s Cybersecurity 2015 review. ISACA applauds and is extremely supportive of this review and wishes you every success.

Globally, cybersecurity is an emerging priority to address increases in cybercrime and, in some instances, cyberwarfare. Factors contributing to the need for improved cybersecurity include: ubiquitous broadband, IT-centric business and society and social stratification of IT skills. To address cybercrime, many governments and institutions launched cybersecurity initiatives, ranging from guidance, through standardisation, to comprehensive legislation and regulation.

Worldwide, there 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 has made a firm commitment to proactively address the skills crisis and deliver for cybersecurity professionals what it has accomplished (and will continue to do) for audit, control and governance professionals over the past 45 years.

Upon considering the defined objectives of the Cybersecurity 2015 review from the Department of Prime Minister and Cabinet, ISACA believes it can render assistance by:
• Addressing Australia’s cybersecurity skill needs and supporting the Australian community members in their understanding of those needs (Objective 5)
• Looking to the future of the Internet (and other emerging business trends and technology), assessing risk and providing advice, training and research about how to make Australia’s online systems more resilient to attack (Objective 1)

ISACA believes the assistance in the above points would enable the Australian government to better protect its own networks and the information it holds on behalf of the Australian people, including critical infrastructure (Objective 3). It would also provide ongoing advice and guidance on technological and international developments in cyberspace (Objective 4) to support the government’s ability to maintain its cybersecurity policies and strategies.

We would like to acknowledge the efforts of the Australian government for the implementation of the Public Governance, Performance and Accountability (PGPA) Act 2013. Placing governance at the pinnacle of every public entity, from which stem embedded systems of risk and control, is the type of better practice ISACA champions through its frameworks and credentials.
Our core message is about generating trust and value with the business through the considered application of technology. Governance frameworks such as the PGPA present the foundation for ICT governance, risk and control. ISACA continues to monitor the progress of Australia’s Public Management Reform Agenda (PMRA) with interest, and would be delighted to assist where appropriate.

ISACA believes the Cybersecurity review is another crucial step in the journey by the Australian Government to strengthen trust in and value from public and private sector information systems. ISACA stands ready to offer its global network of highly experienced and certified volunteers - backed by professional staff – in an ongoing capacity to assist the Australian Government with continuing its journey.

An example of the potential knowledge development for advice and guidance from ISACA is the ongoing European Cybersecurity Implementation Series. Given a reasonable amount of time, ISACA has the capability to create highly targeted and professional guidance materials. We believe that ongoing collaboration and support is essential to building cybersecurity capability and would appreciate the opportunity to respond to any requests from the Australian Government for guidance. This could be accomplished directly with the Government or, as we have achieved previously, by providing practical guidance to small and medium enterprises that struggle to rise to the complex challenge of cybersecurity.

ISACA also remains interested in working with Australian universities and training providers in delivering cybersecurity training, certifications, and research and development. We look forward to meeting with you on 30 March to discuss the challenges and potential opportunities.

Appendix A contains ISACA’s responses to the questions posed in the Cybersecurity Review. Also provided is a recommended mapping of our certifications, and our CSX offerings, against the roles outlined in Australia’s Information Security Manual (ISM). The infographics illustrating the position of cybersecurity in an organisation’s governance structure are sourced from ISACA’s COBIT 5 framework.

Appendix B presents three lines of assistance the Australian Government could find beneficial when addressing cybersecurity: Certification and Training, Academic Outreach and Resources, and Knowledge and Content. There is also an introduction to COBIT 5.

Respectfully submitted,

Robert E Stroud, CGEIT, CRISC, International President

Matthew S Loeb, CAE, Chief Executive Officer

Tony G Hayes, CGEIT, AFCHSE, CHE, FACS, FCPA, FIIA, Immediate Past President

ISACA (www.isaca.org)
About ISACA
With more than 140,000 constituents in 180 countries (and more than 4,000 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 security, assurance, enterprise governance and management of IT and IT-related risk and compliance.

The new ISACA Cybersecurity Nexus (CSX) is a comprehensive set of career progression resources for all levels of cybersecurity professionals. ISACA also continually updates COBIT®, which helps IT professionals and enterprise leaders fulfill their governance and management of IT responsibilities, particularly in the areas of security, risk, assurance and control to deliver value to the enterprise. COBIT is used, adopted and recommended 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 Organization of Standardization (ISO).

Founded in 1969, the non-profit, independent ISACA hosts international conferences, 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.
Appendix A: Answers and Australian Information Security Manual Mapping

Answers

Q. Do current roles and responsibilities for cybersecurity in Australia need clarifying and/or updating?

Australia would benefit from the requirement of training and certification for the roles the Government relies upon for cybersecurity. In Appendix A we have provided a recommended mapping of the roles from the Information Security Manual to certifications offered by ISACA. Our requirement for ongoing professional education ensures our certification holders remain current.

Q. What is the key challenge Australia faces in cybersecurity? What is the key challenge being faced by your organisation in cybersecurity?

The key challenge Australia faces in cybersecurity is a skills crisis. There is a significant global shortage of skilled cybersecurity professionals. Recognising this, ISACA has established the Cyber Security Nexus (CSX) to provide cybersecurity resources for professionals at every level of their cybersecurity careers. CSX offers a central place where cybersecurity professionals can find the information they need related to training, certification, guidance, career development and community.

Q. How can the Australian economy leverage cybersecurity to improve our comparative advantage?

Well governed and well managed information and technology can produce new and enhanced opportunities and sustainable competitive advantages. Cybersecurity itself is an enterprise-goal to optimise risk to meet stakeholder needs of trust and value. Proactive steps leveraging cybersecurity can help minimise the risk of loss of citizen data and classified/sensitive information. ISACA’s COBIT5, and other guidance, supports value creation from cybersecurity investments.

Q. What are key government and/or industry-led strategies that would have the greatest impact on addressing Australia’s cybersecurity skills gap?

When there has been sufficient training and awareness at senior levels of an organisation the relevant human capital issues are identified and addressed. ISACA prepares documents and resources to provide the top level of the organisation with the relevant questions and concepts so they can govern and secure ICT effectively.

Q. How can governments and peak bodies best support the Australian economy to view investment in cybersecurity as an enabler of economic prosperity?

By ensuring that the senior levels of organisations are equipped with sufficient levels of knowledge and appreciation for ICT governance, they will - and do - then apply reasonable and appropriate measures to provide cybersecurity assurances to satisfy their stakeholders’ needs.

Q. How can we achieve the cultural shift needed for the Australian community to view cybersecurity as a key aspect of participating in cyberspace?

Risk perception is influenced by knowledge and experience. Training and awareness are the fundamental keys to unlocking this cultural shift. ISACA’s experience has been that when governments place requirements for certain roles to have professional qualifications or certifications – for security, governance, risk or audit – these positions are seen as leadership roles which are looked upon for guidance and as role-models.
## ISACA Certification Mapping to the Australian Information Security Manual (ISM)

<table>
<thead>
<tr>
<th>ISM Role</th>
<th>ISM Requirement</th>
<th>ISM Control</th>
<th>ISACA Certifications</th>
<th>What are the benefits of these Certifications?</th>
</tr>
</thead>
</table>
| CISO     | The role of the **CISO** is based on industry best practice and has been introduced to ensure that information security is managed at the senior executive level. The **CISO** is typically responsible for:  
- Facilitating communication between security personnel, ICT personnel and business personnel to ensure alignment of business and security objectives  
- Providing strategic–level guidance for the agency security program  
- Ensuring compliance with national policy, standards, regulations and legislation | Agencies must appoint a senior executive, commonly referred to as the **CISO**, who is responsible for coordinating communication between security and business functions as well as overseeing the application of controls and security risk management processes. | **CGEIT** is considered by many companies and governmental agencies as a prerequisite for employees involved with enterprise IT governance.  
- The employee has the knowledge and experience necessary to support and advance the IT governance of an enterprise.  
- The employee maintains ongoing professional development necessary for successful on-the-job performance.  
- The enterprise’s IT and business systems operate with greater efficiencies and optimum effectiveness resulting in greater trust in, and value from, information systems.  
**CRISC**s bring additional professionalism to any organisation by demonstrating a quantifiable standard of knowledge, pursuing continuing education, and adhering to a standard of ethical conduct established by ISACA. **CRISC** employees:  
- Build greater understanding about the impact of IT risk and how it relates to the overall organisation  
- Assure development of more effective plans to mitigate risk  
- Establish a common perspective and language about IT risk that can set the standard for the enterprise |
<table>
<thead>
<tr>
<th>ISM Role</th>
<th>ISM Requirement</th>
<th>ISM Control</th>
<th>ISACA Certifications</th>
<th>What are the benefits of these Certifications?</th>
</tr>
</thead>
<tbody>
<tr>
<td>ITSM</td>
<td>ITSMs are generally considered information security experts and are typically responsible for:</td>
<td>Agencies must appoint at least one executive, commonly referred to as an ITSM, to manage the day-to-day operations of information security within the agency, in line with the strategic directions provided by the CISO or equivalent.</td>
<td>CRISCs bring additional professionalism to any organisation by demonstrating a quantifiable standard of knowledge, pursuing continuing education, and adhering to a standard of ethical conduct established by ISACA. CRISC employees:</td>
<td>Enterprises and government agencies increasingly recognise, require and expect their IS and IT professionals to hold CISM certification. CISM employees:</td>
</tr>
<tr>
<td></td>
<td>• Managing the implementation of security measures</td>
<td></td>
<td>• Build greater understanding about the impact of IT risk and how it relates to the overall organisation</td>
<td>• Identify critical issues and customise company-specific practices to support the governance of information and related technologies</td>
</tr>
<tr>
<td></td>
<td>• Monitoring information security for systems and responding to any cybersecurity incidents</td>
<td></td>
<td>• Assure development of more effective plans to mitigate risk</td>
<td>• Bring credibility to the enterprise for which they are employed</td>
</tr>
<tr>
<td></td>
<td>• Identifying and incorporating appropriate security measures in the development of ICT projects and the information security program</td>
<td></td>
<td>• Establish a common perspective and language about IT risk that can set the standard for the enterprise</td>
<td>• Take a comprehensive view of information systems security management and their relationship to organisational success</td>
</tr>
<tr>
<td></td>
<td>• Establishing contracts and service-level agreements on behalf of the CISO, or equivalent</td>
<td></td>
<td></td>
<td>• Demonstrate to enterprise customers their commitment to compliance, security and integrity; ultimately contributing to the attraction and retention of customers</td>
</tr>
<tr>
<td></td>
<td>• Assisting the CISO or equivalent to develop security budget projections and resource allocations</td>
<td></td>
<td></td>
<td>• Ensure that there is improved alignment between the organisation’s information security program and its broader goals and objectives</td>
</tr>
<tr>
<td></td>
<td>• Providing regular reports on cybersecurity incidents and other areas of particular concern</td>
<td></td>
<td></td>
<td>• Provide the enterprise with a certification for Information security management that is recognised by multinational clients and enterprises, lending credibility to the enterprise</td>
</tr>
<tr>
<td></td>
<td>• Helping system owners to understand and respond to reported audit failures</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ISM Role</td>
<td>ISM Requirement</td>
<td>ISM Control</td>
<td>ISACA Certifications</td>
<td>What are the benefits of these Certifications?</td>
</tr>
<tr>
<td>----------</td>
<td>----------------</td>
<td>-------------</td>
<td>----------------------</td>
<td>-----------------------------------------------</td>
</tr>
</tbody>
</table>
| ITSA     | An ITSM, when fulfilling the designation of ITSA, still maintains full responsibilities for their role as an ITSM in addition to ITSA responsibilities. An ITSA traditionally has the added responsibility of coordinating other ITSMs to ensure that security measures and efforts are undertaken in a coordinated manner. | Agencies must designate an ITSM as the ITSA, to have responsibility for information technology security management across the agency. | CRISCs bring additional professionalism to any organisation by demonstrating a quantifiable standard of knowledge, pursuing continuing education, and adhering to a standard of ethical conduct established by ISACA. CRISC employees:  
- Build greater understanding about the impact of IT risk and how it relates to the overall organisation  
- Assure development of more effective plans to mitigate risk  
- Establish a common perspective and language about IT risk that can set the standard for the enterprise | Enterprises and government agencies increasingly recognise, require and expect their IS and IT professionals to hold CISM certification. CISM employees:  
- Identify critical issues and customise company-specific practices to support the governance of information and related technologies  
- Bring credibility to the enterprise for which they are employed  
- Take a comprehensive view of information systems security management and their relationship to organisational success  
- Demonstrate to enterprise customers their commitment to compliance, security and integrity; ultimately contributing to the attraction and retention of customers  
- Ensure that there is improved alignment between the organisation’s information security program and its broader goals and objectives  
- Provide the enterprise with a certification for Information security management that is recognised by multinational clients and enterprises, lending credibility to the enterprise |
<table>
<thead>
<tr>
<th>ISM Role</th>
<th>ISM Requirement</th>
<th>ISM Control</th>
<th>ISACA Certifications</th>
<th>What are the benefits of these Certifications?</th>
</tr>
</thead>
</table>
| ITSO     | Appointing a person whose responsibility is to ensure the technical security of systems is essential to manage compliance and non-compliance with the controls in this manual. The main responsibility of ITSOs is the implementation and monitoring of technical security measures for systems. Other responsibilities often include:  
- Conducting vulnerability assessments and taking actions to mitigate threats and remediate vulnerabilities  
- Working with ITSMs to respond to cybersecurity incidents  
- Assisting ITSMs with technical remediation activities required as a result of audits  
- Assisting in the selection of security measures to achieve the strategies selected by ITSMs with respect to disaster recovery  
- Raising awareness of information security issues with system owners and personnel | Agencies must appoint at least one expert, commonly referred to as an ITSO, in administering and configuring a broad range of systems as well as analysing and reporting on information security issues. |  | The Cybersecurity Fundamentals Certificate exam tests for foundational knowledge in cybersecurity across five key areas:  
- Cybersecurity concepts  
- Cybersecurity architecture principles  
- Cybersecurity of networks, systems, applications and data  
- The security implications of the adoption of the emerging technologies  
- Incident responses | A new cybersecurity certification is in development and will be performance-based for those who seek to verify their capabilities for ensuring enterprise cybersecurity. The job practice analysis is complete, and plans call for the online exam to be available in mid-2015. |
Appendix B: ISACA Certification, Academic Outreach, Knowledge and COBIT

1. Certification and Training

A key question raised by the review is how to address Australia’s cybersecurity skill needs. ISACA certifications are globally accepted and recognized as leaders in the cybersecurity field. They combine the achievement of passing an exam with credit for required work and educational experience, as well as ongoing professional education, thereby providing credibility for their professional expertise. Certification proves to employers that professionals have what it takes to add value to their enterprise. In fact, many organizations and governmental agencies around the world require or recommend ISACA’s certifications.

ISACA currently offers four certifications in the domains of Risk, Security Management, IT Audit and Governance. In addition, ISACA recently established a new program to focus on cybersecurity - Cybersecurity Nexus (CSX).

As mentioned in Appendix A, CSX provides cybersecurity resources for professionals at every level of their cybersecurity careers. We use the term “Nexus” because CSX represents the one central place where cybersecurity professionals can find the information they need related to training, certification, guidance, career development and community.
ISACA prides itself on providing continuous professional education to its members. Education opportunities exist through our *Journal; Knowledge Center; Conferences; Local chapter events; Online Training* and *COBIT Online*.

ISACA’s professional certifications, CISA, CISM, CGEIT and CRISC are officially compliant with ISO/IEC 17024:2003, General Requirements for Bodies Operating Certification Systems of Persons. ISACA is proud to be recognised with this international standard of performance, as accredited by the American National Standards Institute (ANSI).

**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 27,000 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 practitioners and professionals. Being CISA certified showcases 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 115,000 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.

2. Academic Outreach

Tertiary and vocational education is a key enabler in supporting the raising of cybersecurity awareness and skills across the Australian community. ISACA supports faculty, students and student organisations at colleges and universities around the world who teach and study disciplines related to ISACA’s mission. To encourage participation, ISACA offers:
- Student and academic advocate memberships
- ISACA Model Curricula\(^1\) for IS Audit and Control and Information Security Management
- Educational materials for professors and teachers include the following classroom materials, which were constructed using the advice of a global network of academics and practitioners:

---

\(^1\) ISACA’s Academic Relations Committee manages the curriculum as living programs and welcomes all comments and input.
Academic research is the foundation of many of the breakthroughs and new theories supporting the information security, IT assurance and governance professional space. ISACA is pleased to support and promote academic research projects and actively encourages participation in them.

3. Knowledge and Content

To prepare for the future of technologies and provide resilience for cyberrisk, ISACA actively promotes research that results in the development of products for IT governance, control, assurance, risk and security. ISACA research also informs information technology management, users and professionals about IS controls and the critical role they play in their organisations.

ISACA maintains an Emerging Business and Technology Committee to:

- Identify, monitor and evaluate evolving business and technology trends that impact the use of technology by organisations
- Create (and facilitate the creation of) new knowledge and guidance based on how those trends change the business landscape
- Support ISACA’s ability to utilise this knowledge to facilitate the objectives of its volunteer bodies, foster adoption of ISACA frameworks, and expand the value of ISACA knowledge and certifications
- Support ISACA’s ability to exploit this knowledge.

Following are a selection of white papers and research deliverables relevant to the cybersecurity review:

- Cybersecurity Fundamentals Certificate and Online Course
- Implementing the NIST Cybersecurity Framework
- Transforming Cybersecurity
- Responding to Targeted Cyberattacks
- Cybersecurity: What the Board of Directors Needs to Ask
- Overview of Digital Forensics
- Internet of Things: Risk and Value Considerations
- Advanced Persistent Threat Awareness Study Results
- Advanced Persistent Threats: How To Manage The Risk To Your Business
- Cloud Governance: Questions Boards of Directors Need to Ask
- Vendor Management Using COBIT 5
- Industrial Control System (ICS) Challenges (scheduled availability end of the second quarter 2015)

ISACA invites the Australian Government to access these documents and to remain in contact with us as we keep our white papers and research publications up to date with emerging trends and risk. Additionally, cybersecurity guidance for small and medium enterprises is in the very early stages of development.
**COBIT 5 Value Proposition**

IT is a critical business service for managing the unified communication of information. Information is a key resource for all public sector organisations. There are significant pressures for the Governance of Enterprise IT (GEIT) to be more effective, efficient, innovative and demonstrate value for money in a fast-paced and ever-changing environment, while maintaining or surpassing current levels of transparency, accountability and conformance (with standards, frameworks, policy and legislation). Governing and managing IT 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 IT (evaluate, direct and monitor) from a business perspective that reflects the central role of information and technology in generating value for the enterprise. Such an approach is what COBIT 5 represents.

There are three elements to generating value: benefits realisation, and risk 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 impact 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.

If roles and responsibilities for IT are more clearly defined, the senior executive can focus on setting direction by devolving management activities to their managers and holding them accountable for planning, building and running the technical aspects. The senior executives governing the organisation can then focus their time on ensuring that IT assets create value for stakeholders.

Questions for which answers are needed include:
- How do I get value from the use of IT? And are end users satisfied with the quality of the IT service?
- Am I running an efficient and resilient IT operation?
- Is the information I am processing well secured?
- What critical business processes are dependent on IT, and what are the requirements of these business processes?

While these questions are deceptively simple, getting their answers wrong, or not being able to answer them at all, presents significant risk to any organisation. They cover the multitude of questions that stakeholders (including the public) demand of all public sector organisations. To answer these questions across an entire enterprise, senior executives generally expect to employ many different frameworks, specialists, consultants and receive many (often technical) reports in return.

The many different frameworks, specialists and consultants only ever answer a sub-set of these questions. For example: P3M3, ISO/IEC27001, ISO 31000, Treasury and Finance guidelines and many more are highly specialised and answer specific questions. Each of these sources of guidance require executives and management to wade through multiple reports,
and potentially implement measures that either overlap, or worse, leave gaps across the organisation and its providers. COBIT 5 provides a single comprehensive framework that assists enterprises to achieve their goals and deliver value through effective governance and management of enterprise IT.

The COBIT 5 approach helps Senior Executives:
- Meet stakeholder needs
- Cover the enterprise end-to-end
- Apply a single integrated framework
- Enable a holistic approach
- Separate governance from management

**COBIT 5 helps you get more value from both your information and your technology.** Information is a key resource for all enterprises. From the time that information is created to the moment that it is destroyed, technology plays a significant role across the enterprise. By approaching GEIT from a business perspective, COBIT 5 helps you maximise the trust in, and value from, your organisation’s information and technology.

**COBIT 5 is the only business framework for the governance and management of enterprise IT.** COBIT’s globally accepted principles, practices, analytical tools and models are designed for business executives – not just IT leaders. What’s more, COBIT 5 can be used in any industry and by organisations of all sizes, including public sector government bodies.

**COBIT 5 is relevant and necessary.** COBIT 5 helps you address the needs of stakeholders across the enterprise and clarify goals for more effective decision making. It provides a systematic approach and common vocabulary for tackling many of today’s most challenging aspects of meeting enterprise performance goals and maximising the value of corporate information.

**COBIT 5 helps bring order to complex standards, regulations and frameworks.** No other framework has the breadth of COBIT 5. COBIT provides an end-to-end framework that integrates other approaches and standards and addresses all areas of the enterprise.

**COBIT 5 represents the collective wisdom of global experts.** COBIT 5 delivers thought leadership and guidance from business and IT leaders worldwide. It is the product of a global task force and development team from ISACA, a non-profit, independent association of more than 140,000 governance, security, risk and assurance professionals in more than 180 countries. The most significant revolution in the framework’s 16-year history, COBIT 5 was reviewed by more than 95 experts worldwide. Hundreds more contributed, ensuring it reflects the power of many minds coming together.

IT is complicated.

Governance of IT doesn’t have to be.
COBIT 5’s first and foremost principle is meeting stakeholder needs. These needs are met by creating value. Value is created through benefits being realised, and risk and resources being optimised. Cybersecurity risk management, including the risk management of cyber assets, is one essential component of what ISACA sees as being the fundamental equation for generating value.
There is a duality to risk; it can either be a positive outcome of value creation and/or value preservation, or alternatively it can be a negative outcome of value destruction or of failure to gain. Cybersecurity risk is usually thought of as “adverse IT-related events destroying value;” however, ISACA prefers to consider the matter holistically. Well governed and well managed information and technology can produce new and enhanced opportunities and sustainable competitive advantages.

The Duality of Risk

Cybersecurity impacts organisations from the back-room to the board room. The back-room must be steered by senior leadership to satisfy stakeholder needs. Senior leaders need to proactively anticipate stakeholder requests for reasonable cybersecurity assurances. Cybersecurity is an enterprise-goal to optimise risk to meet stakeholder needs of trust and value.

The Cascade of COBIT 5 Principles to Action