

The Infosec competencies 2005

Including core competencies for:

- Government practitioner
- Accreditor
- Comsec manager
- Comsec practitioner

Contents

	Page No
Introduction	3
Using the competencies matrix	3
Government Core Competency Profile	3
Specialist Core Competency Profiles	4
A Government Core Competency example	5
How to develop your personal target competencies	6
The Infosec competencies	7
Competency Cluster 1 – Infosec expertise	7
1.1 Acquiring and maintaining knowledge	8
1.2 Implementation of Government baseline requirements and compliance with relevant legislation	10
1.3 Using technical security measures	12
Competency Cluster 2 – Business management	14
2.1 Business focus	15
2.2 Planning	17
2.3 Delivering results	19
2.4 Managing resources and value for money (VFM)	21
2.5 Dealing with change	23
Competency Cluster 3 – Dealing with people	25
3.1 Infosec teamwork	26
3.2 Communicating and influencing Infosec issues	28

Introduction

The Infosec Training Paths & Competencies (ITPC) scheme has developed these Infosec competencies to describe the UK Government minimum standards of competency expected of its Infosec practitioners, notably departmental IT security officers (ITSOs). This document also provides core competency profiles (CCPs) for others involved in government Infosec activities, namely system accreditors, Comsec managers and Comsec practitioners. The CCPs are mandated for those seeking to achieve the ITPC Certificate of Infosec Competency in their chosen area of responsibility.

The competencies were developed by a review panel of departmental ITSOs and representatives of the UK security authorities. The matrix is subject to review by a similar body and by the ITSO Forum before formal endorsement from Cabinet Office.

The competency clusters in this matrix are expressed generically, to allow the competencies to be integrated with others already used in organisational appraisal schemes. Only skills directly relevant to Infosec activities have been included: these may be combined with others from local competency frameworks to complete the competency profile for a specific post. Organisations should add further detail or illustrative examples to individual competency descriptions in order to provide an accurate and measurable description of each competency required locally.

To discuss any issues relating to the Infosec competencies, including their use in organisational appraisal schemes, contact the ITPC Secretariat. For further information on the ITPC Certificate visit the ITPC website or contact the ITPC Secretariat. The Infosec competencies matrix is an updateable standard which relies on input from the community it serves to maintain its currency and relevance. If you have comments or suggestions on its content or application, please contact the ITPC Secretariat.

The ITPC Scheme
Cabinet Office CSIA
6th floor
Stockley House
130 Wilton Road
London SW1V 1LQ

itpc@cabinet-office.x.gsi.gov.uk
www.seriousaboutinfosec.gov.uk

Using the competencies matrix

The matrix provides generic competencies from which individual organisations, and candidates for the ITPC Certificate of Infosec Competency, are encouraged to develop their own, measurable, target competencies. In certificate submissions, these target competencies are used by ITPC scheme examiners to assess dissertations.

Target competencies must of course be relevant to the role and achievable; but they must also reflect faithfully the intrinsic meaning of the relevant source core competency.

Government Core Competency Profile (CCP)

The Government CCP is primarily a recognised baseline requirement for departmental ITSOs. As such, it represents the minimum level of competency an ITSO should achieve. Candidates for the ITPC Government Practitioner Certificate are required to adopt this CCP.

The competencies are, necessarily, expressed in general terms. ITPC Certificate candidates are required to consider each competency in turn and add to it a specific illustration of how it applies to their role – one that can be observed or measured in some way. For example: if the stated competency stipulates 'understanding the vulnerabilities of an operating system', the target competency should specify which operating system the candidate uses.

Many certificate candidates will operate at a level below that of the ITSO; the Government CCP allows for scoping, by definition of 'sphere of influence', in order to specify commensurate levels of competency within defined areas of activity.

Where competencies describe influencing 'across the organisation' and similar, ITPC Certificate candidates should replace that term with a description of their sphere of activity. This may be a system and its users, the team they manage, or those they advise on Infosec issues – be they within their own department or company, or a part of it – even across a community of organisations.

ITPC Certificate candidates are allowed flexibility in the way they use the Government CCP: generally, they should develop target competencies from within the CCP closest to the role they fulfil. In exceptional cases, a particular competency within a profile may appear too demanding or outside the scope of their role. In such cases, they may select a lower competency description from the relevant competency cluster. However, this should only be considered in exceptional cases; both the candidate and their supporter must submit to the scheme their case for doing so.

Some candidates may wish to show their competency rises above the baseline requirement described in the Government CCP; in this case, higher competency descriptions within the respective clusters may be selected.

Specialist Core Competency Profiles (CCPs)

Specialist CCPs have been developed for accreditors, Comsec managers and Comsec practitioners. Candidates for the ITPC Certificates in these specialist areas are required to adopt the relevant CCP: competency is achieved only by meeting or exceeding all relevant descriptions in the CCP entries in the matrix.

The competencies are, necessarily, expressed in general terms. ITPC Certificate candidates are required to consider each competency in turn and add to it a specific illustration of how it applies to their role – one that can be observed or measured in some way. For example: if the stated competency stipulates 'understanding the vulnerabilities of an operating system', the target competency should specify which operating system the candidate uses.

Where competencies describe influencing 'across the organisation' and similar, ITPC Certificate candidates should replace that term with a description of their sphere of activity. This may be a system and its users, the team they manage, or those they advise on Infosec issues – be they within their own department or company, or a part of it – even across a community of organisations.

If you are an ITPC candidate and are not sure how to develop your target competencies, contact the ITPC Secretariat – they are there to help.

A Government Core Competency example

The Government CCP is within a framework of progressively more demanding competencies. These recognise the different levels of Infosec expertise required in different roles, from those who are required simply to address Infosec requirements in their work to those whose work demands higher ITSO or specialist expertise.

As already stated, candidates for the ITPC Government Practitioner Certificate are required to adopt the Government CCP or higher competency descriptions, unless exceptionally agreed with the scheme.

1.1 Acquiring and Maintaining Knowledge

		Government Core Competency	
Maintains sufficient expertise to meet their individual security responsibilities.	Maintains specialist Infosec expertise in own work area and understands related protective security issues; can advise and coach others in own specialism.	Maintains currency of knowledge of Government baseline measures and recommended practices. Maintains broad practical security expertise extending beyond own work area; maintains awareness of Infosec activities.	Maintains sufficient expertise in relevant Infosec trends to inform strategic policy development; has skills and knowledge to enable them to represent their organisation as an expert in the field.
This column generally relates to those who simply address Infosec in their work e.g. complying with security operating procedures	This column generally relates to those with e.g. team responsibilities who manage, rather than develop, Infosec policy	This column generally relates to those with strategic security responsibilities. Often, this describes the baseline for Government ITSOs	This column generally relates to those with higher ITSO or specialist expertise. May also reflect working across business boundaries

The heading shows that this column describes the Government CCP baseline

How to develop your personal target competencies

Target competencies are developed from the components of a CCP, by adding details to each description. These details should ensure that:

- the scope of the candidate’s activities are represented;
- the descriptions include local examples of each relevant item; and
- the target competency is measurable – in other words, an outcome by which competency can be assessed.

Here is an example, for a system security manager, using competency 1.1 of the Government Practitioner CCP. The process is the same for other CCPs. For more help, see our How To... Create Target Competencies fact sheet on our web site.

STEP 1. Review the competencies in your selected CCP with your supporter. Identify how they relate to your role.

1.1 Acquiring and Maintaining Knowledge

		Government Core Competency	
Maintains sufficient expertise to meet their individual security responsibilities.	Maintains specialist Infosec expertise in own work area and understands related protective security issues; can advise and coach others in own specialism.	Maintains currency of knowledge of Government baseline measures and recommended practices.	Maintains sufficient expertise in relevant Infosec trends to inform strategic policy development; has skills and knowledge to enable them to represent their organisation as an expert in the field.

Government Core Competency

Maintains currency of knowledge of Government baseline measures and recommended practices. Maintains broad practical security expertise extending beyond own work area; maintains awareness of Infosec implications of business activities.

STEP 2. Consider how each description can be amended to reflect your work: include local standards, business-specific and system-specific information wherever possible.

1.1 Acquiring and Maintaining Knowledge

		Government Core Competency	
Maintains sufficient expertise to meet their individual security responsibilities.	Maintains specialist Infosec expertise in own work area and understands related protective security issues; can advise and coach others in own specialism.	Maintains currency of knowledge of Government baseline measures and recommended practices. Maintains broad practical security expertise extending beyond own work area; maintains awareness of Infosec implications of business activities.	Maintains sufficient expertise in relevant Infosec trends to inform strategic policy development; has skills and knowledge to enable them to represent their organisation as an expert in the field.

Government Core Competency

Maintains currency of knowledge of Government baseline measures and recommended practices. Maintains broad practical security expertise extending beyond own work area; maintains awareness of Infosec implications of business activities.

- *What other standards do I need to use?*
- *What other expertise do I need beyond my own work area?*
- *What are my organisation’s business activities?*

STEP 3. Add relevant and measurable details to the core competency, to complete your own target competency. Number the target competency to match the core competency, for future reference in your dissertation.

Target Competency 1.1 – Government Core Competency

Maintains currency of knowledge of Government baseline measures, recommended practices *and departmental security policy relevant to the secure operation of the system.*

Maintains broad practical security expertise extending beyond *the system, to include GSI Community Security Policy requirements.*

Maintains awareness of Infosec implications of *departmental activities including its electronic services to the citizen and its 2003–2004 project to initiate sharing of information with contracted service providers.*

The Infosec competencies

The Infosec competencies are divided into three clusters:

- Infosec expertise;
- Business management; and
- Dealing with people.

For non-specialist roles, different levels of competence are provided for different roles. Those seeking to achieve the ITPC Government Practitioner Certificate of Infosec Competency should use those specified in the column headed 'Government Core Competency' or higher levels, unless lower-level competencies have exceptionally been agreed with the ITPC Scheme Secretariat.

The competencies are arranged in numeric order on the following pages. Competencies for ITSOs and general infosec roles are given on one page. Those for specialist roles, i.e. accreditor, Comsec manager and Comsec practitioner, are given on the following page.

Competency cluster 1 – Infosec expertise

Acquiring and maintaining knowledge and skills relevant to implementing effective information security

Core Competencies:

- 1.1 Acquiring and maintaining knowledge
- 1.2 Implementation of Government baseline requirements and compliance with relevant legislation
- 1.3 Using technical security measures

1.1 Acquiring and maintaining knowledge

How to use this table is illustrated on p.5

		Government Core Competency	
Maintains sufficient expertise to meet their individual security responsibilities.	Maintains specialist Infosec expertise in own work area and understands related protective security issues; can advise and coach others in own specialism.	Maintains currency of knowledge of Government baseline measures and recommended practices. Maintains broad practical security expertise extending beyond own work area; maintains awareness of Infosec implications of business activities.	Maintains sufficient expertise in relevant Infosec trends to inform strategic policy development; has skills and knowledge to enable them to represent their organisation as an expert in the field.

1.1 Acquiring and maintaining knowledge

Core competencies for specialist Infosec roles

Accreditor Core Competency	Comsec Practitioner Core Competency	Comsec Manager Core Competency
<p>Understands and remains current with the scope and content of Government baseline policy requirements (as laid out in the Manual of Protective Security, its supporting documents and their local derivatives).</p> <p>Maintains currency with relevant aspects of legislation and industry standards. For example: the pivotal role of risk assessment, and the business need and implementation requirements for Business Continuity.</p>	<p>Identifies and undertakes relevant professional development to ensure they maintain currency with the policy contained in Government Infosec Standard 4 and related UK government and local/departmental directives and recommended practice.</p> <p>Takes note of relevant CINRAS and related outputs (e.g. UNIRAS) and maintains sufficient knowledge to oversee or otherwise manage the operation of crypto and other Comsec technical equipments.</p>	<p>Identifies and undertakes relevant professional development to ensure they maintain a strategic understanding of the policy contained in Government Infosec Standard 4 and related UK Government and local/departmental directives and recommended practice.</p> <p>Takes note of relevant CINRAS and related outputs (e.g. UNIRAS) and maintains sufficient knowledge generally to oversee or otherwise ensure communications security across the organisation.</p> <p>Maintains a working knowledge of related Information Assurance issues beyond their own Comsec discipline.</p>

1.2 Implementation of Government baseline requirements and compliance with relevant legislation

How to use this table is illustrated on p.5

			Government Core Competency
Complies with Government and organisational policy, and legislation relevant to their individual responsibilities – chiefly for example through observance of security operating procedures.	Fulfils a role in ensuring that their own area of responsibility complies with national and organisational baseline requirements and relevant legislation, for example by conducting technical risk assessments and developing and maintaining system security documentation.	Ensures all relevant organisational, national and legislative requirements are considered within business area and ensures system security policies correctly assess and manage the risk to the system, by monitoring and periodically reviewing security provision. Consults with central organisational authorities to ensure security solutions comply with Government Infosec policy.	Ensures security policy addresses organisational, national and legislative requirements consistently and remains commensurate with the risk across the organisation. Formally accredits or ensures the accreditation of systems. Interfaces with national security, cryptographic, formal evaluation and/or professional bodies as required, to implement Government Infosec policy.

1.2 Implementation of Government baseline requirements and compliance with relevant legislation

Core competencies for specialist Infosec roles

Accreditor Core Competency	Comsec Practitioner Core Competency	Comsec Manager Core Competency
<p>Assesses that the boundaries and scope of the target of accreditation are valid.</p> <p>Ensures that the risk has been assessed accurately and that the security strategy meets relevant Government baseline policy (and best practice recommendations where appropriate).</p> <p>Develops risk management strategies to meet business requirements.</p> <p>Ensures the security strategy provides appropriate ISO/IEC 17799 and legislative compliance.</p> <p>Provides Accreditation Aftercare to ensure the continuing validity of accredited status.</p>	<p>Takes practical measures to ensure that secure communications systems within own area of responsibility comply with Government national, legislative and organisational baseline requirements, including Government Infosec Standard 4 and other relevant policies and directives.</p>	<p>Takes strategic measures to ensure compliance with Government Comsec standards (including specifically Government Infosec Standard 4) and procedures on behalf of their organisation. Also, ensures compliance with legislative and organisational requirements.</p> <p>Ensures that the implementation of policy meets Government baseline and other appropriate requirements.</p>

1.3 Using technical security measures

How to use this table is illustrated on p.5

		Government Core Competency	
Uses hardware and software securely, for example as required by Security Operating Procedures.	Correctly specifies, configures or operates relevant technical protective measures; may manage operational aspects of security in their own area of responsibility.	Has broad knowledge of technical security issues, understands the principal security issues of IT platforms and applications; develops requirements for technical Infosec measures within own business area.	Has in-depth expertise in software and hardware systems, platforms and applications relevant to own area of responsibility. Contributes to technical aspects of Infosec policy for the organisation and advises security strategists on technical aspects of implementing secure systems.

1.3 Using technical security measures

Core competencies for specialist Infosec roles

Accreditor Core Competency	Comsec Practitioner Core Competency	Comsec Manager Core Competency
<p>Understands the principles of technical security in applications.</p> <p>Assesses the appropriate applications and their technical security measures.</p> <p>Ensures that technical security measures integrate with other security measures to meet the assessed security requirement.</p> <p>Identifies the threats and vulnerabilities to information and communications systems assets and the likelihood of impacts on the Confidentiality, Integrity and Availability of those assets; recognises where these require technical expertise and seeks ways to utilise such support.</p>	<p>Understands the technical aspects of implementing crypto equipment and key material, and principal Comsec management issues of accounting, account management and transfer of key material.</p> <p>Recognises ways in which Comsec can be integrated effectively with other security measures.</p>	<p>Recognises ways in which technical aspects of Comsec can be integrated effectively with other security measures and consistently identifies which of these are the most effective.</p>

Competency cluster 2 – Business management

Integrating Infosec requirements with those of the business of the organisation;
managing Infosec within the individual's sphere of activity

Core Competencies:

- 2.1 Business focus
- 2.2 Planning
- 2.3 Delivering results
- 2.4 Managing resources and value for money (VFM)
- 2.5 Dealing with change

2.1 Business focus

How to use this table is illustrated on p.5

		Government Core Competency	
Applies relevant Infosec policy reliably in own area of individual responsibility, and appreciates the business drivers for security.	Takes the initiative in satisfying the Infosec need in own area of responsibility, while meeting business requirements in a secure manner.	Understands business aims and objectives, and establishes, develops or advises on Infosec policy (and/or local working standards) that manage the risk to protect and enable these. Provides guidance on security in consultation with central organisational authorities and promotes business benefits of security awareness and Information Security.	Identifies strategic security goals for the organisation and influences corporate security policies and plans which recognise the developing needs of the business; provides advice and guidance on implementing security across the organisation. Encourages reciprocal links with strategic functions within the organisation, and with external bodies, whose activities may impact on security.

2.1 Business focus

Core competencies for specialist Infosec roles

Accreditor Core Competency	Comsec Practitioner Core Competency	Comsec Manager Core Competency
<p>Ensures key players in the organisation are engaged to understand both the business and the security requirements.</p> <p>Works in partnership with relevant personnel to assess and implement security strategies which are commensurate with the risk and the business requirement and meet national baseline policy where relevant.</p> <p>Maintains accountable documentation of all their decisions and communications relevant to the accreditation process.</p>	<p>Takes the initiative in satisfying the Comsec requirement in own area of responsibility, while meeting business needs in a secure manner.</p> <p>Provides guidance on Comsec in consultation with relevant organisational and/or Government authorities. Maintains accountable documentation of all their actions and communications relevant to the implementation, and protection, of Comsec and crypto elements.</p> <p>Promotes the business benefits of Comsec to the organisation through briefings and other representations.</p>	<p>Establishes, develops or advises on Comsec policy (and/or local working standards) that manage the risk to enable Business aims and objectives.</p> <p>Provides guidance to decision-makers on Comsec policy and practice, in consultation with relevant national authorities.</p> <p>Develops and maintains organisational Comsec policy and procedures to safeguard business requirements.</p> <p>Promotes the business benefits of Comsec, including general Comsec Awareness, to the organisation through briefings and other representations.</p>

2.2 Planning

How to use this table is illustrated on p.5

		Government Core Competency	
Actively maintains an awareness of how Government and organisational Infosec policy requirements impact on own work, and applies lessons learned from training and experience in a practical way in own work.	Develops the application of Infosec measures in a way that supports the organisation's strategic business direction and initiatives in own area of work.	Contributes to and advises on the strategic application of Infosec policy. Ensures that the application of Infosec policy supports business needs. Examples may include appropriate business continuity plans and contingency measures.	Proactively leads the process of developing Infosec policy; takes major decisions affecting the direction of Infosec policy across a significant sphere of activity e.g. an organisation or a community of related bodies.

2.2 Planning

Core competencies for specialist Infosec roles

Accreditor Core Competency	Comsec Practitioner Core Competency	Comsec Manager Core Competency
<p>Plans accreditation activities to integrate with project schedules and business needs.</p> <p>Prioritises activities and resources according to the importance of accreditation relative to the business need.</p> <p>Remains focused on relevant accreditation and security issues.</p> <p>Makes timely and objective decisions based on best available evidence and sound analysis.</p>	<p>Produces and/or maintains plans for routine and exceptional contingency and Business Continuity, including establishing and exercising emergency action plans in accordance with Government and/or organisational policy.</p> <p>Produces and/or maintains plans for acquiring, maintaining and disposing of crypto equipment and material.</p>	<p>Produces or approves plans for the general management of communications security; ensures that emergency action plans for the protection of Comsec systems are established in accordance with Government and/or organisational policy.</p> <p>Ensures that procurement and development projects give adequate consideration to Comsec requirements.</p>

2.3 Delivering results

How to use this table is illustrated on p.5

		Government Core Competency	
Carries out Infosec responsibilities to meet locally agreed security standards within own duties, including for example compliance with routine security procedures and incident reporting mechanisms.	Delivers Infosec coverage to the standard required in own sphere of activity; takes whole or partial responsibility for ensuring staff within this area meet their security responsibilities.	Influences, contributes to or advises on the strategic direction taken on Infosec within own sphere of activity; utilises appropriate mechanisms to achieve organisational security goals. Examples include incident reporting procedures and training programs to review security and maintain awareness.	Takes formal responsibility for the achievement of cost-effective and Risk Management-based Infosec across the organisation; ensures that new Infosec initiatives are implemented effectively and utilises strategic mechanisms such as incident reporting procedures and training to review security and maintain awareness.

2.3 Delivering results

Core competencies for specialist Infosec roles

Accreditor Core Competency	Comsec Practitioner Core Competency	Comsec Manager Core Competency
<p>Provides clear and accountable documented recommendations, independent of external pressures.</p> <p>Is resilient, is not put off by setbacks and displays drive and energy to achieve results.</p> <p>Ensures work is planned, prioritised and delivered to meet requirements.</p> <p>Understands appropriate management techniques and uses them when applicable.</p> <p>Considers options to accept, transfer, avoid or limit risks, and ensures security mechanisms and countermeasures are managed to keep delivery of security objectives on track.</p>	<p>Delivers effectively and on a timely basis, through Comsec application, communications systems with adequate and appropriate levels of confidentiality, integrity and availability. Takes whole or partial responsibility for ensuring that relevant staff meet their Comsec responsibilities.</p> <p>Utilises appropriate Comsec mechanisms and procedures to achieve organisational security goals.</p> <p>Provides clear and accountable documentation as required throughout the crypto material and equipment lifecycle, for items under their control.</p>	<p>Consistently delivers to the Business, communications systems that are commensurate with risk to the assets they protect and that address the Business operational need.</p> <p>Utilises appropriate strategic Comsec mechanisms and procedures to achieve organisational security goals.</p> <p>Provides clear and accountable documentation as required.</p>

2.4 Managing resources and value for money (VFM)

How to use this table is illustrated on p.5

	Government Core Competency		
Seeks VFM in operating Infosec measures within own work.	Seeks VFM in the application of Infosec measures within own sphere of activity – for example, by judging the relative cost-effectiveness of technical and non-technical countermeasures in protective security strategies.	Influences the cost-effective use of resources and ensures security policies across an organisation facilitate VFM in the application of Infosec strategic and technical measures, relative to the assessed risk.	Plans and achieves VFM in devising Infosec policies and plans across an organisation or across organisational boundaries, for example by utilising existing security measures in protective security strategies for new systems.

2.4 Managing resources and value for money (VFM)

Core competencies for specialist Infosec roles

Accreditor Core Competency	Comsec Practitioner Core Competency	Comsec Manager Core Competency
<p>Evaluates the cost-effectiveness of proposed security strategies, individual measures and/or business transactions.</p> <p>Provides an accreditation service to the Business in an effective, efficient and economic manner. Identifies where existing protective security measures can be utilised in system security strategies, and balances technical with non-technical measures.</p> <p>Negotiates and appropriately distributes resources to meet accreditation objectives.</p> <p>May monitor and evaluate security suppliers' performance and ensure adherence to contract terms.</p> <p>Implements cost effective risk management, utilising identified security strategies and balancing technical and non-technical measures.</p>	<p>Manages crypto material and equipment to support business requirements. Within their area of work, seeks cost-effective use of Comsec resources and ensures these facilitate VFM, commensurate with the risk and aligned with Government Infosec Standard 4 and related local/departmental baseline policies.</p>	<p>Plans and achieves VFM in devising Comsec policies and plans across the organisation or across organisational boundaries – for example, by utilising existing security measures in protective security strategies for new systems.</p> <p>Where appropriate, establishes and manages material and human Comsec resources.</p> <p>Ensures these strategies remain commensurate with the risk and aligned with Government Infosec Standard 4 and related local organisational baseline policies.</p>

2.5 Dealing with change

How to use this table is illustrated on p.5

			Government Core Competency
Responds positively to changing local security requirements and accepts the need for Infosec.	Promotes security awareness and contributes constructively to changes in security procedures in own area.	Promotes and initiates change, with due regard for Infosec implications, and motivates others to co-operate and contribute towards change in security procedures in own area, to meet its business requirements.	Promotes and initiates change in the protective security requirement through compliance monitoring, reviewing the security requirement and reacting in a timely and proportionate way to developments in the threat, technology and its uses, and business practices.

2.5 Dealing with change

Core competencies for specialist Infosec roles

Accreditor Core Competency	Comsec Practitioner Core Competency	Comsec Manager Core Competency
<p>Advises and negotiates to counter opposition to change, in order to protect business and security objectives.</p> <p>Is open to new ways of working and adapts flexibly to change.</p> <p>Is prepared to initiate and implement change and encourages a positive attitude in others.</p> <p>Ensures accredited status is maintained against change in technology, policy or standards, the risk and business operations and thereby contributes, via advice and negotiation, to business continuity protection.</p> <p>Ensures they are consulted where configuration management, change control or other system management operations may affect the security status of the subject of accreditation.</p> <p>Ensures that changes to IT or communications systems risks and conflicting priorities are successfully managed throughout the lifecycle of the system.</p>	<p>Demonstrates a practical and flexible approach in adapting to changing requirements for Comsec provision. Responds constructively to changes in Comsec policy and procedures that affect items under their control.</p> <p>Reacts promptly and provides timely management of Comsec as business or operational requirements dictate.</p>	<p>Demonstrates a practical and flexible approach in adapting to changing legislation and national requirements for Comsec provision. Promotes and initiates changes in organisational Comsec policy and procedures to address developments in national policy and changes in the local (usually, organisational) security environment.</p> <p>Reacts promptly and provides timely management of Comsec as business or operational requirements dictate.</p>

Competency cluster 3 – Dealing with people

Working with others, internally/externally, to establish and maintain appropriate levels of security within the organisation and its contractors

Core Competencies:

- 3.1 Infosec teamwork
- 3.2 Communicating and influencing Infosec issues

3.1 Infosec teamwork

How to use this table is illustrated on p.5

		Government Core Competency	
Participates effectively in supporting local Infosec standards as part of a team – for example, in shared security procedures; is proactive in identifying and reporting security issues encountered in own work.	Leads or materially participates within own work area in compliance with Infosec standards and baseline requirements; may monitor and specify local security standards and/or procedures.	Leads Infosec teams or organisational functions that have complex security aims or face significant challenges to achieving and maintaining Infosec. Negotiates and may maintain control or oversight of Infosec in outsourced and contracted projects.	Negotiates and/or facilitates the achievement and maintenance of Infosec baseline requirements and standards across organisational boundaries with differing business cultures. For example, may perform or oversee accreditation of systems across a diverse community.

3.1 Infosec teamwork

Core competencies for specialist Infosec roles

Accreditor Core Competency	Comsec Practitioner Core Competency	Comsec Manager Core Competency
<p>Negotiates and/or facilitates the achievement and maintenance of Infosec baseline requirements and standards across organisational boundaries with differing business cultures, where appropriate.</p> <p>Works effectively with other relevant security staff, project teams or Accreditation Panels to ensure the security of systems for which they have particular responsibility is commensurate with the risk to those systems.</p> <p>Knows when to seek help from and involve others, listens and takes account of diverse needs and objectives.</p> <p>Resolves conflicts effectively and gives confidence to others.</p>	<p>Negotiates and/or facilitates the achievement and maintenance of Comsec baseline requirements and standards. Leads or co-operates within own area of work to achieve compliance with Government Infosec Standard 4 policy and related local/departmental directives and policies.</p> <p>Works effectively with other relevant security staff and project teams, recognising when to seek help in issues beyond their scope and identifying correctly appropriate sources of expertise.</p>	<p>Provides leadership across the organisation to achieve compliance with Government Infosec Standard 4 policy and related local/departmental directives and policies.</p> <p>Leads or works effectively with other relevant security staff and project teams, recognising when to seek help in issues beyond their expertise and identifying correctly appropriate sources of expertise.</p>

3.2 Communicating and influencing Infosec issues

How to use this table is illustrated on p.5

		Government Core Competency	
Co-operates with an appropriate range of staff in the organisation and/or with external contacts to implement effectively the required Infosec strategies and measures.	Influential in promoting Infosec requirements, in dealings with senior staff in the organisation, and externally. Promotes Infosec competence both in practical terms and in general awareness within own business area.	Influences Infosec policy/strategic negotiations within the organisation and/or externally; may include detailed security aspects of contract negotiations. Promotes Infosec knowledge and awareness through sponsorship of an effective education, training and awareness programme; may originate and present education and training events.	Can adapt the expression of Infosec issues and requirements to a variety of audiences both within and outside the organisation such that the message is clearly understood. Is persuasive in championing Infosec across the organisation and/or a body of related organisations.

3.2 Communicating and influencing Infosec issues

Core competencies for specialist Infosec roles

Accreditor Core Competency	Comsec Practitioner Core Competency	Comsec Manager Core Competency
<p>Can adapt the expression of accreditation issues and requirements to a variety of audiences both within and outside the organisation such that the message is clearly understood.</p> <p>Influences and advises projects on security and accreditation issues.</p> <p>Produces clear and accountable documentation of all actions taken in the accreditation process.</p> <p>Influences security outcomes through a risk management approach to accreditation.</p>	<p>Is influential in supporting Comsec requirements, in advising and communicating Comsec issues to all staff in the organisation, and externally.</p> <p>Reports in a timely manner Comsec issues to affected business, policy and/or technical areas.</p> <p>Promotes Comsec competence both in practical terms and in general awareness in those who manage or otherwise use crypto items under their control.</p>	<p>Is influential in supporting Comsec requirements, in providing specific guidance and more generally communicating Comsec issues (for example, via targeted briefings) to operational decision-makers in the organisation, and externally.</p> <p>Is influential in promoting acceptance of Comsec requirements to senior decision-makers (for example the Senior Risk Officer) within the organisation and externally.</p> <p>Promotes Comsec knowledge and awareness through sponsorship of an effective education, training and awareness programme; may originate and present education and training events.</p>