



Internet security: Check list

Risk assessment

Good practice	Good practice met	Action plan	Target date
Roles and responsibilities			
<p>Roles and responsibilities for the security of the internet system and its components have been clearly defined, documented, approved and communicated. These should include responsibilities for security design, implementation and administration.</p>	<p>Yes <input type="checkbox"/> In part <input type="checkbox"/> No <input type="checkbox"/></p>	<p>..... </p>	<p>..... </p>
<p>Staff responsible for the security of the internet system and its components have appropriate skills, experience and qualifications.</p>	<p>Yes <input type="checkbox"/> In part <input type="checkbox"/> No <input type="checkbox"/></p>	<p>..... </p>	<p>..... </p>
<p>Staff responsible for the security of the internet system and its components are maintaining their skills/knowledge to keep them current.</p>	<p>Yes <input type="checkbox"/> In part <input type="checkbox"/> No <input type="checkbox"/></p>	<p>..... </p>	<p>..... </p>
Risk management			
<p>Risks to the current or planned internet system and its components have been assessed and prioritised.</p> <p>Risks are the potential for damage to the agency's internet system and its components, and the likelihood of damage. Risk assessment should also include consideration of legal and regulatory risks such as non-compliance with the requirements of the Privacy Act and/or Spam Act.</p> <p>Recognised standards include AS/NZS 4360:1999: <i>Risk management</i> which provides guidance for establishing and implementing a risk management process.</p>	<p>Yes <input type="checkbox"/> In part <input type="checkbox"/> No <input type="checkbox"/></p>	<p>..... </p>	<p>..... </p>
<p>Plans to mitigate or insure against prioritised risks have been developed and implemented.</p>	<p>Yes <input type="checkbox"/> In part <input type="checkbox"/> No <input type="checkbox"/></p>	<p>..... </p>	<p>..... </p>
<p>Risks to the internet system and its components are periodically reassessed, and reprioritised as required.</p>	<p>Yes <input type="checkbox"/> In part <input type="checkbox"/> No <input type="checkbox"/></p>	<p>..... </p>	<p>..... </p>

Policy and procedure development

Good practice	Good practice met	Action plan	Target date
Policy and procedures			
<p>An information security policy has been developed in accordance with recognised standards. The policy has been documented, approved and communicated throughout the agency.</p> <p>An information security policy can include the agency's general approach to information security, and general rules about what is allowed and what is not.</p> <p>Recognised standards include AS/NZS ISO/IEC 17799:2001 <i>Information technology - Code of practice for information security management</i>.</p>	<p>Yes <input type="checkbox"/></p> <p>In part <input type="checkbox"/></p> <p>No <input type="checkbox"/></p>		
<p>Internet security procedures consistent with the information security policy have been developed, documented, approved and communicated to relevant staff.</p> <p>Internet security procedures include step-by-step instructions about how to protect the internet system and its components.</p>	<p>Yes <input type="checkbox"/></p> <p>In part <input type="checkbox"/></p> <p>No <input type="checkbox"/></p>		
<p>Security incident procedures have been developed and documented. The procedures have been communicated to relevant staff, or throughout the agency, as applicable.</p> <p>Security incidents can include detection of unauthorised access to the internet system.</p> <p>Security incident procedures can include what to do when an incident occurs, who an incident must be reported to, and how it must be reported.</p>	<p>Yes <input type="checkbox"/></p> <p>In part <input type="checkbox"/></p> <p>No <input type="checkbox"/></p>		
<p>Policies and procedures are periodically reassessed to maintain their currency and applicability.</p>	<p>Yes <input type="checkbox"/></p> <p>In part <input type="checkbox"/></p> <p>No <input type="checkbox"/></p>		
Outsourced arrangements			
<p>If the internet system or its components are outsourced (in whole or part) to an external third party, the contract requires the party to mitigate or insure against assessed and prioritised risks.</p>	<p>Yes <input type="checkbox"/></p> <p>In part <input type="checkbox"/></p> <p>No <input type="checkbox"/></p>		
<p>Contracts with external third parties for outsourced services include the right to conduct independent audits of their operations.</p>	<p>Yes <input type="checkbox"/></p> <p>In part <input type="checkbox"/></p> <p>No <input type="checkbox"/></p>		
<p>Independent assurance is periodically obtained and evaluated by the agency on the effective operation of external party security procedures.</p> <p>Independent assurance can include the conduct of security audits of the third party, initiated either by the agency or the third party. The frequency and type of audits should depend on the assessed risk exposure to the agency.</p>	<p>Yes <input type="checkbox"/></p> <p>In part <input type="checkbox"/></p> <p>No <input type="checkbox"/></p>		

Controls implementation

Good practice	Good practice met	Action plan	Target date
Internet application security			
<p>If the internet system stores or transacts confidential data, users are authenticated before being granted access to that data.</p> <p>Confidential data can include information confidential to the agency or to internet users (such as personal or credit card details).</p> <p>Authentication can include entering a user name and password, or use of encryption techniques, to verify a user's identity. The extent of authentication procedures implemented should reflect the risks identified to the internet system.</p>	<p>Yes <input type="checkbox"/></p> <p>In part <input type="checkbox"/></p> <p>No <input type="checkbox"/></p>		
<p>Users can only access parts of the internet system they are authorised to access.</p>	<p>Yes <input type="checkbox"/></p> <p>In part <input type="checkbox"/></p> <p>No <input type="checkbox"/></p>		
<p>A privacy policy and procedures have been developed, documented, approved and communicated throughout the agency, and to users as applicable. They include requirements for handling information used and stored by internet systems.</p>	<p>Yes <input type="checkbox"/></p> <p>In part <input type="checkbox"/></p> <p>No <input type="checkbox"/></p>		
<p>If the internet system stores and transacts confidential data, the data is securely stored.</p> <p>Secure data storage can include requiring passwords for access, encrypting data, using file and directory access controls and locating data on another server.</p>	<p>Yes <input type="checkbox"/></p> <p>In part <input type="checkbox"/></p> <p>No <input type="checkbox"/></p>		
<p>Internet applications check automatically that all input data is in the correct format.</p>	<p>Yes <input type="checkbox"/></p> <p>In part <input type="checkbox"/></p> <p>No <input type="checkbox"/></p>		
Backup and recovery			
<p>Disaster recovery and/or business continuity plans have been developed, documented, approved and communicated.</p> <p>Disaster recovery and/or business continuity plans include steps that the agency will take if its internet system or components fail. The extent and complexity of the plans depends on the likely impact of the assessed and prioritised risks to the agency's operations.</p>	<p>Yes <input type="checkbox"/></p> <p>In part <input type="checkbox"/></p> <p>No <input type="checkbox"/></p>		
<p>Disaster recovery and/or business continuity plans are periodically tested and updated if required.</p>	<p>Yes <input type="checkbox"/></p> <p>In part <input type="checkbox"/></p> <p>No <input type="checkbox"/></p>		
<p>A backup policy for the internet system and its components has been documented, approved and communicated to relevant staff.</p> <p>Backing-up is making a copy of data, system settings and software so that they are not lost if the originals become unusable.</p>	<p>Yes <input type="checkbox"/></p> <p>In part <input type="checkbox"/></p> <p>No <input type="checkbox"/></p>		

Good practice	Good practice met	Action plan	Target date
Backup and recovery (continued)			
<p>All data, internet applications and the operating system are backed-up in line with the backup policy.</p>	<p>Yes <input type="checkbox"/> In part <input type="checkbox"/> No <input type="checkbox"/></p>		
<p>Backup media are stored in a secure location. Backup media are periodically relocated off-site to another location not close to the internet system.</p> <p>Backup media can include tapes, CDs, DVDs and removable hard disks.</p> <p>A secure location can include a locked, fireproof safe, as well as restrictions on who can access backup media.</p>	<p>Yes <input type="checkbox"/> In part <input type="checkbox"/> No <input type="checkbox"/></p>		
<p>Backup media are periodically tested to ensure data can be recovered.</p>	<p>Yes <input type="checkbox"/> In part <input type="checkbox"/> No <input type="checkbox"/></p>		
Change management			
<p>Change management policies and procedures to implement and modify the internet system and its components (and in particular for internet applications) have been developed, documented, approved and communicated throughout the agency.</p>	<p>Yes <input type="checkbox"/> In part <input type="checkbox"/> No <input type="checkbox"/></p>		
<p>All changes to the internet system and its components (and, in particular, internet applications) are tested to ensure that they are secure before being implemented.</p>	<p>Yes <input type="checkbox"/> In part <input type="checkbox"/> No <input type="checkbox"/></p>		
Perimeter defence			
<p>A firewall is used to separate the agency's internal network from the internet, and the firewall is correctly configured.</p> <p>Configuration is the process of adjusting the hardware and settings so that the firewall operates at maximum effectiveness.</p>	<p>Yes <input type="checkbox"/> In part <input type="checkbox"/> No <input type="checkbox"/></p>		
<p>The internet system is placed within the demilitarised zone (DMZ) using an access control device.</p> <p>An access control device can include a router or firewall.</p>	<p>Yes <input type="checkbox"/> In part <input type="checkbox"/> No <input type="checkbox"/></p>		

Good practice	Good practice met	Action plan	Target date
Perimeter defence (continued)			
<p>Firewall policies and procedures have been developed, documented, approved, communicated and implemented.</p> <p>Firewall policies and procedures can specify allowable communications to and from the internet and DMZ. Procedures can also cover changing firewall rules, upgrading firewall software and monitoring firewall logs.</p>	<p>Yes <input type="checkbox"/></p> <p>In part <input type="checkbox"/></p> <p>No <input type="checkbox"/></p>		
<p>All changes to the configuration of the firewall comply with the agency's documented change management policy and procedures.</p>	<p>Yes <input type="checkbox"/></p> <p>In part <input type="checkbox"/></p> <p>No <input type="checkbox"/></p>		
<p>Firewall rules are reviewed periodically to ensure that they are secure and comply with the firewall policy.</p> <p>Firewall rules define the specific communications that can pass through the firewall.</p>	<p>Yes <input type="checkbox"/></p> <p>In part <input type="checkbox"/></p> <p>No <input type="checkbox"/></p>		
<p>Firewall logs are regularly monitored for security violations and incidents, using applications to identify high-risk connections and threats. Action is taken and violations and incidents reported in line with procedures.</p> <p>Firewall logs are the records of communications accepted or rejected by the firewall.</p>	<p>Yes <input type="checkbox"/></p> <p>In part <input type="checkbox"/></p> <p>No <input type="checkbox"/></p>		
Security hardening			
<p>Good practice security configuration guides, specific to the agency's internet systems and components, have been followed.</p> <p>Good practice security configuration guides are provided by software and hardware vendors, and by reputable information security organisations, to help agencies secure specific internet services, operating systems and other components.</p>	<p>Yes <input type="checkbox"/></p> <p>In part <input type="checkbox"/></p> <p>No <input type="checkbox"/></p>		
<p>The internet system only uses the minimum applications and operating system functions required by the agency, and other applications and functions have been removed.</p>	<p>Yes <input type="checkbox"/></p> <p>In part <input type="checkbox"/></p> <p>No <input type="checkbox"/></p>		
<p>Applications that allow users to perform powerful system functions are not installed on the system or, when installed, their use is tightly controlled.</p> <p>Powerful system functions are functions that allow major changes to the way the system operates.</p>	<p>Yes <input type="checkbox"/></p> <p>In part <input type="checkbox"/></p> <p>No <input type="checkbox"/></p>		

Good practice	Good practice met	Action plan	Target date
Security hardening (continued)			
<p>A password policy and guidelines have been developed and compliance is either system or manually enforced. This should aim to ensure that all passwords are sufficiently complex and are changed on first use and on a regular basis.</p>	<p>Yes <input type="checkbox"/> In part <input type="checkbox"/> No <input type="checkbox"/></p>		
<p>Security alerts relating to the internet system and its components are regularly received, reviewed and actioned by IT staff as applicable.</p> <p>Security alerts can include information about system vulnerabilities such as bugs in software or hardware, ways to fix the vulnerabilities and the ways that attackers are exploiting these vulnerabilities.</p>	<p>Yes <input type="checkbox"/> In part <input type="checkbox"/> No <input type="checkbox"/></p>		
<p>The internet system hardware and related equipment is located in a secure area, and access to it is tightly controlled.</p>	<p>Yes <input type="checkbox"/> In part <input type="checkbox"/> No <input type="checkbox"/></p>		
<p>Patches and updates are tested and implemented as a high priority.</p> <p>Patches and updates are "fixes" for system vulnerabilities, bugs or configuration settings in software or hardware that are released by vendors.</p>	<p>Yes <input type="checkbox"/> In part <input type="checkbox"/> No <input type="checkbox"/></p>		
<p>Vulnerability scanning is periodically undertaken to identify and correct security weaknesses in the internet system and its components.</p> <p>Vulnerability scanning uses software to scan for known security flaws or weaknesses within a system.</p>	<p>Yes <input type="checkbox"/> In part <input type="checkbox"/> No <input type="checkbox"/></p>		
Antivirus procedures			
<p>A policy covering viruses and trojans has been developed, documented, approved and communicated.</p> <p>Viruses are applications that are designed to do something unexpected or undesirable to the internet system or its components. They are often spread from computer to computer, without user knowledge or permission.</p> <p>Trojans are applications that are hidden in legitimate applications and that open a virus or other destructive application when they are run.</p>	<p>Yes <input type="checkbox"/> In part <input type="checkbox"/> No <input type="checkbox"/></p>		
<p>The internet system and relevant components have an antivirus application correctly installed, configured and activated to detect viruses and trojans.</p>	<p>Yes <input type="checkbox"/> In part <input type="checkbox"/> No <input type="checkbox"/></p>		
<p>The antivirus application is automatically and frequently updated to minimise the risk of new viruses and trojans being undetected.</p>	<p>Yes <input type="checkbox"/> In part <input type="checkbox"/> No <input type="checkbox"/></p>		

Good practice	Good practice met	Action plan	Target date
Email			
<p>An email policy has been developed, documented, approved and communicated.</p> <p>Email policies should establish clear rules for which files and software are allowed to be received or sent.</p>	<p>Yes <input type="checkbox"/></p> <p>In part <input type="checkbox"/></p> <p>No <input type="checkbox"/></p>		
<p>Inbound and outbound emails are scanned to restrict access to viruses and unauthorised types of files. Viruses and unauthorised types of files are quarantined or rejected.</p>	<p>Yes <input type="checkbox"/></p> <p>In part <input type="checkbox"/></p> <p>No <input type="checkbox"/></p>		
<p>Unsolicited bulk commercial email (spam) is identified, blocked and rejected.</p>	<p>Yes <input type="checkbox"/></p> <p>In part <input type="checkbox"/></p> <p>No <input type="checkbox"/></p>		
<p>Attackers are "prevented" from sending emails through (bounced off) the agency's email service, to make it appear they originated from the agency.</p>	<p>Yes <input type="checkbox"/></p> <p>In part <input type="checkbox"/></p> <p>No <input type="checkbox"/></p>		
Encryption and authentication			
<p>Where the internet system sends or receives confidential information, encryption and a method of authentication is used to protect individual privacy, and to establish the agency's identity.</p> <p>Secure Socket Layer (SSL) is a common method used to secure internet communications and authenticate the identity of organisations.</p> <p>Encryption is the scrambling of data in such a way that a secret code is needed to unscramble it.</p> <p>Methods of authentication can include a password or digital certificate.</p>	<p>Yes <input type="checkbox"/></p> <p>In part <input type="checkbox"/></p> <p>No <input type="checkbox"/></p>		
<p>Encryption keys of 128 bit or greater are used to encrypt confidential communications.</p> <p>Encryption keys are the secret code that is used to scramble or unscramble data.</p>	<p>Yes <input type="checkbox"/></p> <p>In part <input type="checkbox"/></p> <p>No <input type="checkbox"/></p>		
<p>If digital certificates are used, they are current and have been issued by a reputable certificate authority.</p> <p>A digital certificate is an electronic document used during a transaction that confirms the agency's identity.</p> <p>A reputable certificate authority is a trusted third party that verifies the identity of organisations and their websites, and issues a digital certificate.</p>	<p>Yes <input type="checkbox"/></p> <p>In part <input type="checkbox"/></p> <p>No <input type="checkbox"/></p>		
<p>If digital certificates are used, they are securely stored and protected by passwords, and by file and directory level security.</p> <p>File and directory level security refers to controls over the rights of a user or system to access directories and files.</p>	<p>Yes <input type="checkbox"/></p> <p>In part <input type="checkbox"/></p> <p>No <input type="checkbox"/></p>		

Audit and monitoring

Good practice	Good practice met	Action plan	Target date
Security and activity monitoring			
<p>Audit logs on the internet system and its components are generated, collected, and secured from tampering and unauthorised access.</p> <p>Audit logs are records of dates, times, incidents, actions and other events that have occurred on the internet system and its components.</p>	<p>Yes <input type="checkbox"/></p> <p>In part <input type="checkbox"/></p> <p>No <input type="checkbox"/></p>		
Audit logs are regularly backed-up.	<p>Yes <input type="checkbox"/></p> <p>In part <input type="checkbox"/></p> <p>No <input type="checkbox"/></p>		
Audit logs are regularly monitored for security violations and incidents. Action is taken, and violations and incidents reported, in line with procedures.	<p>Yes <input type="checkbox"/></p> <p>In part <input type="checkbox"/></p> <p>No <input type="checkbox"/></p>		
<p>Intrusion detection applications are installed and operating on the internet system and its components.</p> <p>Intrusion detection applications inspect all communication and identify likely attempts to break into the system, or detect unauthorised access to system files.</p>	<p>Yes <input type="checkbox"/></p> <p>In part <input type="checkbox"/></p> <p>No <input type="checkbox"/></p>		
Audit			
<p>A security audit has been conducted on the internet system and its components.</p> <p>A security audit is the step-by-step process to determine if the system is well-secured against attackers. The type of security audits can vary, and include:</p> <ul style="list-style-type: none"> • compliance with information security policies and procedures • assessment of the configuration of an internet system or its components • testing of general computer controls. 	<p>Yes <input type="checkbox"/></p> <p>In part <input type="checkbox"/></p> <p>No <input type="checkbox"/></p>		
Security audits are conducted at a frequency influenced by the risk assessment (previously referred).	<p>Yes <input type="checkbox"/></p> <p>In part <input type="checkbox"/></p> <p>No <input type="checkbox"/></p>		