



Information Security Manual: March 2022 Changes

Published: 10 March 2022

Summary of content changes

Changes for the March 2022 update of the [Information Security Manual](#) (ISM) are covered below.

Cyber security principles

The existing detect and respond principles were amended to reflect that the identification of cyber security incidents is a detection principle rather than a response principle. Furthermore, the existing detect principle was amended to reflect that the detection of cyber security events is based upon the collection and analysis of event logs.

The previous principles were:

- **D1:** Cyber security events and anomalous activities are detected, collected, correlated and analysed in a timely manner.
- **R1:** Cyber security incidents are identified and reported both internally and externally to relevant bodies in a timely manner.

The revised principles are:

- **D1:** Event logs are collected and analysed in a timely manner to detect cyber security events.
- **D2:** Cyber security events are analysed in a timely manner to identify cyber security incidents.
- **R1:** Cyber security incidents are reported both internally and externally to relevant bodies in a timely manner.

Audit terminology

Due to the confusing use of audit terminology, references to 'audited' have been changed to 'verified'. For example, an ICT equipment register is verified (rather than audited) on a regular basis. This will allow security personnel, or other suitable parties, to conduct such activities rather than having to rely on the use of an organisation's internal auditors. In addition, ISM-1301 has been rescinded as the recommendation to track network devices is covered by the recommendation to track ICT equipment (ISM-0336).

New Security Controls	Modified Security Controls	Rescinded Security Controls
	ISM-0211, ISM-0336, ISM-0660, ISM-1243, ISM-1294, ISM-1493, ISM-1571, ISM-1543, ISM-1637, ISM-1645, ISM-1713	ISM-1301

Cyber supply chain considerations

The recommendation to choose components and services relevant to the security of systems from suppliers and service providers that have made a commitment to secure-by-design practices has been amended to suppliers and service providers that have made a commitment to secure-by-design principles, secure programming practices and maintaining the security of their products.

New Security Controls	Modified Security Controls	Rescinded Security Controls
ISM-1568		

Using managed service providers

Managed service providers manage the services of an organisation on their behalf. This may include application services, authentication services, backup services, cloud services, desktop services, enterprise mobility services, gateway services, hosting services, network services, procurement services, security services, support services, and many other business-related services. In doing so, managed service providers may manage services from their customers' premises or their own premises. In considering security risks associated with managed services, an organisation should consider all managed service providers that have access to their facilities, systems or data.

New Security Controls	Modified Security Controls	Rescinded Security Controls
ISM-1736, ISM-1737		

Monitoring compliance with contractual requirements

While some forms of outsourcing, such as the use of cloud services or systems provided by managed service providers, require a security assessment at regular points in time, such as every two years, this does not exempt outsourced services providers from being continually monitored for compliance with security requirements stipulated within contractual arrangements. In doing so, an organisation should regularly exercise their right to verify compliance with security requirements specified in contractual requirements in order to ensure compliance is being maintained between any regularly scheduled formal security assessments.

New Security Controls	Modified Security Controls	Rescinded Security Controls
ISM-1738		

Approval of security architecture

If security documentation is not reviewed and approved by an appropriate authority, system owners risk failing in their duty to ensure that appropriate security controls have been identified and implemented for systems and their operating environments. In doing so, it is important that a system's security architecture, as outlined within the system security plan and supported by the incident response plan and continuous monitoring plan, is approved by the system's authorising officer prior to the development of the system.

New Security Controls	Modified Security Controls	Rescinded Security Controls
ISM-1739		

Business email compromise

Business email compromise, a form of financial fraud, is when an adversary attempts to scam an organisation out of money or assets with the assistance of a compromised email account. In dealing with such situations, personnel should have clear guidance to verify bank account details, think critically before actioning unusual payment requests, and have a process to report threatening demands for immediate action, pressure for secrecy or requests to circumvent normal business processes and procedures.

New Security Controls	Modified Security Controls	Rescinded Security Controls
-----------------------	----------------------------	-----------------------------

ISM-1740

Operating system selection

When selecting operating systems, it is important that an organisation preferences vendors that have demonstrated a commitment to secure-by-design principles, secure programming practices and maintaining the security of their products.

New Security Controls	Modified Security Controls	Rescinded Security Controls
-----------------------	----------------------------	-----------------------------

ISM-1743

Operating system releases

The recommendation to use the latest release, or previous release, of operating systems for workstations, servers and networks devices has been expanded to cover operating systems for other ICT equipment as well.

New Security Controls	Modified Security Controls	Rescinded Security Controls
-----------------------	----------------------------	-----------------------------

ISM-1744

Use of 64-bit operating systems

The recommendation to use 64-bit versions of Microsoft Windows operating systems has been expanded to cover 64-bit versions of all operating systems where supported. This allows an organisation to leverage additional security functionality of modern processors that isn't available to 32-bit versions of operating systems.

New Security Controls	Modified Security Controls	Rescinded Security Controls
-----------------------	----------------------------	-----------------------------

ISM-1408

Operating system exploit protection functionality

The recommendation to implement Microsoft exploit protection functionality has been expanded to cover exploit protection functionality that may exist in any operating system.

New Security Controls	Modified Security Controls	Rescinded Security Controls
	ISM-1492	

Boot process protection

To provide security for the boot process, Microsoft introduced Early Launch Antimalware, Secure Boot, Trusted Boot and Measured Boot in Microsoft Windows 10 and equivalent versions of Microsoft Windows Server. These features can assist in preventing rootkits and bootkits from executing, thereby providing protection whilst the operating system boots.

New Security Controls	Modified Security Controls	Rescinded Security Controls
		ISM-1745

Script execution engines

The recommendation to prevent unprivileged users from running script execution engines in Microsoft Windows has been expanded to encompass the use of script execution engines in any operating system.

New Security Controls	Modified Security Controls	Rescinded Security Controls
	ISM-1491	

Using local administrator accounts

The recommendation to disable the use of local administrator accounts has been removed due to a conflict with the [Essential Eight Maturity Model](#). Furthermore, the recommendation allowing any privileged account to bypass application control has been paired back to local administrator accounts and break glass accounts.

New Security Controls	Modified Security Controls	Rescinded Security Controls
	ISM-0846	ISM-1410, ISM-1469

Application control logging

The recommendation to capture specific details of event logs associated with application control (ISM-0957) was rescinded due to significant overlap with existing event logging recommendations (ISM-0585).

New Security Controls	Modified Security Controls	Rescinded Security Controls
	ISM-0585	ISM-0957

Software firewalls

The recommendation to implement a software firewall to restrict inbound and outbound network connections has been amended to restricting inbound and outbound network connections to an organisation-approved set of applications and services.

New Security Controls	Modified Security Controls	Rescinded Security Controls
	ISM-1416	

Antivirus software

The recommendation to use reputation rating functionality for antivirus software (ISM-1390) was merged into overarching recommendations for antivirus software (ISM-1417).

New Security Controls	Modified Security Controls	Rescinded Security Controls
	ISM-1417	ISM-1390

Device access control software

Existing language for the use of device access control software has been standardised around reading from and writing to both removable media and devices.

New Security Controls	Modified Security Controls	Rescinded Security Controls
	ISM-0343, ISM-1418	

Monitoring account logons, logoffs and lockouts

The existing recommendation to monitoring account logons and logoffs (ISM-0584) was merged with recommendations regarding operating system event logging (ISM-0582). Furthermore, a new recommendation to monitor account lockouts (i.e. event ID 4740) was introduced. Finally, the existing recommendation to investigate account lockouts (ISM-0431) was rescinded as it is now more accurately covered by ISM-1747 relating to monitoring and responding to unusual operating system event logs – in this case instances of suspicious account lockouts.

New Security Controls	Modified Security Controls	Rescinded Security Controls
	ISM-0582	ISM-0431, ISM-0584

Application selection

When selecting applications, it is important that an organisation preferences vendors that have demonstrated a commitment to secure-by-design principles, secure programming practices and maintaining the security of their products.

New Security Controls	Modified Security Controls	Rescinded Security Controls
	ISM-0938	

Hardening applications

The recommendation to harden the use of web browsers, Microsoft Office and PDF software has been expanded to cover other office productivity suites, email clients and security products. This aligns with the emphasis placed on

protecting these types of products by the [Essential Eight Maturity Model](#). Furthermore, additional rationale has been included to note that when Australian Cyber Security Centre (ACSC) and vendor hardening guidance conflicts, preference should be given to implementing ACSC hardening guidance.

New Security Controls	Modified Security Controls	Rescinded Security Controls
ISM-1748	ISM-1235, ISM-1470	

Memorised secrets for multi-factor authentication

Rather than supporting only the use of passwords for multi-factor authentication, multi-factor authentication recommendations have been amended to support the use of any form of memorised secret, such as personal identification numbers, passwords or passphrases.

New Security Controls	Modified Security Controls	Rescinded Security Controls
	ISM-1559, ISM-1560, ISM-1561	

Reuse of single factors from multi-factor authentication

The recommendation to prevent the reuse of a single factor used as part of multi-factor authentication for single-factor authentication to other systems was rescinded as it was not deemed practical. For example, in the case of multi-factor authentication for remote access to systems that don't normally use multi-factor authentication, to do so would what have required that all users be issued with two different user accounts, one using a single factor for access and one using multiple factors for remote access – each with different passphrases.

New Security Controls	Modified Security Controls	Rescinded Security Controls
		ISM-1357

Verifying users when requesting account unlocks

The recommendation for users to provide sufficient evidence to verify their identity when requesting an account unlock was rescinded as it provided little security benefit. For example, if a locked account was unlocked by a service desk member the user would still need to know their original credentials in order to logon again. In cases where new credentials were required, such activities would fall under the scope of recommendations for verifying a user's identity before issuing new credentials (ISM-1593). Note, any repeated lockouts of an account (which could indicate a password guessing attack taking place) is captured by the monitoring of account lockout events (i.e. event ID 4740) under ISM-0582.

New Security Controls	Modified Security Controls	Rescinded Security Controls
		ISM-0976

Storing physical credentials with systems

Due to perceptions that this recommendation prevented the use of password managers and hardware security modules, it was amended to refer to physical credentials being stored with systems.

New Security Controls	Modified Security Controls	Rescinded Security Controls
	ISM-0418	

Storing credentials on systems

The previous recommendation to ensure that credentials are hashed, salted and stretched when stored on systems has been expanded to include the use of password managers and hardware security modules. Furthermore, the existing recommendation within the [Guidelines for Database Systems](#) that duplicated the hashing, salting and stretching advice (ISM-1252) was rescinded.

New Security Controls	Modified Security Controls	Rescinded Security Controls
	ISM-1402	ISM-1252

Limiting the number of cached credentials

When using Microsoft Windows systems, cached credentials are stored in the Security Accounts Manager database and can allow a user to logon to a workstation that they have previously logged onto even if the domain is not available. Whilst this functionality may be desirable from an availability perspective, this functionality can be abused by an adversary who can retrieve these cached credentials. To reduce this risk, cached credentials should be limited to only one previous logon.

New Security Controls	Modified Security Controls	Rescinded Security Controls
ISM-1749		

Virtualisation hardening

Requirements for software-based isolation mechanisms to be from a vendor that uses secure programming practices has been expanded to a vendor that has demonstrated a commitment to secure-by-design principles, secure programming practices and maintaining the security of their products.

New Security Controls	Modified Security Controls	Rescinded Security Controls
	ISM-1460	

System administration processes and procedures

Due to significant overlap, previous change management recommendations are now captured under system administration processes and procedures.

New Security Controls	Modified Security Controls	Rescinded Security Controls
	ISM-1211	

Using separate administrative infrastructure for high value servers

The security of administrative activities can be improved by segregating administrative infrastructure from an organisation's wider network. In doing so, the use of a jump server (also known as a jump host or jump box) can be an effective way of simplifying and securing administrative activities. Furthermore, using separate jump servers for the administration of critical servers, high-value servers and regular servers can further assist in protecting these assets.

New Security Controls	Modified Security Controls	Rescinded Security Controls
ISM-1750	ISM-1381, ISM-1385, ISM-1386, ISM-1388	ISM-1383

Patch management processes and procedures

Previous iterations of the [Essential Eight Maturity Model](#) drew a distinction between how to patch 'applications and drivers' and 'operating systems and firmware'. As such requirements are no longer stipulated in the [Essential Eight Maturity Model](#), the previous six recommendations have been collapsed into one recommendation.

New Security Controls	Modified Security Controls	Rescinded Security Controls
	ISM-0298	ISM-0303, ISM-1497, ISM-1498, ISM-1499, ISM-1500

Patching other ICT equipment

While existing recommendations covered patching security vulnerabilities in workstations, servers and network devices, they did not cover patching security vulnerabilities in other ICT equipment.

New Security Controls	Modified Security Controls	Rescinded Security Controls
ISM-1751, ISM-1752		

Unsupported network devices and other ICT equipment

While existing recommendations covered the replacement of unsupported applications and operating systems, they did not cover the replacement of unsupported network devices and other ICT equipment. This is important as an organisation should ensure that network devices and other ICT equipment remain supported by vendors and do not become a weak point on networks. At a minimum, if unsupported network devices and other ICT equipment are used on networks, they should be recognised and risk-managed as appropriate.

New Security Controls	Modified Security Controls	Rescinded Security Controls
ISM-1753		

Protection of event logs

The approach to the management of event logs has been standardised to align with the [Essential Eight Maturity Model](#). Furthermore, specific events to be logged, such as those related to databases, operating systems and web applications, have been moved to relevant guidelines.

New Security Controls	Modified Security Controls	Rescinded Security Controls
ISM-1747, ISM-1757, ISM-1758, ISM-1775, ISM-1776, ISM-1777	ISM-1536, ISM-1537	ISM-0586

Software testing

In addition to ensuring applications are robustly tested for security vulnerabilities prior to their initial release, they should also be robustly tested for security vulnerabilities following any maintenance activities. Subsequently, any security vulnerabilities that are identified should be remedied.

New Security Controls	Modified Security Controls	Rescinded Security Controls
ISM-1754	ISM-0402	

Vulnerability disclosure programs

In support of the existing recommendation to implement a vulnerability disclosure program, two new recommendations have been introduced to cover the development and implementation of a vulnerability disclosure policy, and the development and implementation of vulnerability disclosure processes and procedures.

New Security Controls	Modified Security Controls	Rescinded Security Controls
ISM-1755, ISM-1756		

Encrypting database server hard drives

The recommendation to encrypt the hard disks of database servers (ISM-1425) was rescinded due to duplication of existing recommendations to encrypt all data stored on media (ISM-1059) using full disk encryption (ISM-0459).

New Security Controls	Modified Security Controls	Rescinded Security Controls
		ISM-1425

Aggregated database contents

The recommendation to implement database views and database roles due to aggregated database contents (ISM-1258) was rescinded due to existing recommendations covering the enforcement of the need-to-know principle as part of business as usual practices (ISM-1268).

New Security Controls	Modified Security Controls	Rescinded Security Controls
		ISM-1258

Cryptographic recommendations for OFFICIAL to PROTECTED data

While existing recommendations for the use of ASD-Approved Cryptographic Algorithms to protect OFFICIAL through to PROTECTED data addressed minimum key lengths, they didn't address recommended key lengths.

New Security Controls	Modified Security Controls	Rescinded Security Controls
ISM-1766	ISM-0472, ISM-0474, ISM-0475, ISM-0476, ISM-1630	

Cryptographic recommendations for SECRET to TOP SECRET data

The existing table outlining cryptographic algorithms for use with High Assurance Cryptographic Equipment has been converted into discrete recommendations. Furthermore, the recommendation to give preference to the United State's Commercial National Security Algorithm suite algorithms and key sizes (ISM-1232) has been rescinded in preference to including recommended key lengths for each individual algorithm.

New Security Controls	Modified Security Controls	Rescinded Security Controls
ISM-1759, ISM-1760, ISM-1761, ISM-1762, ISM-1763, ISM-1764, ISM-1765, ISM-1767, ISM-1768, ISM-1769, ISM-1770		ISM-1232

Deprecation of IKE Version 1 for IPsec

The Internet Key Exchange version 1 (IKEv1) protocol was obsoleted by the IKE version 2 (IKEv2) protocol in December 2005. Since IKEv2 has now been widely adopted, and in doing so addresses various problems with IKEv1, approval for the use of IKEv1 as part of Internet Protocol security implementations has been rescinded.

New Security Controls	Modified Security Controls	Rescinded Security Controls
ISM-1771, ISM-1772	ISM-0998, ISM-0999, ISM-1233	ISM-0497, ISM-1001

Gateway architectures

Existing recommendations for gateway architectures and their configuration (ISM-0631) were split into discrete recommendations with duplicate content being removed.

New Security Controls	Modified Security Controls	Rescinded Security Controls
ISM-1774	ISM-0631, ISM-0634, ISM-1037	

Stakeholders for connected security domains

The existing recommendation that system owners be formal stakeholders for all security domains connected via gateways (ISM-0607) was rescinded due to duplication with the intent of the recommendation that system owners monitor each system, and associated cyber threats, security risks and security controls on an ongoing basis (ISM-1526). Notably, this requires system owners to be aware of the cyber threats posed to their systems by gateways and other connected systems. In doing so, system owners are encouraged to leverage requirements from the [Guidelines for Outsourcing](#) to achieve this outcome, such as exercising the right to verify compliance with security requirements documented in contractual arrangements (ISM-1738) and the ability to access all logs relating to their organisation's data and services (ISM-1573).

New Security Controls	Modified Security Controls	Rescinded Security Controls
		ISM-0607

System administrators of gateways

The existing recommendation (ISM-0613) for system administrators of gateways connected to Australian Eyes Only (AUSTEO) or Australian Government Access Only (AGAO) networks to be Australian nationals was re-scoped to just AUSTEO networks. Meanwhile, a new recommendation was introduced (ISM-1773) to reflect that seconded foreign nationals are capable of performing system administration activities for gateways connected to AGAO and Releasable To (REL) networks.

New Security Controls	Modified Security Controls	Rescinded Security Controls
ISM-1773	ISM-0613	

Gateway authentication

The existing recommendation that users be authenticated to gateways (ISM-0620) was rescinded due to duplication with the existing recommendation that users be authentication to systems (ISM-1546). In addition, the recommendation to use multi-factor authentication (ISM-1039) was rescinded due to duplication of existing multi-factor authentication recommendations (ISM-0974 and ISM-1173).

New Security Controls	Modified Security Controls	Rescinded Security Controls
		ISM-0620, ISM-1039

Implementing a Cross Domain Solution

The recommendation to contact the ACSC when introducing additional connectivity to Cross Domain Solutions (ISM-0627) was merged into the recommendation to contact the ACSC when designing and deploying Cross Domain Solutions (ISM-0597).

New Security Controls	Modified Security Controls	Rescinded Security Controls
	ISM-0597	ISM-0627

Firewall requirements

The existing recommendation noting 'the requirement to use a firewall as part of gateway infrastructure is met by both parties independently; shared ICT equipment does not satisfy the requirements of both parties' (ISM-1194) was rescinded as it was deemed to be more appropriate as rationale.

New Security Controls	Modified Security Controls	Rescinded Security Controls
		ISM-1194

TLS inspection

The existing recommendation that legal advice be sought regarding monitoring activities (ISM-0996) was rescinded due to duplication with the existing recommendation that legal advice be sought regarding advising users of the extent of monitoring activities for systems (ISM-0979).

New Security Controls	Modified Security Controls	Rescinded Security Controls
		ISM-0996

Allowing access to websites

The recommendation to implement a list of website categories for web content filters (ISM-1170) was merged into the recommendation to implement a list of organisation-approved domain names (ISM-0958) as an alternative approach.

New Security Controls	Modified Security Controls	Rescinded Security Controls
	ISM-0958	ISM-1170

Blocking access to websites

The recommendation to implement a list of blocked websites only if a list of allowed websites wasn't implemented was merged into recommendations to block dynamic domain names and domain names that can be registered anonymously for free, thereby reflecting that even if a list of approved website categories is implemented that tailored blocking of specific known malicious domain names can still be beneficial.

New Security Controls	Modified Security Controls	Rescinded Security Controls
	ISM-1236	ISM-0959, ISM-0960

Failing content inspection

Existing recommendations to block files that fail content inspection (ISM-1291 and ISM-1292) were rescinded due to duplicating the overarching recommendation to block all malicious content that is identified by content filters.

New Security Controls	Modified Security Controls	Rescinded Security Controls
	ISM-0651	ISM-1291, ISM-1292

Validating file integrity

The recommendation to block files that fail digital signature checks (ISM-0677) was expanded to cover files that fail checksum checks.

New Security Controls	Modified Security Controls	Rescinded Security Controls
	ISM-0677	

Export of highly sensitive data

The existing recommendation to conduct keyword searches on all textual data when exporting AUSTEO or AGAO data from a system (ISM-0678) was merged into the overarching recommendation to establish processes and procedures to prevent AUSTEO and AGAO data in both textual and non-textual forms from being exported to foreign systems (ISM-1535). In addition, the recommended to prevent the export of REL data has also been included to prevent export to specific foreign systems that it is not authorised to be exported to.

New Security Controls	Modified Security Controls	Rescinded Security Controls
	ISM-1535	ISM-0678

Quarantine of data transfers

Previous guidance within the [Guidelines for Data Transfers](#) lacked recommendations for how to handle failures of security checks as part of manual data import and data export activities, such as via the use of removable media. As such, recommendations were introduced to ensure that when manually importing or exporting data to systems, all data that fails security checks is quarantined until reviewed and subsequently approved or not approved for release.

New Security Controls	Modified Security Controls	Rescinded Security Controls
ISM-1778, ISM-1779		

Miscellaneous changes

Miscellaneous changes were made to rationale and recommendations throughout the publication to clarify content without changing intent. This included a review from the [Guidelines for System Hardening](#) chapter through to the [Guidelines for Data Transfers](#) chapter.

New Security Controls	Modified Security Controls	Rescinded Security Controls
ISM-1741, ISM-1742, ISM-1746	ISM-0039, ISM-0109, ISM-0252, ISM-0260, ISM-0261, ISM-0263, ISM-0269, ISM-0300, ISM-0310, ISM-0311, ISM-0315, ISM-0330,	

New Security Controls	Modified Security Controls	Rescinded Security Controls
	ISM-0362, ISM-0368, ISM-0380, ISM-0382, ISM-0383, ISM-0401, ISM-0428, ISM-0434, ISM-0455, ISM-0457, ISM-0462, ISM-0465, ISM-0469, ISM-0477, ISM-0487, ISM-0488, ISM-0489, ISM-0490, ISM-0496, ISM-0498, ISM-0501, ISM-0506, ISM-0516, ISM-0521, ISM-0536, ISM-0546, ISM-0569, ISM-0571, ISM-0574, ISM-0589, ISM-0590, ISM-0591, ISM-0610, ISM-0611, ISM-0612, ISM-0616, ISM-0619, ISM-0622, ISM-0626, ISM-0628, ISM-0629, ISM-0635, ISM-0637, ISM-0639, ISM-0643, ISM-0645, ISM-0648, ISM-0649, ISM-0652, ISM-0657, ISM-0658, ISM-0659, ISM-0661, ISM-0664, ISM-0669, ISM-0670, ISM-0675, ISM-0718, ISM-0853, ISM-0961, ISM-0963, ISM-0988, ISM-0991, ISM-1023, ISM-1024, ISM-1028, ISM-1030, ISM-1034, ISM-1080, ISM-1089, ISM-1139, ISM-1157, ISM-1158, ISM-1171, ISM-1181, ISM-1182, ISM-1185, ISM-1186, ISM-1187, ISM-1192, ISM-1227, ISM-1228, ISM-1234, ISM-1237, ISM-1238, ISM-1239, ISM-1240, ISM-1241, ISM-1247, ISM-1251, ISM-1260, ISM-1269, ISM-1270, ISM-1273, ISM-1274, ISM-1277, ISM-1278, ISM-1284, ISM-1286, ISM-1287, ISM-1288, ISM-1289, ISM-1290, ISM-1293, ISM-1304, ISM-1312, ISM-1316, ISM-1317, ISM-1318, ISM-1324, ISM-1338, ISM-1361, ISM-1369, ISM-1370, ISM-1372, ISM-1373, ISM-1374, ISM-1375, ISM-1389, ISM-1392, ISM-1405, ISM-1420, ISM-1424, ISM-1427, ISM-1428, ISM-1429, ISM-1431, ISM-1437, ISM-1439, ISM-1448, ISM-1457, ISM-1461, ISM-1467, ISM-1480, ISM-1483, ISM-1506, ISM-1520, ISM-1521, ISM-1522, ISM-1523, ISM-1524, ISM-1528, ISM-1532, ISM-1553,	

New Security Controls	Modified Security Controls	Rescinded Security Controls
	ISM-1558, ISM-1573, ISM-1574, ISM-1576, ISM-1577, ISM-1578, ISM-1581, ISM-1590, ISM-1592, ISM-1593, ISM-1594, ISM-1595, ISM-1596, ISM-1601, ISM-1605, ISM-1606, ISM-1608, ISM-1632, ISM-1638, ISM-1641, ISM-1709, ISM-1710, ISM-1712, ISM-1717, ISM-1722, ISM-1723, ISM-1724, ISM-1725, ISM-1726, ISM-1727	

Contact details

If you have any questions regarding this guidance you can [write to us](#) or call us on 1300 CYBER1 (1300 292 371).