Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Australian Government Information Security Manual Changes Document

NOVEMBER 2018

Removal of security controls

In reviewing security controls from the previous release of the ***Australian Government Information Security Manual*** (ISM), the following criteria were used:

- Does the security control need to be removed due to ***Protective Security Policy Framework*** (PSPF) reforms?
- Does the security control need to be removed due to a change in the threat environment?
- Does the security control need to be changed due to a change in technology?
- Does the security control need to be changed due to a change in policy position?
- Is the security control of sufficient value to be retained?
- Is the security control duplicated elsewhere in the document?
- Is the security part of a group of similar security controls that could be combined?

As a result of this review, 258 of 945 security controls (roughly 27 percent) were removed.

The security controls that were removed are listed in the following table.

Security Control	Reason
0001	Removed due to a change from a compliance culture to a risk management culture.
0003	Removed due to a change from a compliance culture to a risk management culture.
0007	Removed due to a change from a compliance culture to a risk management culture.
0008	Removed due to a change from a compliance culture to a risk management culture.
0009	Removed as the fundamentals of risk management don't need to be duplicated within this publication.
0013	Removed to ensure a focus on Chief Information Security Officers (CISOs) as the authority for all cyber security matters within organisations.

0025	Removed to ensure a focus on CISOs as the authority for all cyber security matters within organisations.
0039	Removed to ensure a focus on system-specific security documentation.
0040	Removed to ensure a focus on system-specific security documentation.
0044	Removed due to being better served as supporting information.
0046	Removed due to being better served as supporting information.
0049	Removed to ensure a focus on system-specific security documentation.
0051	Removed due to a merge of relevant content into security control 0042.
0055	Removed due to a merge of relevant content into security control 0042.
0056	Removed due to a merge of relevant content into security control 0042.
0057	Removed due to being better served as supporting information.
0058	Removed due to a merge of relevant content into security control 0043.
0059	Removed due to a merge of relevant content into security control 0043.
0062	Removed due to this activity being coordinated at the discretion of chief wardens within organisations.
0067	Removed due to being better served as supporting information.
0069	Removed due to not having a strong reason to be retained. Reaccreditation should be triggered by significant changes to a system or its operating environment, not an arbitrary timeframe.
0070	Removed due to not having a strong reason to be retained. Reaccreditation should be triggered by significant changes to a system or its operating environment, not an arbitrary timeframe.
0071	Removed due to covering the same intent as security control 0605.
0076	Removed due to being better served as supporting information.
0077	Removed due to being better served as supporting information.
0082	Removed due to being better served as supporting information.
0112	Removed due to a merge of relevant content into security control 1163.

0113	Removed due to a merge of relevant content into security control 1163.
0117	Removed due to duplication of intent of security control 0115.
0118	Removed due to being insufficiently defined as a security control.
0119	Removed due to being replaced by a new section focused on daily backups as per the associated Essential Eight mitigation strategy.
0121	Removed due to not having a strong reason to be retained.
0124	Removed due to a merge of relevant content into security control 0922.
0126	Removed due to a merge of relevant content into security control 0125.
0129	Removed due to not having a strong reason to be retained.
0130	Removed due to a merge of relevant content into security control 0922.
0131	Removed due to duplication of intent of security control 0043.
0132	Removed due to duplication of intent of security control 0043.
0134	Removed due to a merge of relevant content into security control 0133.
0135	Removed due to a merge of relevant content into security control 0133.
0136	Removed due to a merge of relevant content into security control 0133.
0139	Removed due to a merge of relevant content into security control 0140.
0150	Removed due to not having a strong reason to be retained.
0162	Removed due to being better served as supporting information.
0172	Removed due to duplication of intent of security control 0225.
0196	Removed due to a merge of relevant content into security control 0195.
0209	Removed due to a merge of relevant content into security controls 0208 and 0210.
0238	Removed due to a merge of relevant content into security control 0237.
0242	Removed due to being better served as supporting information.

0244	Removed due to a merge of relevant content into security control 0245.
0251	Removed due to duplication of intent of security control 0252.
0253	Removed due to being better served as supporting information.
0255	Removed due to a merge of relevant content into security control 0252.
0256	Removed due to duplication of intent of security control 0922.
0266	Removed due to being better served as supporting information.
0275	Removed due to a merge of relevant content into security control 0273.
0279	Removed due to being better served as supporting information.
0282	Removed due to it leading to a perception that using unevaluated products is risky.
0283	Removed due to duplication of intent of security control 0290.
0284	Removed due to duplication of intent of security control 0285.
0287	Removed due to being better served as supporting information.
0291	Removed due to being better served as supporting information.
0297	Removed due to being better served as supporting information.
0308	Removed due to being covered by the intent of security control 0306.
0319	Removed due to being better served as supporting information.
0321	Removed due to a merge of relevant content into security control 0315.
0322	Removed due to duplication of intent of security control 1359.
0329	Removed due to a merge of relevant content into security control 0375.
0333	Removed due to being better served as supporting information.
0334	Removed due to being better served as supporting information.
0335	Removed due to changes to the classification system for Australian Government information.
0344	Removed due to a merge of relevant content into security control 0345.

0346	Removed due to duplication of intent of security control 1359.
0353	Removed as sanitised media can be treated as OFFICIAL unless otherwise specified.
0364	Removed due to duplication of intent of security control 0366.
0413	Removed due to duplication of intent of security control 0041.
0416	Removed due to being better served as supporting information.
0419	Removed due to a merge of relevant content into security control 1402.
0440	Removed due to duplication of intent of security control 0441.
0442	Removed to ensure a focus on system-specific security documentation.
0456	Removed due to a merge of relevant content into security control 0455.
0463	Removed due to duplication of intent of security control 0289.
0464	Removed due to duplication of intent of security control 0289.
0482	Removed due to Secure Sockets Layer (SSL) no longer being an ASD Approved Cryptographic Algorithm (AACA).
0486	Removed due to being better served as supporting information.
0495	Removed due to a merge of relevant content into security control 0494.
0500	Removed due to being better served as supporting information.
0502	Removed due to being covered by an Australian Communications Security Instruction (ACSI).
0503	Removed due to being covered by an ACSI.
0504	Removed due to being covered by an ACSI.
0507	Removed due to being covered by an ACSI.
0509	Removed due to being covered by an ACSI.
0510	Removed due to being covered by an ACSI.
0511	Removed due to being covered by an ACSI.

0513	Removed due to being better served as supporting information.
0514	Removed due to being covered by the intent of security control 0518.
0515	Removed due to being covered by the intent of security control 0518.
0525	Removed due to being covered by the intent of security control 0809.
0533	Removed due to a merge of relevant content into security control 0534.
0577	Removed due to a merge of relevant content into security control 1028.
0583	Removed due to a merge of relevant content into security control 0582.
0587	Removed due to a merge of relevant content into security control 1405.
0609	Removed due to a merge of relevant content into security control 0610.
0662	Removed due to a merge of relevant content into security control 0663.
0685	Removed due to being a legacy security control that is no longer applicable.
0693	Removed due to a merge of relevant content into security control 1400.
0700	Removed due to a merge of relevant content into security control 0701.
0710	Removed due to a change from a compliance culture to a risk management culture.
0711	Removed due to a change from a compliance culture to a risk management culture.
0713	Removed due to a change from a compliance culture to a risk management culture.
0741	Removed to ensure a focus on CISOs as the authority for all cyber security matters within organisations.
0768	Removed to ensure a focus on CISOs as the authority for all cyber security matters within organisations.
0787	Removed due to being better served as supporting information.
0788	Removed to ensure a focus on system-specific security documentation.
0789	Removed due to a merge of relevant content into security control 0042.
0790	Removed due to a merge of relevant content into security control 0042.

0791	Removed due to being better served as supporting information.
0793	Removed due to being better served as supporting information.
0795	Removed due to being a moot point when considered in the context of security control 0064.
0797	Removed due to covering the same intent as security control 0047.
0798	This activity may be conducted in support of a security assessment but is not the primary focus of a security assessment. The primary focus of a security assessment is to assess the selection, implementation and effectiveness of security controls identified in the Statement of Applicability (SoA).
0806	Removed due to covering the same intent as security control 0805.
0807	Removed due to a merge of relevant content into security control 1140.
0808	Removed due to a merge of relevant content into security control 0064.
0818	Removed due to being better served as supporting information.
0819	Removed due to being better served as supporting information.
0822	Removed due to being better served as supporting information.
0823	Removed due to not having a strong reason to be retained.
0830	Removed due to a merge of relevant content into security control 0225.
0832	Removed due to a merge of relevant content into security control 1059.
0845	Replaced by security controls 1503 and 1508.
0852	Removed due to changes to the classification system for Australian Government information.
0856	Replaced by security controls 1503 and 1508.
0865	Removed due to being a legacy security control that is no longer applicable.
0872	Removed due to covering the same intent as security control 0064.
0876	Removed due to a change from a compliance culture to a risk management culture.
0879	Removed due to not having a strong reason to be retained.
0885	Removed due to being better served as supporting information.

0886	Removed due to being better served as supporting information.
0887	Removed due to covering the same intent as security control 0047.
0890	Removed to ensure a focus on system-specific security documentation.
0893	Removed to ensure a focus on system-specific security documentation.
0894	Removed to ensure a focus on system-specific security documentation.
0895	Removed due to a merge of relevant content into security control 0041.
0902	Removed due to being better served as supporting information.
0909	Removed due to a merge of relevant content into security control 0911.
0912	Removed due to a merge of relevant content into security control 1211.
0913	Removed due to a merge of relevant content into security control 1510.
0914	Removed due to a merge of relevant content into security control 1510.
0915	Removed due to being better served as supporting information.
0916	Removed due to being better served as supporting information.
0922	Removed due to a merge of relevant content into security control 0252.
0929	Removed due to being already covered in security controls 0221, 1058 and 1155.
0937	Removed due to being better served as supporting information.
0941	Removed due to being better served as supporting information.
0943	Removed due to a merge of relevant content into security control 0306.
0967	Removed due to being better served as supporting information for security control 0278.
0968	Removed due to being better served as supporting information for security control 0278.
0969	Removed due to being covered by security control 0270.
0973	Removed due to a merge of relevant content into security control 0415.
0980	Removed due to being better served as supporting information.

0985	Removed due to being covered by more recent secure administration security controls.
0987	Removed due to a split of content into security controls 0582, 1536 and 1537.
0989	Removed due to being covered by security control 0586.
0997	Removed due to a merge of relevant content into security control 0488.
1002	Removed due to being better served as supporting information.
1003	Removed due to being covered by an ACSI.
1004	Removed due to being covered by an ACSI.
1005	Removed due to being covered by an ACSI.
1029	Removed due to a merge of relevant content into security control 1030.
1033	Removed due to a merge of relevant content into security control 1417.
1047	Removed due to a merge of relevant content into security control 1399.
1061	Removed due to a change from a compliance culture to a risk management culture.
1066	Removed due to duplication of intent of security control 1067.
1068	Removed due to a merge of relevant content into security control 0354.
1072	Removed due to being too prescriptive.
1077	Removed due to duplication of intent of security control 0678.
1097	Removed due to a merge of relevant content into security controls 0208 and 0210.
1129	Removed due to a merge of relevant content into security control 1128.
1141	Removed due to being better served as supporting information.
1142	Removed due to being better served as supporting information.
1147	Removed due to a merge of relevant content into security control 0820.
1148	Removed due to a merge of relevant content into security control 0821.
1153	Removed due to being better served as supporting information.

1154	Removed due to a merge of relevant content into security control 0888.
1159	Removed due to this activity being coordinated at the discretion of chief wardens within organisations.
1166	Removed due to duplication of intent of security control 1200.
1167	Removed due to duplication of intent of security control 1202.
1168	Removed due to being better served as supporting information.
1169	Removed due to duplication of intent of security control 1359.
1176	Removed due to a merge of relevant content into security control 0584.
1177	Removed as this decision should be left up to the information owner.
1180	Removed due to a merge of relevant content into security control 1178.
1190	Removed due to being better served as supporting information.
1197	Removed due to duplication of intent of security control 1202.
1201	Removed due to not having a strong reason to be retained.
1203	The fundamentals of risk management don’t need to be duplicated within this publication.
1204	The fundamentals of risk management don’t need to be duplicated within this publication.
1205	The fundamentals of risk management don’t need to be duplicated within this publication.
1206	The fundamentals of risk management don’t need to be duplicated within this publication.
1207	The fundamentals of risk management don’t need to be duplicated within this publication.
1208	The fundamentals of risk management don’t need to be duplicated within this publication.
1210	Removed due to duplication of activities that occur as part of the accreditation process.
1212	Removed due to duplication of intent of security control 0123.
1214	Removed due to being better served as supporting information.
1224	Removed due to being better served as supporting information.

1229	Removed due to being better served as supporting information.
1230	Removed due to being better served as supporting information.
1231	Removed as Suite B requirements are mandated by ASD rather than being guidance.
1248	Removed due to a merge of relevant content into security control 1247.
1266	Removed due to a merge of relevant content into security control 1247.
1303	Removed due to a merge of relevant content into security control 1301.
1305	Removed due to duplication of intent of security control 0988.
1307	Removed due to duplication of intent of security control 1195.
1328	Removed due to relating to PEAP and EAP-TTLS which are not recommended for 802.1X authentication on wireless networks.
1329	Removed due to relating to PEAP and EAP-TTLS which are not recommended for 802.1X authentication on wireless networks.
1331	Removed due to a merge of relevant content into security control 1454.
1333	Removed due to being better served as supporting information.
1336	Removed due to duplication of intent of security control 0631.
1337	Removed due to duplication of intent of security control 1299.
1340	Removed due to duplication of intent of security control 0922.
1342	Removed due to duplication of intent of security control 0290.
1343	Removed due to being better served as supporting information.
1344	Removed due to a merge of relevant content into security control 1405.
1345	Removed due to duplication of intent of security control 0631.
1347	Removed due to being better served as supporting information.
1353	Removed as compliance with mandatory PSPF requirements are articulated within the PSPF.
1354	Removed as compliance with mandatory PSPF requirements are articulated within the PSPF.

1355	Removed as compliance with mandatory PSPF requirements are articulated within the PSPF.
1356	Removed due to a merge of relevant content into security control 0240.
1358	Removed due to a merge of relevant content into security control 0157.
1360	Removed due to a merge of relevant content into security control 0361.
1367	Removed due to duplication of intent of security control 1195.
1379	Removed due to a change from a compliance culture to a risk management culture.
1391	Removed due to a merge of relevant content into security control 1392.
1393	Removed due to duplication of intent of security control 0140.
1397	Removed due to a merge of relevant content into security control 1396.
1398	Removed due to being better served as supporting information.
1406	Removed due to not having a strong reason to be retained.
1411	Removed due to being better served as supporting information.
1413	Removed due to a merge of relevant content into security control 0843.
1415	Removed due to a merge of relevant content into security control 1414.
1421	Removed due to duplication of intent of security control 1420.
1423	Removed due to a merge of relevant content into security control 0401.
1440	Removed due to a merge of relevant content into security control 1439.
1442	Removed due to being better served as supporting information.
1443	Removed due to a merge of relevant content into security control 1322.
1444	Removed due to a merge of relevant content into security control 1324.
1447	Removed due to duplication of intent of security control 1139.
1455	Removed due to being better served as supporting information.
1459	Removed due to a merge of relevant content into security control 0100.

1462	Removed due to a merge of relevant content into security control 1461.
1463	Removed due to a merge of relevant content into security control 1461.
1465	Removed due to being better served as supporting information.
1466	Removed due to being better served as supporting information.
1475	Removed due to a merge of relevant content into security control 0472.
1476	Removed due to a merge of relevant content into security control 0473.
1477	Removed due to a merge of relevant content into security control 0476.

Modification of security controls

In reviewing security controls from the previous release of the ISM, the use of compliance-based language, such as 'should' and 'must', was removed from security controls. This resulted in the modification of 687 security controls. In addition, a number of security controls were modified to merge in content from other security controls, clarify their intent or clarify the classifications that they were applicable to.

Addition of security controls

In reviewing security controls from the previous release of the ISM, the following criteria were used:

- Does a security control require additional clarification?
- Would a security control be better served by being two or more distinct security controls?
- Does supporting information exist that isn't related to a security control?
- Do gaps exist in security control coverage?

As a result of this review, 63 security controls were added.

The security controls that were added are listed in the following table.

Security Control	Reason
1478	Added to clarify the intended responsibilities of a CISO
1479	Added as a result of a split of security control 0385.
1480	Added to address a gap in guidance on sharing peripherals between official or classified systems and highly classified systems.
1481	Added to address a gap in guidance on organisation-owned mobile devices.
1482	Added to address a gap in guidance on organisation-owned mobile devices.

1483	Added to address a gap in guidance on the use of the latest versions of software on important servers.
1484	Added to address a gap in guidance on the hardening of web browsers.
1485	Added to address a gap in guidance on the hardening of web browsers.
1486	Added to address a gap in guidance on the hardening of web browsers.
1487	Added to address a gap in guidance on the hardening of Microsoft Office.
1488	Added to address a gap in guidance on the hardening of Microsoft Office.
1489	Added to address a gap in guidance on the hardening of Microsoft Office.
1490	Added to address a gap in guidance on the use of application whitelisting on important servers.
1491	Added to address a gap in guidance on the use of script execution engines in operating systems.
1492	Added to address a gap in guidance on the use of exploit protection functionality in modern operating systems that no longer support the use of EMET.
1493	Added to address a gap in guidance on the maintenance of an inventory of software and hardware that may require patching of security vulnerabilities.
1494	Added to address a gap in guidance on operating system and firmware patching.
1495	Added to address a gap in guidance on operating system and firmware patching.
1496	Added to address a gap in guidance on operating system and firmware patching.
1497	Added to address a gap in guidance on operating system and firmware patching.
1498	Added to address a gap in guidance on operating system and firmware patching.
1499	Added to address a gap in guidance on operating system and firmware patching.
1500	Added to address a gap in guidance on operating system and firmware patching.
1501	Added to address a gap in guidance on the use of unsupported workstations, servers and ICT equipment.
1502	Added as a result of a split of security control 0561.
1503	Added to mirror security control 1508 but for standard users instead of privileged users.

1504	Added to address a gap in guidance on multi-factor authentication.
1505	Added to address a gap in guidance on multi-factor authentication.
1506	Added to address a gap in guidance on disabling the use of SSH version 1.
1507	Added to address a gap in guidance on privileged access to systems and resources.
1508	Added to address a gap in guidance on privileged access to systems and resources.
1509	Added to address a gap in guidance on privileged access to systems and resources.
1510	Added to address a gap in guidance on data backups.
1511	Added to address a gap in guidance on data backups.
1512	Added to address a gap in guidance on data backups.
1513	Added to address a gap in guidance on data backups.
1514	Added to address a gap in guidance on data backups.
1515	Added to address a gap in guidance on data backups.
1516	Added to address a gap in guidance on data backups.
1517	Added to address a gap in guidance on the destruction of microform.
1518	Added to address a gap in guidance on mitigating denial-of-service attacks.
1519	Added to support the consideration and documentation of security risks associated with systems that are connected to gateways.
1520	Added to address a gap in guidance on the management of gateways.
1521	Added to address a gap in guidance on the separation of data flows in Cross Domain Solutions (CDS).
1522	Added to address a gap in guidance on the separation of data flows in CDS.
1523	Added to address a gap in guidance on the logging of security-related events for CDS.
1524	Added to address a gap in guidance on content filters in CDS.
1525	Added to address a gap in guidance on system owners registering systems with their accreditation authority.

1526	Added to address a gap in guidance on system owners monitoring security risks and the effectiveness of security controls throughout the lifetime of their systems.
1527	Added to address a gap in guidance on firewalls between official systems and public network infrastructure.
1528	Added to address a gap in guidance on firewalls between classified systems and public network infrastructure.
1529	Added to address a gap in guidance on the use of highly classified outsourced cloud services.
1530	Added to recognise the three layers of physical security for assets. For example, the facility, the server/communications room and the security container/lockable commercial cabinet.
1531	Added to address a gap in guidance on the development of test plans as part of security assessments.
1532	Added as a result of a split of security control 0529.
1533	Added to address a gap in guidance on the development of a policy for the management of mobile devices within an organisation.
1534	Added to address a gap in guidance on the destruction of printer ribbons from printers and MFDs.
1535	Added as a result of a split of security control 0678.
1536	Added as a result of a split of security control 0987.
1537	Added as a result of a split of security control 0987.
1538	Added as a result of a split of security control 0420 due to different classifications that nationally releasability information can be used with.
1539	Added as a result of a split of security control 0269 due to different classifications that nationally releasability information can be used with.
1540	Added to address a gap in guidance on the use of Domain-based Message Authentication, Reporting and Conformance (DMARC).