The 2017 ISM Controls update from a Microsoft 365 perspective

Microsoft 365 and the 2017 ISM Controls

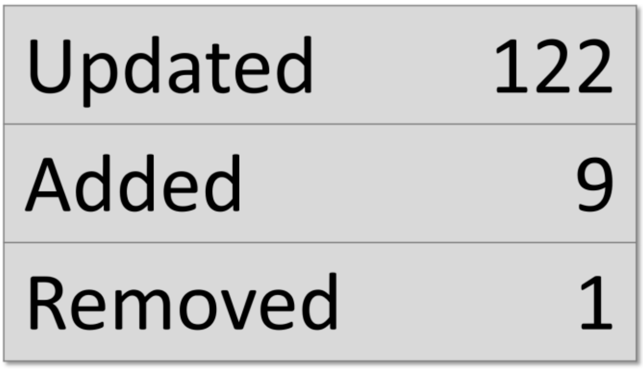
- Published on February 17, 2018
  https://www.linkedin.com/pulse/microsoft-365-2017-ism-controls-aaron-dinnage/

At the end of November, 2017, the Australian Signals Directorate released an update to the Information Security Manual controls. The ISM is “the standard which governs the security of government ICT systems”. It is held in high regard both inside and out of government alike, such that it's not uncommon to find private organizations leveraging the ISM to assist their own risk-based ICT decision making. So when the ISM gets an update it's important to dig in and understand the changes.

In this article, we'll take a tour around the noteworthy updates and examine them from the perspective of an organization that is adopting Microsoft 365. Microsoft 365 is of course shorthand for Microsoft's Office 365, Enterprise Mobility + Security (EM+S), and Windows 10 products. To learn more about the Microsoft 365 suite, you can check out my earlier article Unpacking Microsoft 365. And on the theme of ASD guidance alignment, I've also written about Microsoft 365 and the ASD Essential Eight, which looks at the suite from a slightly different angle and complements this article in a number of areas.

Overview

It's worth noting up front that this update is **not** a seismic shift in any sense, the overarching principles of the ISM have not changed and the updates that have been made are for the most part minor. However, this does represent a substantial improvement to the readability and clarity of the document.



Updated	122
Added	9
Removed	1

The majority of the 122 control changes in the 2017 ISM Controls Update are for readability and clarity, but some are more substantial. There are nine new controls, and one control has been removed altogether. It is the substantial updates, new, and removed controls that will be the focus of this article.

As we navigate through the changes I'll use chapter titles and section headings from the ISM to lay out this article, starting with ...

Backup Strategy

Part of the chapter “Business Continuity and Disaster Recovery Plans”, Backup Strategy has had some rewording that is not only a clarification, but particularly relevant for Software as a Service offerings such as Office 365 and EM+S.

The following text has been removed and replaced:

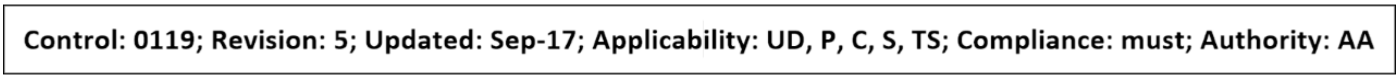
Removed:

Where practical, backups should be stored offline to mitigate the risk of agency data being unavailable due to compromise or deletion.

To accommodate modern cloud services the replacement text now elaborates that when backups are stored online, mitigations must be in place to address the risk to data.

“Mechanisms must be implemented to mitigate the risk of agency data being unavailable due to compromise or deletion. Such mechanisms include storing backups offline where practical. If backups are stored online, such mechanisms include … ”

Several suggested ways to mitigate data loss are then described. All of which are addressed in the delivery of Microsoft 365 services.


Control: 0119; Revision: 5; Updated: Sep-17; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA

The one control in this section is 0119, which has had the following line added to the control description:

“ensure that backups cannot be maliciously modified/corrupted or deleted without appropriate authorisation. **”**

This update shows an understanding that cloud services can be reliable and secure even if they go about achieving that in new and different ways. In the context of Microsoft 365 services, this is certainly true.

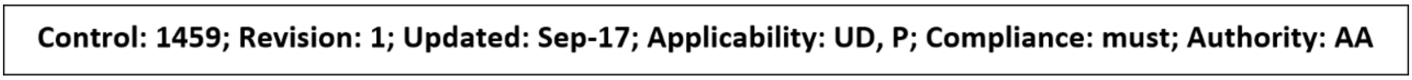
Microsoft 365 is able to safeguard customer data using a number of online backup techniques. You can read more about the Microsoft 365 customer controls and the approach used by Microsoft in my article Microsoft 365 and the Essential Eight.

Microsoft online services customers can read more about the resiliency and backup features of Office 365 in the white paper “Office 365 - Data Resiliency” which is available in the Microsoft Service Trust Portal (under Trust Documents, FAQs and White Papers).

Certification of cloud services

This section of the ISM speaks to the process by which cloud services get listed on the ASD Certified Cloud Services List (CCSL).

Office 365 is certified and listed on the CCSL, having completed two IRAP assessments to date, the most recent in mid-2017.


Control: 1459; Revision: 1; Updated: Sep-17; Applicability: UD, P; Compliance: must; Authority: AA

Control 1459 has been updated to remove the list of events that could trigger the need for re-certification to occur, and replaced them with the simple requirement that the process must occur “at least every two years”.

Office 365 continues to evolve and receive new products, features, and updates at a rapid cadence. And it's fair to say that cloud services providers are looking for ways to ensure continuous compliance, without a two year time lag.

In the meantime, IRAP reports are available to Microsoft online services customers through the Service Trust Portal (under Compliance Reports, GRC Assessment Reports). I'd strongly encourage you to take a look at the assessors comments and recommendations.

It will be interesting to see if, and how, this section changes in the future in response to DTA's recently released Secure Cloud Strategy, which I'll be writing an article about soon.

Cyber Security Incidents

Some small but significant changes have been made to this section to shift the focus from not just the prevention of incidents, but to include greater rigour around the detection of incidents. Also, the sources of data used in detection are called out for attention. This importantly differs from simply deploying tools for the detection of cyber security incidents, to ensuring that the right sources of data are available, configured, and leveraged properly.

Control: 0120; Revision: 3; Updated: Sep-17; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA

Control 0120 has been updated to reflect this shift of perspective, and now reads:

“Agencies must develop, implement and maintain data sources, procedures and tools to ensure that: •Any security alerts generated by systems are investigated. •Systems and data sources are able to be searched for key indicators of compromise including but not limited to IP addresses, domains and file hashes. ”

In the Office 365 context, this means not only turning on Audit Logging across the platform, but also exporting logs, directly ingesting data into an existing SIEM and/or taking up the security monitoring features within Microsoft 365 and across the broader Microsoft platform, such as Azure Security Center, Operations Management Suite, and Azure ATP when it launches later this year.

EM+S includes Microsoft Cloud App Security, a Cloud Access Security Broker (CASB), which leverages the audit data directly from Office 365 and other sources to provide tooling that addresses these requirements for Office 365 and other SaaS and on-premises environments.

Ultimately, it is important to not only understand the auditing and logging data held within the service, but also how to receive alerts, make decisions, and perform searches across it.

For further reading on this topic see “Office 365 - Auditing and Reporting features” which is available to Microsoft online services customers through the Service Trust Portal (under Trust Documents, FAQs and White Papers).

Posting personal information to online services

Prior to this update the ASD had encouraged all government staff to avoid putting the sort of information online that makes up a LinkedIn profile, or more importantly in this context, a user profile in Office 365. However, this ISM control has now been removed.

Removed:

Control: 0924; Revision: 1; Updated: Nov-10; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA

Personnel should avoid posting personal information, such as the following, on websites:

- past and present employment details
- personal details
- schools/institutions
- clubs/hobbies
- educational qualifications
- current work duties
- work contact details.

I've written about this in a separate article, looking at it from the perspective of using LinkedIn. However, this is of course also relevant for Microsoft 365.

Office 365 in particular receives a lot of user identity data through the identity synchronization tool Azure AD Connect. Citing concerns raised by the control above, some customers have limited the data synchronization attributes within Azure AD Connect and prevented them being populated into Office 365.

Having a complete user profile in Office 365 actually improves the usefulness of many of the tools within the service. For example, Office 365 Search is infused with user data which make results more relevant, this also applies to the built-in eDiscovery capabilities. Delve, Workflows, Dynamic Group membership, contact cards, and analytics are all driven by the user metadata present in the service. Exchange Online, SharePoint Online, Skype for Business, and Teams are all enhanced by rich user profiles. Restricting attribute synchronization into Office 365 consequently diminishes the value of all of these features.

With this ISM control now removed, organisations can relax that position and take greater benefit from Office 365 as a result.

PSPF Mandatory Mitigation Requirement Explained

The core of the changes to this chapter of the ISM are in broadening the guidance from the ASD Top Four to the new ASD Essential Eight. You'll find more information on the Top 4 and the Eight at the ASD web site in the publication Strategies to Mitigate Cyber Security Incidents.

I've also written an article about Microsoft 365 and the Essential Eight which looks at how organisations can apply the features of Microsoft 365 to address the Eight, but also how Microsoft addresses the requirements of the Eight in delivering the services.

Hardening SOE configurations

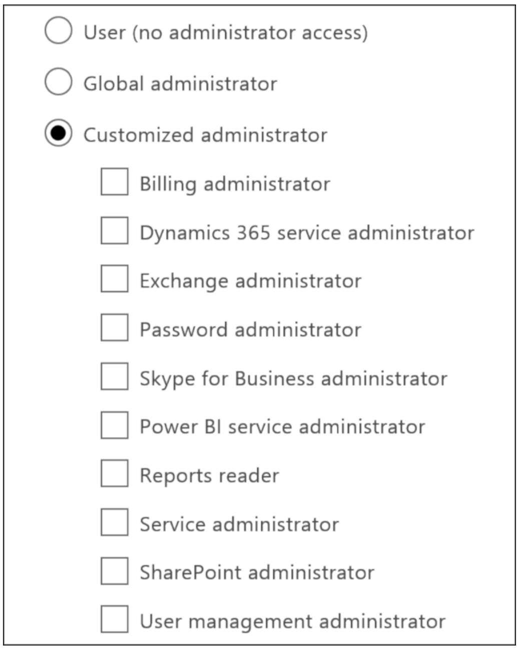
A new control has been added to directly target the practice of using Domain Admin accounts where Local Admin accounts would suffice.

Control: 1469; Revision: 0; Updated: Sep-17; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA

The control description reads:

"Unique domain accounts with local administrative privileges, but without domain administrative privileges, should be used for workstation and server management. "

Whilst this is not immediately applicable to an organisation adopting Microsoft 365, I've included it here because it is a good reminder that separate service and role based administration permissions should be assigned within Microsoft 365 services, such as Office 365. For example, instead of assigning the Global Administrator role, customers should look to utilise the various service administrator and functional roles.



○ User (no administrator access)

○ Global administrator

● Customized administrator

- □ Billing administrator
- □ Dynamics 365 service administrator
- □ Exchange administrator
- □ Password administrator
- □ Skype for Business administrator
- □ Power BI service administrator
- □ Reports reader
- □ Service administrator
- □ SharePoint administrator
- □ User management administrator

Permissions within the Microsoft 365 applications should also be used to avoid assigning unnecessary administrator privileges.

When it comes to how Microsoft implements administrator rights within Microsoft 365 services, there is a process known as 'Lockbox' that provides time-bound admin access and delivers a *no standing admin permissions* outcome. That is, no Microsoft engineer has an account with any standing access to administer the services.

Microsoft online services customers can find more information on the Lockbox process in the white paper "Office 365 - Administrative Access Controls" from the Service Trust Portal (under Trust Documents, FAQs and White Papers).

Organisations can implement their own Lockbox-like system of admin access control for both Office 365 and Azure using Privileged Identity Management. For on-premises there is the Privileged Access Management feature of Microsoft Identity Manager, which is included in Microsoft 365 Enterprise licensing.

Hardening application configurations

In this section, Control 1411 has been updated and a new control carved out.

Control: 1411; Revision: 1; Updated: Sep-17; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA

Control 1411 has been reworded as:

“Any security functionality in applications should be enabled and configured for maximum security. ”

This new wording indicates that just enabling some security functions is not enough, it could be *argued* that the configuration of the service should be to its *maximum security* capability.

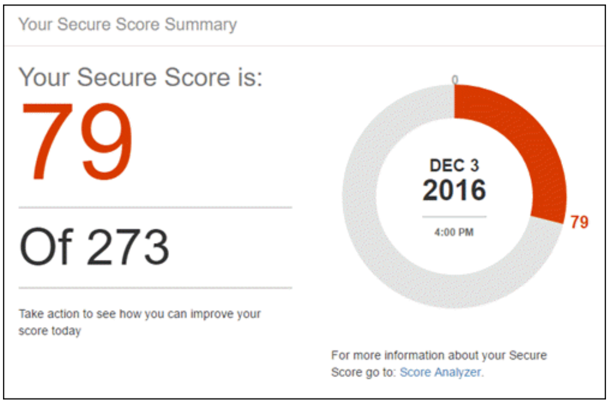
To help customers configure services for optimal security and compliance Microsoft has included Office 365 Secure Score and Compliance Manager.

Office 365 Secure Score

Secure Score analyses an Office 365 tenant's security posture against a wide range of features and Microsoft recommendations and then provides a very simple and easy to understand score which can be monitored and reported over time.

Customers can review all the recommendations that roll up into their score and establish actions to complete that will ultimately improve the score.

Available to all Office 365 Business Premium and Office 365 Enterprise (E1/E3/E5) customers today, Secure Score is accessible to administrators through the Admin Centre or by direct link.



Your Secure Score Summary

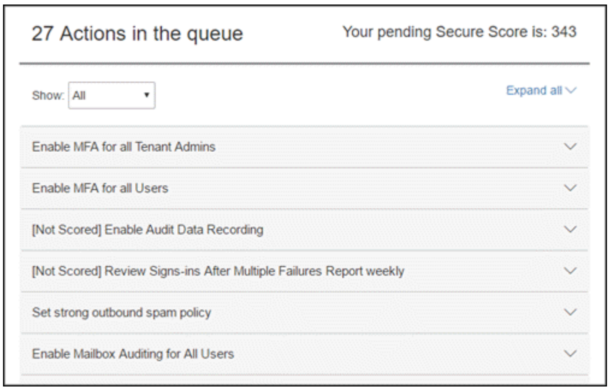
Your Secure Score is:

79

Of 273

Take action to see how you can improve your score today

For more information about your Secure Score go to: Score Analyzer.



27 Actions in the queue

Your pending Secure Score is: 343

Show: All

Enable MFA for all Tenant Admins

Enable MFA for all Users

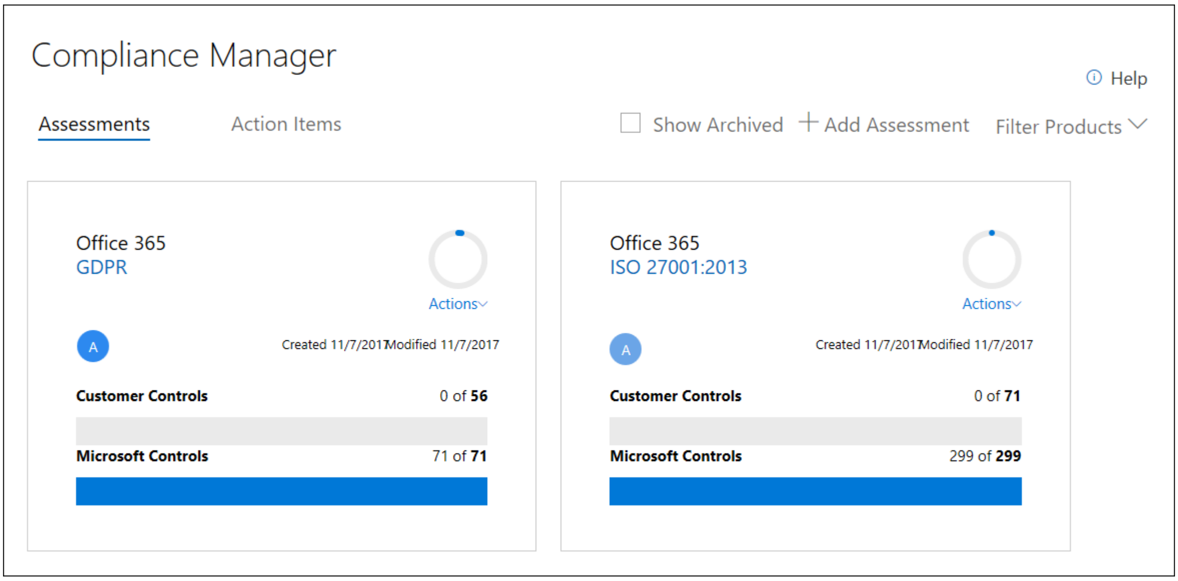
[Not Scored] Enable Audit Data Recording

[Not Scored] Review Signs-ins After Multiple Failures Report weekly

Set strong outbound spam policy

Enable Mailbox Auditing for All Users

Compliance Manager



Office 365
GDPR
Created 11/7/2017 Modified 11/7/2017
Customer Controls 0 of 56
Microsoft Controls 71 of 71

Office 365
ISO 27001:2013
Created 11/7/2017 Modified 11/7/2017
Customer Controls 0 of 71
Microsoft Controls 299 of 299

Currently rolling out to all Microsoft Online Services customers, Compliance Manager is a reporting tool built into the Service Trust Portal which allows customers to generate a report on their organizations compliance against common standards from around the world. The report is based specifically on that customers configuration of Microsoft Online Services like Office 365 and Azure.

At present, ISO 27001, ISO 27018, and GDPR compliance reports can be generated, with FedRamp and NIST 800-53 coming soon, and more to follow.

For ASD Essential Eight compliance please refer to my article on Microsoft 365 and the Essential Eight.

Control: 1470; Revision: 0; Updated: Sep-17; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA

Additional wording has been taken out of Control 1411 and moved into a new control. This related to disabling unrequired functionality and now forms ISM Control 1470.

*"*Any unrequired functionality in applications should be disabled. *"*

Microsoft 365 customers should ensure that only required components are enabled through a combination of correct user license allocation and tenant configuration to disable those product features. Each component will vary in its particular configuration, so consult product online documentation and reach out to your Microsoft account team or support team, or preferred Microsoft Gold Partner for further information.

Conversely, one of the great things about the feature controls within Microsoft 365 services is that organizations can selectively enable and disable products & features on a user-by-user basis. Online services customers should ensure they are at least testing unused and emerging products & features to avoid missing out on new functionality, new security measures, or new useful products.

Application Whitelisting

Control: 1471; Revision: 0; Updated: Sep-17; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA

This new Control 1471 simply mandates Application Whitelisting rules based on publisher certificates are to be scoped to both the publisher name and product name.

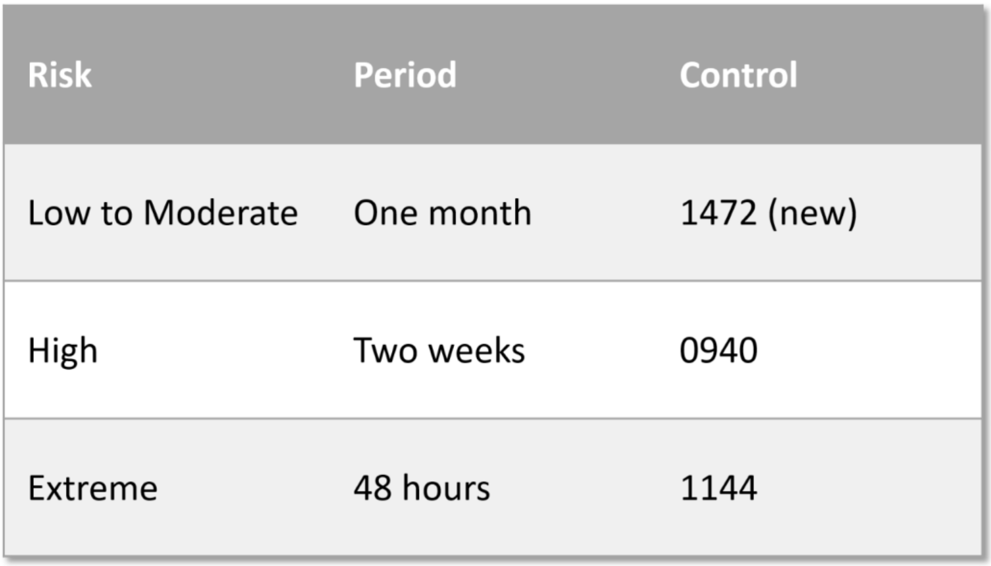
Windows 10 features a range of application whitelisting features including AppLocker, Device Guard, and Windows Defender Application Control. These can be deployed to meet a wide range of whitelisting scenarios, including the specific configurations described in the ISM.

For a detailed look of how Microsoft 365 can address Application Whitelisting requirements please refer to my existing article on Microsoft 365 and the Essential Eight.

Software Patching

Control: 1472; Revision: 0; Updated: Sep-17; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA

This new control is accompanied by updates to existing controls (1144, 0940) and relates to software patching timeframe requirements, summarised below:



Risk	Period	Control
Low to Moderate	One month	1472 (new)
High	Two weeks	0940
Extreme	48 hours	1144

As with Application Whitelisting above, there is a detailed discussion on how Microsoft 365 addresses Software Patching requirements in my article on Microsoft 365 and the Essential Eight and further information can be found in the IRAP reports that are available to Microsoft online services customers through the Service Trust Portal (under Compliance Reports, GRC Assessment Reports).

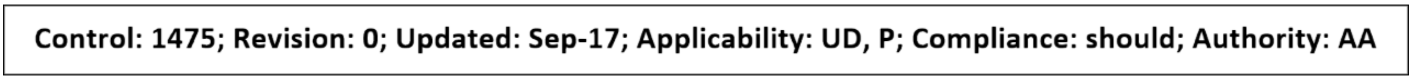
Cryptography

It's important to note when talking about Cryptography that whatever the standard is today, it will change in the future. Cryptographic standards are always marching forward to stay one step ahead of the attacks against them.

I'll limit the discussion below to details up to **Protected** classification and omit detail relating to highly classified information (**Confidential**, **Secret**, and **Top Secret**) as these are not within the scope of Office 365 and EM+S. Simply note that additional controls take effect at **Confidential** security classification and above but that the following is appropriate for **Unclassified DLM** and **Protected**.

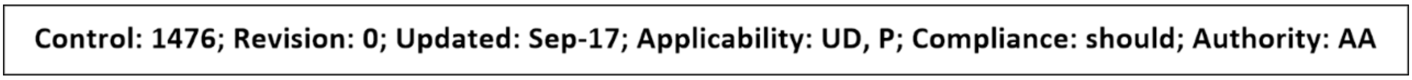
ASD Approved Cryptographic Algorithms

This section alone contains 3 of the 9 new controls that were added in the 2017 ISM Controls Update. Each new control is designed to add a recommended practice over and above an existing minimum requirement for encryption key lengths. I would expect over time to see the recommendation become the minimum and new recommendations for larger key lengths and new algorithms come in.



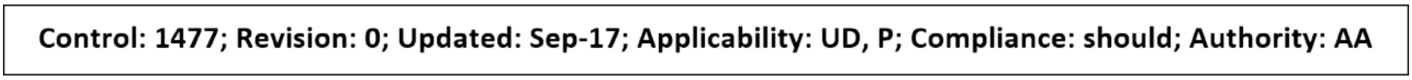
Control: 1475; Revision: 0; Updated: Sep-17; Applicability: UD, P; Compliance: should; Authority: AA

“Agencies using DH for the approved use of agreeing on encryption session keys should use a modulus of at least 2048 bits. **”**



Control: 1476; Revision: 0; Updated: Sep-17; Applicability: UD, P; Compliance: should; Authority: AA

“Agencies using DSA for the approved use of digital signatures should use a modulus of at least 2048 bits. **”**



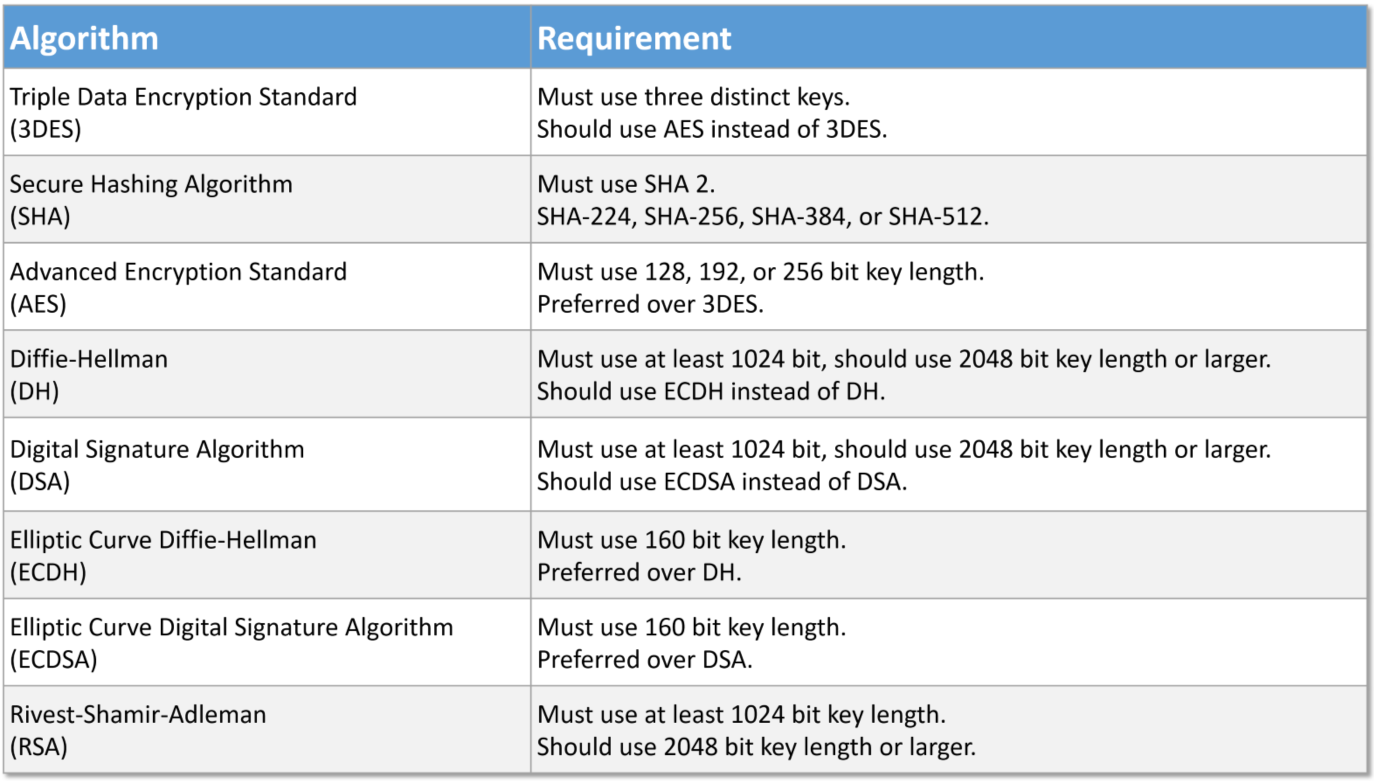
Control: 1477; Revision: 0; Updated: Sep-17; Applicability: UD, P; Compliance: should; Authority: AA

“Agencies using RSA, both for the approved use of digital signatures and passing encryption session keys or similar keys, should use a modulus of at least 2048 bits. **”**

The related controls to the above new controls are 0472, 0473, and 0476 respectively, they are present on the same pages as these controls in the ISM, however none of those controls were updated in the 2017 Controls release.

Controls 1054 and 0480 have been updated to require SHA-2 hashing algorithms and 3DES with three distinct keys, respectively.

Summary of updated cryptographic algorithm requirements (UD/P)



Algorithm	Requirement
Triple Data Encryption Standard (3DES)	Must use three distinct keys. Should use AES instead of 3DES.
Secure Hashing Algorithm (SHA)	Must use SHA 2. SHA-224, SHA-256, SHA-384, or SHA-512.
Advanced Encryption Standard (AES)	Must use 128, 192, or 256 bit key length. Preferred over 3DES.
Diffie-Hellman (DH)	Must use at least 1024 bit, should use 2048 bit key length or larger. Should use ECDH instead of DH.
Digital Signature Algorithm (DSA)	Must use at least 1024 bit, should use 2048 bit key length or larger. Should use ECDSA instead of DSA.
Elliptic Curve Diffie-Hellman (ECDH)	Must use 160 bit key length. Preferred over DH.
Elliptic Curve Digital Signature Algorithm (ECDSA)	Must use 160 bit key length. Preferred over DSA.
Rivest-Shamir-Adleman (RSA)	Must use at least 1024 bit key length. Should use 2048 bit key length or larger.

The ISM Controls section on protecting highly classified information has only received minor updates, nothing functional.

The ISM already speaks to quantum computing and it's potential to alter the landscape of encryption techniques used. This is due to the ability for quantum computers to solve the traditionally difficult problems that underpin many of the mainstream encryption technologies in use today, making it much simpler to break them. In the meantime, there remains other things that continue to challenge encryption standards, such as advancements in traditional computer processor speeds, algorithm breakthroughs, and the discovery of exploitable weaknesses in existing cryptographic implementations. All of these things make encryption a moving target, one that future ISM revisions will no doubt continue to update around.

If we consider these updates in the context of Microsoft 365, we find that the online services meet them already. For example, Microsoft 365 meets these requirements in user sessions, provides customer-managed encryption technologies that meet these requirements, and further implements these requirements internally in the encryption of data in transit and at rest within the Microsoft data centre network. This shouldn't really be a surprise, as Microsoft is an active participant in the encryption community, working with government and industry to stay at the leading edge.

One example of how Microsoft delivers strong encryption is through Azure Information Protection and the underlying Azure RMS implementation that leverages the following cryptographic algorithms:

- AES (128 & 256 bit) for content encryption.
- RSA (2048 bit, optional legacy 1024 bit) for content key protection.
- SHA (256 bit) for certificate signing.

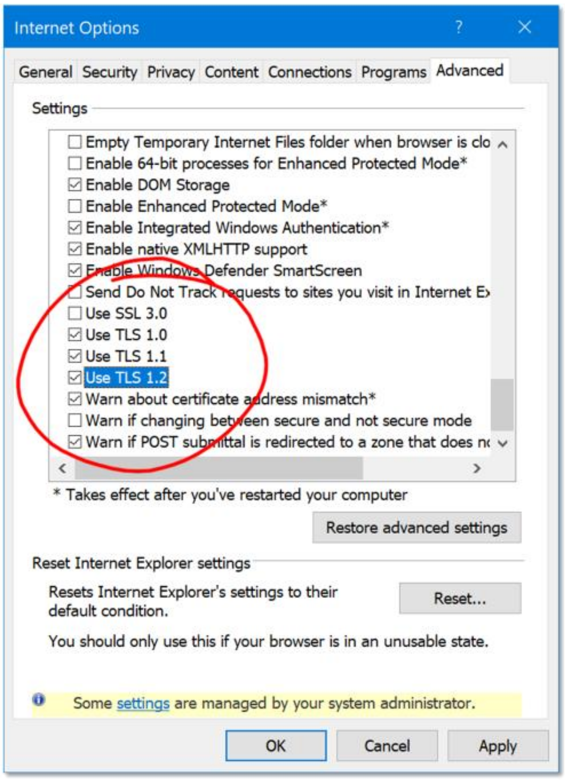
For client connectivity, TLS encryption is utilised across Microsoft 365. Customers can validate client connection encryption protocols and algorithms at these links:

- Office 365 Portal

- Exchange Online
- SharePoint Online / OneDrive for Business
- Skype for Business (SIP)
- Skype for Business (Web)
- Exchange Online Protection

These links utilise Qualys SSL Labs and SSL-Tools.net to test web and mail servers respectively. You can use these services to test any other Microsoft online service URL for compliance.

TLS 1.2 is supported and preferred, but customers need to explicitly disable support for earlier versions of TLS if they didn't want their endpoints to use them. Whilst the ISM only requires TLS 1.0 or above (and forbids SSL), it has become clear recently that TLS 1.0 should not be used, and I expect the next update to the ISM will move the requirement to TLS 1.2.



□ Empty Temporary Internet Files folder when browser is clo
□ Enable 64-bit processes for Enhanced Protected Mode*
☑ Enable DOM Storage
□ Enable Enhanced Protected Mode*
☑ Enable Integrated Windows Authentication*
☑ Enable native XMLHTTP support
☑ Enable Windows Defender SmartScreen
□ Send Do Not Track requests to sites you visit in Internet E
□ Use SSL 3.0
☑ Use TLS 1.0
☑ Use TLS 1.1
☑ Use TLS 1.2
☑ Warn about certificate address mismatch*
□ Warn if changing between secure and not secure mode
☑ Warn if POST submittal is redirected to a zone that does n

* Takes effect after you've restarted your computer

Resets Internet Explorer's settings to their default condition.

You should only use this if your browser is in an unusable state.

Some settings are managed by your system administrator.

In March of 2018, Microsoft will end support for earlier versions of TLS and only support TLS 1.2 for connections in *and* out of Office 365 going forward. You can read more about this decision in the support article "Preparing for the mandatory use of TLS 1.2 in Office 365".

The above links and further information on how Microsoft 365 works internally can be found in the white paper "Microsoft Cloud - Encryption", which is available to Microsoft online services customers through the Service Trust Portal (under Trust Documents, FAQs and White Papers).

If you're performing a Threat & Risk Assessment or investigating how Microsoft 365 can meet your obligations under the ISM then I'd highly recommend using the above white paper as a first port of call for all things encryption, and follow up with your Microsoft account team to arrange more detailed discussions.

Miscellaneous

There are 2 other new controls which I didn't mention above because they don't have direct relevance to Microsoft 365, but which I'll list here for completeness.

Control: 1473; Revision: 0; Updated: Sep-17; Applicability: C, S, TS; Compliance: must; Authority: AA

“Privileged users must use a dedicated workstation when performing privileged tasks. ”

Control: 1474; Revision: 0; Updated: Sep-17; Applicability: C, S, TS; Compliance: must; Authority: AA

“Agencies must only allow management traffic to originate from network zones that are used to administer systems and applications. ”

As both of the above controls relate to **Confidential** security classification and above I've not spoken to them here. Additionally, they are quite straightforward requirements whose inclusion in the ISM just makes good sense.

Finally, there is one control that I believe needs an update but didn't get one...

Control: 1389; Revision: 0; Updated: Feb-14; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA

Control 1389 has not been updated since its introduction in February 2014. The control reads:

“Email and web content entering a security domain should be automatically run in a dynamic malware analysis sandbox to detect suspicious behaviour. ”

By 2016, as much as 97% of malware was already polymorphic (source: Webroot). That is, almost all of the malware being deployed is of a type that routinely evades traditional anti-malware engines but may still be detected by sandboxing mechanisms referred to in this control.

In early 2014, sandboxing content in this way was complex and expensive, but now cloud vendors are able to leverage enormous compute power in their datacentres to deliver sandboxing services on email and file content in a simple and cost effective way.

Control 1389 is specifically calling out a readily available mechanism to address the rise of polymorphic malware, and so this control needs to be updated to “**must**” compliance, not “**should**” as it is today. In other words, the malware game is changing and our standards need to change with it.

In a Microsoft 365 context, Office 365 Advanced Threat Protection sandboxes links and attachments in email, and in files in SharePoint Online, OneDrive for Business, and Microsoft Teams.

As we've seen earlier there has also been a shift towards post-breach detection and remediation. To that end, Windows 10 Advanced Threat Protection is directly relevant for its ability to roll-up the data feeds and management of Windows Defender features and integrate preventative protection, post-breach detection, investigation and response. This lands in a single security portal which can view and manage the security feeds and events across an organisation.

Windows 10 ATP integrates with Office 365 ATP to provide wholistic coverage from cloud to desktop, and thanks to the recent Hexadite acquisition we'll soon see automated remediation across those platforms to reduce the burden on IT Security Operations.

Conclusion

Microsoft 365 services fare particularly well in light of the updated controls. The ISM is now more accommodating of cloud computing in general, and specifically improves the standing of SaaS services. We can see that Microsoft 365 has evolved its security posture in the same direction the ISM has evolved. This shouldn't really be a surprise, Microsoft works closely with governments around the world to ensure Office 365, EM+S, and Windows maintain their reputation for both compliance and security excellence.

Through the combination of Office 365 and EM+S, Microsoft has a comprehensive security and compliance offering for cloud services, and through the integration with Windows 10 an end-to-end solution for the modern workplace.

Microsoft has technical specialists that can go into far greater detail on any of the areas discussed here. This is particularly true where an enterprise agreement is in place, such as that with Australian Government customers. To organise a deeper conversation please reach out to your Microsoft account team contact. Microsoft partners also have access to more detailed information and should reach out to their Microsoft One Commercial Partner team contact to arrange a deeper discussion on these topics.

Organizations that would like assistance in performing threat and risk assessments or accreditation against Microsoft 365 should reach out to their Microsoft account team, our cybersecurity specialists are working with customers right now in doing just that.

If you'd like to read more, the ISM documents and a change summary are available at the ASD website. Additionally, the Protective Security Policy Framework (PSPF) is a companion to the ISM and defines relevant implementation details relating to security classifications and protective markings, as well as risk management policy for ICT outsourcing & cloud.

On that topic, you'll find another recent article of mine talks specifically to those protective markings and how they apply to email. Again, there is relevance here to Microsoft 365.