Understanding the PROTECTED certification of Office 365

Office 365 and PROTECTED Certification: Part 1

- Published on September 3, 2018
  https://www.linkedin.com/pulse/office-365-protected-certification-part-1-aaron-dinnage/

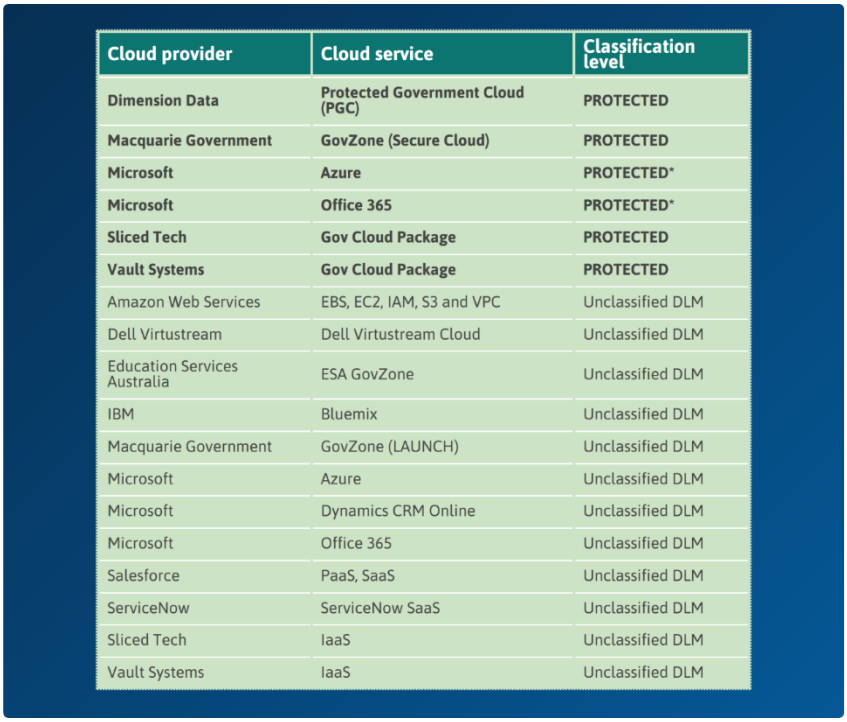
April 3rd, 2018 was a milestone in the Australian cloud computing journey. On the same day that Microsoft launched two new Azure regions in Canberra, both Azure and Office 365 were certified to handle government PROTECTED classified information across the Melbourne, Sydney, and Canberra data centre regions.

Both Microsoft Azure and Office 365 are the first hyperscale cloud services to be added to the Australian Government Certified Cloud Services List (CCSL) at PROTECTED certification level. Office 365 is also the first Software as a Service, or SaaS, cloud platform to receive PROTECTED certification.

More recently, on August 22nd, 2018 the Digital Transformation Agency announced they would be the first Australian Government agency to deploy Office 365 for PROTECTED email and collaboration, taking advantage of the recent certification uplift.

This is not only a fantastic outcome for the agency, but also demonstrates a commitment to the risk-based approach to information security, and to the Secure Cloud Strategy that DTA themselves published earlier in the year.

With the momentum building around PROTECTED Office 365 it's past due for me to break down the certification and configuration recommendations that support it!



Cloud provider	Cloud service	Classification level
Dimension Data	**Protected Government Cloud (PGC)**	**PROTECTED**
Macquarie Government	**GovZone (Secure Cloud)**	**PROTECTED**
Microsoft	**Azure**	**PROTECTED***
Microsoft	**Office 365**	**PROTECTED***
Sliced Tech	**Gov Cloud Package**	**PROTECTED**
Vault Systems	**Gov Cloud Package**	**PROTECTED**
Amazon Web Services	EBS, EC2, IAM, S3 and VPC	Unclassified DLM
Dell Virtustream	Dell Virtustream Cloud	Unclassified DLM
Education Services Australia	ESA GovZone	Unclassified DLM
IBM	Bluemix	Unclassified DLM
Macquarie Government	GovZone (LAUNCH)	Unclassified DLM
Microsoft	Azure	Unclassified DLM
Microsoft	Dynamics CRM Online	Unclassified DLM
Microsoft	Office 365	Unclassified DLM
Salesforce	PaaS, SaaS	Unclassified DLM
ServiceNow	ServiceNow SaaS	Unclassified DLM
Sliced Tech	IaaS	Unclassified DLM
Vault Systems	IaaS	Unclassified DLM

In the screenshot above you can see the CCSL from August 2018, with Office 365 and Azure listed as both **Unclassified DLM** and as **PROTECTED** certified services.

This is an important achievement that has big implications for not only government organizations around the country, but any business that is looking to align with government security recommended practices.

In this two part series of articles we'll walk through the certification in detail.

Part 1 is all about context. We'll look at the Australian Government security classification system, the certification process, and what it means in a practical sense, as well as the implications for Office 365 customers.

In Part 2 we'll look at which components of the service are in and out of scope, and what features and configurations Microsoft are recommending customers utilise to meet their compliance objectives. I'll share recommendations on how to actually set up and run a PROTECTED Office 365 environment.

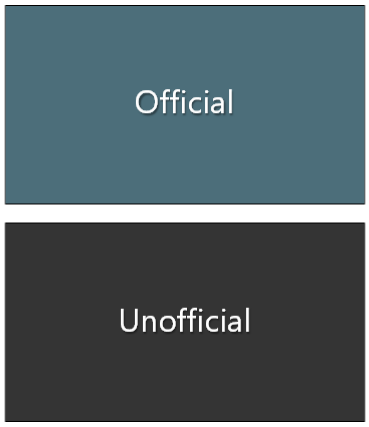
So, let's start by exploring the broader context of this major announcement…

The Australian Government Security Classification System

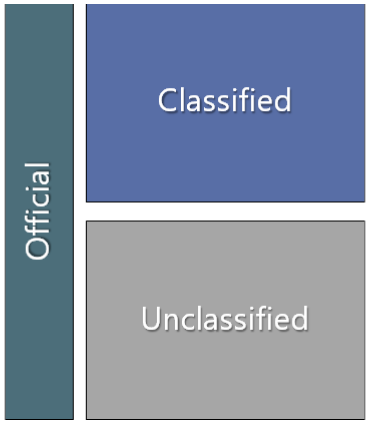
For those that don't regularly work with the Australian classification system, what follows is a brief explanation for reference. If you do, then by all means feel free to skip ahead…

We've all heard phrases like "*it's top secret*" and "*that's classified*" in TV and movies, but these are real terms with a meaning that is well defined in the government information security space. In this context, it's important to clarify terms like "unclassified" and "protected" to understand what this latest certification outcome really means.

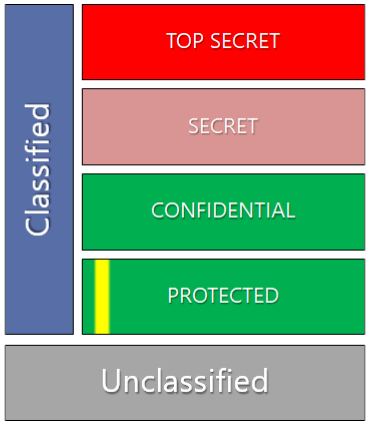
The Protective Security Policy Framework (PSPF) defines the classification system, as well as the framework for securing government information. The Information Security Manual (ISM) then defines the security controls that are appropriate for information systems that handle official material. There is a handy guide to the Australian Government Security Classification System available as part of the PSPF, which includes a thorough explanation and links to further information. I'll try to summarise the relevant aspects below.



At the broadest perspective, information is considered either **Official** or **Unofficial**. Where Official information covers all the material used in the operation of government agencies. And Unofficial information is not related to government business and is therefore not a part of the classification system. For example, an Unofficial item might be a personal email to a friend.

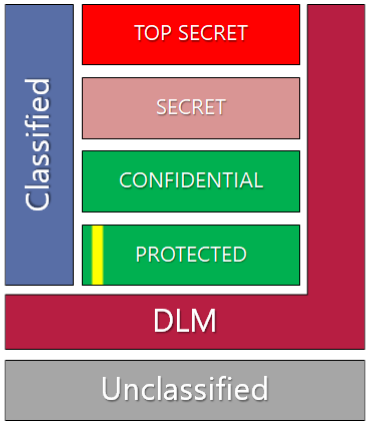


Official information is further categorized as either **Classified** or **Unclassified** depending on its security needs. Information that does not need increased security is termed Unclassified. Where as Classified and sensitive Official information may have legal, political, personal, or national security implications if released. This necessitates **Protective Markings**, which are a way of indicating that the content requires some additional considerations in its handling. We'll talk more about protective markings a little later.



There are four levels of security classification, corresponding to impact: **TOP SECRET**, **SECRET**, **CONFIDENTIAL**, and **PROTECTED**.

The bulk of the information handled by government on a day-to-day basis tends to be Unclassified, and doesn't need increased security. Those outside of government may have noticed **[SEC=UNCLASSIFIED]** in the email subject line from a government contact. This example tells you that the sender considers the content to be Unclassified (I've written about subject line markings here before). Unclassified information moves reasonably freely within government and doesn't need to be handled with additional care.



Some kinds of official information do need additional care, they may require what's called a **Dissemination Limiting Marker** (DLM). A DLM informs the reader of the particular sensitivity of the information.

There are five Dissemination Limiting Markers defined in the PSPF:

• **Sensitive -** Information that is subject to secrecy provisions, or where disclosure is limited or prohibited by legislation.

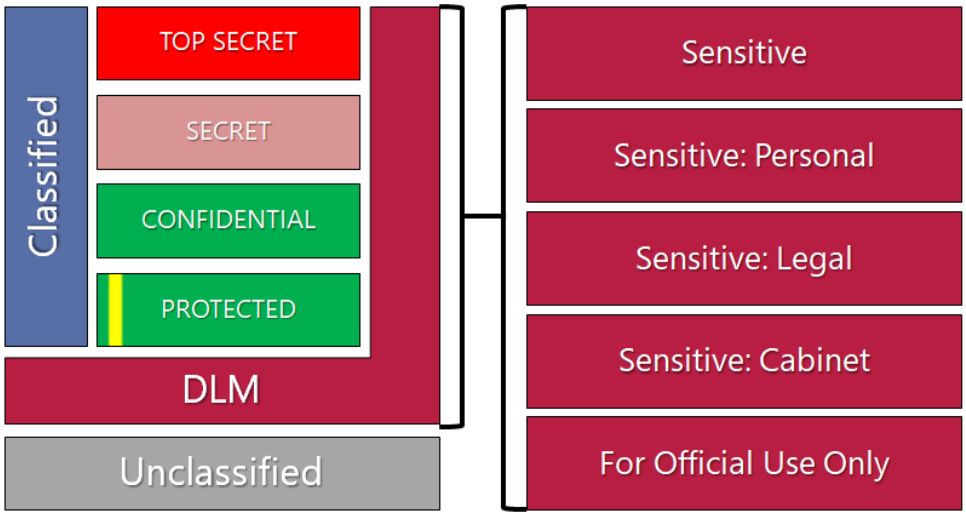
• **Sensitive: Personal -** Sensitive personal information as defined by the Privacy Act 1988.

• **Sensitive: Legal -** Information that may be subject to legal professional privilege.

• **Sensitive: Cabinet -** Any document submitted (or proposed to be submitted) to Cabinet, any official records of Cabinet, and any information that would reveal any of the deliberations, decisions, or matters submitted (or proposed to be submitted) to Cabinet is to have this DLM applied and be security classified as PROTECTED or higher.

• **For Official Use Only (FOUO) -** Unclassified information which could cause limited damage if compromised.

The *For Official Use Only* DLM and each of the classified types are aligned to different Business Impact Levels, ranging in severity with their potential to negatively impact on the national interest (or the interests of states and territories), organisations, or individuals.



As you can see above, a DLM can be applied in isolation of or in addition to a security classification.

Note: The PSPF is currently undergoing a significant revision which will simplify the Australian Government security classification system. The ISM is likewise being overhauled in parallel. Check back later when these changes land as I will be updating this material.

PROTECTED

PROTECTED classified information could be expected to **cause damage** to the national interest, organisations, or individuals. Including (amongst other things), up to a $10 billion loss to the economy, damaging or disrupting significant state or territory infrastructure, or leading to serious harm or potentially life-threatening injury to an individual.

"It's classified. I could tell you, but then I'd have to kill you." - **Maverick**.

It's not quite as dramatic as that line from the film Top Gun, but as we've seen, it's pretty serious. Misusing or inappropriately disclosing security classified material is a crime and could result in spending time in prison, so it's no joke. Should PROTECTED material leak, bad things can happen. People who deal with this kind of information require baseline security clearance and organizations must do significantly more to secure PROTECTED information than they would for Unclassified.

"The PROTECTED security classification should be used when the compromise of the confidentiality of information could be expected to cause damage to the national interest, organisations or individuals." - **PSPF**

Both the ISM and the PSPF list additional security controls for PROTECTED information and PROTECTED information systems, over and above those for Unclassified / DLM. For instance, there are over 40 additional ISM controls that Office 365 was evaluated against on top of the controls for Unclassified DLM certification.

As we've seen above, PROTECTED certification is not just a step up from Unclassified DLM, it is a different category of information altogether. PROTECTED material is *classified* material.

The Certified Cloud Services List (CCSL)

Back in April 2015, the CCSL was introduced to assist government organizations to choose cloud services that had demonstrated their suitability to handle official government information. Up until March 2017, all the services on the CCSL were listed as “Unclassified DLM”. That is, they were able to handle Official information including Unclassified and DLM, but not Classified information. At the time, no services had been certified at PROTECTED.

The process for getting listed on the CCSL begins with completing an IRAP assessment, engaging a specially trained security professional who can evaluate services against the controls of the ISM. But getting an IRAP assessor to review your platform is only the first step. You then need to work with the Australian Cyber Security Centre (ACSC) as they analyse the assessment and request clarifications, explanations, and even **changes** to your service before they certify it.

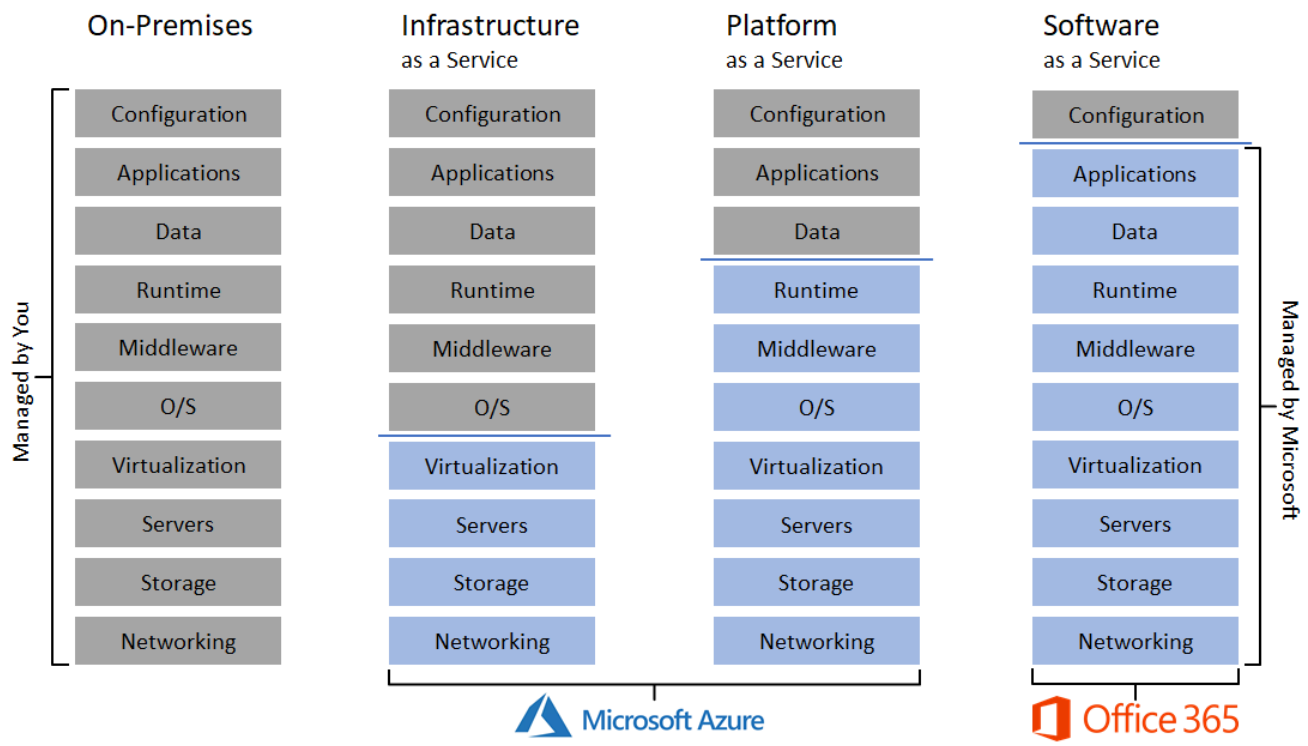
It can take months, or even years of effort before a service moves from having completed an IRAP assessment to being certified at the recommended classification level, and there is no guarantee that a successful IRAP assessment will even result in certification at all! The process is documented on the ACSC website, and summarised in the publication Anatomy of a Cloud Certification, which is quite a great reference. I've also summarised the Assessment, Certification, and Accreditation process in my recent discussion on how the DTA were the first to deploy Office 365 PROTECTED configuration in Australian Government. So if you'd like to understand that process further I'd recommend checking it out.

Suffice to say, it's a long road to certification. And once it has been achieved it starts all over again. Services must be continuously reviewed and re-certified to ensure ongoing compliance.

The result is that the CCSL is the **only** place to find Australian Government certified cloud services. If it's not on the CCSL it's either not **certified**, or it's not **cloud**.

Let's unpack that a little bit…

Australian Government broadly aligns with the NIST definition for cloud, which defines the three service models, their essential characteristics, and the various deployment models that constitute 'cloud'.



Each of the three service models are represented on the CCSL today:

• **Infrastructure as a Service (IaaS)** - Customers can host virtual machines on the cloud service provider's hypervisor platform. The customer is responsible for everything that operates inside the VM, and so retains the most control of the platform, but also the most effort to maintain it. As the simplest form of cloud service, IaaS is the most common service model on the CCSL today. Microsoft Azure can host IaaS workloads.

• **Platform as a Service (PaaS)** - Customers can host applications, written or modified to run on that cloud service provider's application stack. The benefit of PaaS over IaaS is that the customer is no longer responsible for management of the underlying application stack, just the application itself. It's more cost effective, scalable, and responsive. Microsoft Azure can also host PaaS workloads.

• **Software as a Service (SaaS)** - Customers subscribe to an application service, or suite of services, provisioned, maintained, and provided directly from the cloud service provider. In this model, configurability is limited to what each application allows. Microsoft Office 365 is a SaaS service, and at the time of writing is the only SaaS that is PROTECTED certified.

The definition further provides for different hosting models, including:

• **Private cloud** - dedicated to a single customer.

• **Community cloud** - dedicated to a shared community of customers.

• **Public cloud** - not limited to a single customer or community.

• **Hybrid cloud** - stretched across multiple clouds.

Both Microsoft Azure and Office 365 are public cloud services, which offers the greatest scale and efficiency over the other hosting models. Azure and Office 365 cover the full range of service models, and are capable of also being leveraged in hybrid configurations with existing on-premises infrastructure and applications.

Whilst not part of the NIST definition back in 2011, the term hyperscale has gained prominence in the industry and is used to describe only the largest of cloud services which can seamlessly grow in capacity to match customer demands. It is commonly accepted that Microsoft is one of a small number of global providers that can deliver a hyperscale cloud. As such, Microsoft is the only hyperscale cloud service provider to offer a PROTECTED certified cloud service in Australia today. The benefit to customers is unmatched scale, range of services, and cost effectiveness.

When it comes to qualifying as a cloud service provider on the CCSL, there is a question of eligibility. It's fashionable, for example, for traditional hosting providers to claim they are providing a "cloud" service, when in reality their offering doesn't exhibit even the first of the NIST defined cloud characteristics: ***On-demand self-service***

"A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider." - **NIST**.

If your talking to a vendor who claims to have their own PROTECTED cloud, and it's not on the list, you should challenge them to explain that statement. Perhaps what they are offering you is not actually a cloud service, or it's not actually certified. And as we've discussed, an IRAP assessment is only the first step…

Why is the CCSL so important?

The CCSL is the formal recognition that a cloud service provider not only meets the definition of a cloud service, but has an offering that is suitable for Australian government organizations and all that entails. If a service is not on the CCSL, it's a case of *buyer beware*.

Knowing that all of the certified providers have gone through the same process to get listed, gives consumers a very high degree of confidence in those platforms.

And this really highlights a concept that Microsoft talks about a lot, and that customers are realising as they investigate the market, that not all clouds are created equal. It's the realisation that "the cloud" is not one thing. The definition of cloud leaves a lot of room for vendors to implement wildly different services. The CCSL is what tells a customer whether the cloud they are looking at is appropriate for government use or not.

Office 365 and the CCSL

Office 365 has been listed on the CCSL since its inception in April of 2015. Back then, both Microsoft Azure and Office 365 received Unclassified DLM certification. A subsequent effort was undertaken to renew certification not only at the Unclassified DLM level, but to move both Azure and Office 365 up to the PROTECTED classification level.

That effort resulted in a favourable IRAP assessment that has been published and available for Microsoft customers to download and review since July, 2017. Microsoft customers can find it on the Service Trust Portal.

When cloud providers achieve PROTECTED level certification it is because they've **invested significantly** to make that happen. Every cloud provider on the CCSL has undertaken substantial work at the physical facilities, hardware, personnel, networking, process, policy, and software layers. There is also a rigorous

engagement undertaken with ACSC to ensure every detail is understood and validated against the strict requirements of the classification. It is not easy, it is not quick, it is not to be taken lightly. But it does demonstrate to every customer, government or private sector, that the cloud service provider is secure, serious, and invested.

Every cloud service provider on the CCSL should be proud of what they have achieved. And every customer should be confident that these providers have capable, secure, and compliant offerings.

As someone who's been close to Microsoft's efforts around Office 365 certification, I've seen what it takes.

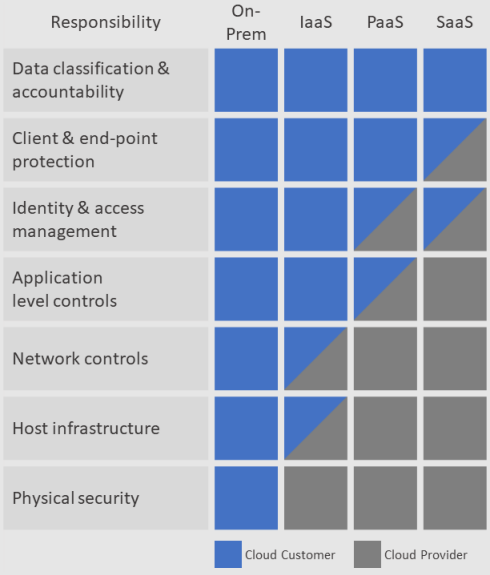
Office 365 didn't go from zero to PROTECTED overnight however, it benefitted from Microsoft's global commitment to security, compliance, and privacy. Being aligned with global and regional standards such as ISO 27001, 27017, and 27018, SSAE SOC 1 & 2, FISMA, FedRAMP, and others, has meant that Office 365 was already being delivered in Australia to an internationally recognised high level of security, compliance, and privacy. This in turn made the process of completing an IRAP assessment recommending PROTECTED certification somewhat easier. Though more work was needed to meet the unapologetically (and appropriately so!) high standards.

The Office 365 data centres within Australia have been lifted up to SCEC Zone 3 rated, in accordance with ASIO T4 Protective Security requirements and the PSPF, this ensures the appropriate physical security is in place to be able to house PROTECTED certified services. As an aside, the new Azure regions in Canberra are in SCEC Zone 4 rated facilities. These are amongst the most highly secured commercial facilities in Australia.

With PROTECTED certification, **existing** Office 365 tenancies are now able to be configured for handling PROTECTED information. There is no need to rebuild for PROTECTED, and there is no separate product or 'version' that needs to be deployed. It is the same service that was previously certified for Unclassified DLM, now certified for PROTECTED. This is another feature unique to the Microsoft offerings on the CCSL. Other cloud services have been specifically engineered or packaged to target PROTECTED workloads. It is a strength of the Microsoft platform that it can be configured *in-situ* to meet PROTECTED requirements.

Shared Responsibilities for Cloud Computing

Customers will need to configure Office 365 to meet their PROTECTED ISM control obligations, in line with Microsoft's Shared Responsibilities for Cloud Computing guidance. The shared responsibility model delineates the responsibilities of the cloud service provider (Microsoft) from those of the customer, and where each party has a responsibility.



In the diagram above you can see that for a SaaS product, such as Office 365, there is a significant amount of responsibility that lands solely with the cloud service provider. This of course is the great benefit of SaaS, and having Office 365 PROTECTED certified gives customers a lot of assurance that the bulk of the work is being handled directly by Microsoft in a manner consistent with the standards of the ISM. For these aspects of the service there is nothing more the customer needs to do, Microsoft has it covered.

The diagram also calls out that customers themselves are exclusively responsible and accountable for data classification. I don't think there is anything contentious or debatable about that. It's important that customers classify and label their content appropriately, regardless of using on-premises or cloud-based solutions. Within government, this is of course already a well established practice.

Office 365 provides customers with numerous ways to route and handle content based on its classification, and within the wider Microsoft 365 suite there is Azure Information Protection (AIP). AIP helps customers to consistently classify and label content, as well as encrypt, protect, track, and revoke access. We'll discuss AIP further in Part 2 of this article series.

The most interesting area of the responsibility diagram is the two items in the middle. Those of *shared responsibility*. These are areas where the service provider needs to work with the customer to establish a configuration that is appropriate.

The two shared responsibility areas for SaaS applications are *client & end-point protection*, and *identity & access management*. Customers that are already deploying workloads into SaaS applications will be familiar with the heavy focus on these areas from their cloud service provider. For customer's that haven't made a significant push into this space, or perhaps haven't been exposed to this way of thinking, these are concepts that require some deeper inspection.

Microsoft has been working with ACSC to develop a configuration that is appropriate for Australian government, which is the subject of the PROTECTED Office 365 consumer guide, and the main focus of Part 2 in this article series.

What's a “Consumer Guide”?

The CCSL refers to a so called 'Consumer Guide' for using Office 365 and Azure services at PROTECTED classification level. But this term is not a familiar term that is used or define elsewhere, so what are they talking about in this case?

The consumer guides are documentation Microsoft customers can use to help them configure their Azure and Office 365 environment to Microsoft's recommended practices for securing PROTECTED classified information.

There's nothing unusual about providing configuration guidance.

When Office 365 was certified at Unclassified DLM there was additional guidance on the recommended configuration. It wasn't called out on the CCSL page, which meant customers needed to enquire about it. The advice was simple, it was to use Active Directory Federation Services (ADFS) to control the authentication of users to Office 365 against Active Directory on-premises, in real-time.

As the ISM is a risk-based framework there is no single correct configuration, so each customer will decide on what is right for them based on their organizations risk profile, choice of capabilities to deploy, and existing IT investments. However, it is appropriate for the vendor to *put a stake in the ground* and publish a set of recommendations and guidance. That's exactly what Microsoft is doing with the consumer guides.

Having recommended configuration guidance to support their cloud services is not unusual on the CCSL, and I think it's appropriate for a vendor to be up front and clear about those recommendations that help customers stay safe and secure on their platform.

Azure customers can access the certification report and consumer guides today on the Microsoft Service Trust Portal. As soon as the same artefacts are available for Office 365, this is where they too will be published. In the meantime, the Office 365 IRAP report is already available from there.

Customer benefits of PROTECTED Office 365

Government organizations spend a lot of time, effort, and money in building and maintaining platforms to handle their PROTECTED material. The security and compliance requirements are higher, making it harder to implement a PROTECTED environment, and naturally it costs more money to do so. Running these environments often involves specially trained staff with government security clearances. Maintaining these environments carries all the same cost overheads.

With Office 365, government organizations can configure a cost-effective cloud service to meet, and exceed, their security and compliance obligations without the extensive build, maintenance, and on-premises, hosting, or outsourcer costs. Office 365 offers a PROTECTED solution at a lower total cost of ownership.

Office 365 is a modern and 'evergreen' cloud service. That is to say, Office 365 is always running the latest versions, with the latest patching. Customers never need to upgrade Office 365, because it is always kept up to date for them. This means the end of costly and disruptive IT upgrade and refresh cycles for the workloads that get moved into Office 365.

And Office 365 is more environmentally friendly. Not only has Microsoft been carbon neutral since 2012, but Office 365 has a smaller carbon footprint to begin with. By leveraging the inherent efficiencies and economies of scale, Office 365 can deliver its services at a fraction of the environmental impact of a customers traditional deployment.

Office 365 also offers governments around the country a modern collaboration platform that supports their various workplace flexibility initiatives. This is a great opportunity for government to side step another round of platform upgrades, get modern and current, and stay current going forward.

PROTECTED level Office 365 extends the opportunity to Australian government organizations to achieve the same benefits from cloud productivity, innovation, and cost reduction that Australia's commercial enterprises have been benefiting from over the past few years. This is the opportunity for government to match the private sector in terms of modern, scalable, and efficient IT.

It's an exciting time to be in Australian IT, working with government organizations around the country!

To be continued…

Keep an eye out for **Part 2** of this article series, where we will dive into the scope of the certification, and look at specific recommendations around products, features, licensing, and configuration. I'll also include an FAQ, so if you have a question you'd like answered please drop me line.