

Production Ready Cloud Platform

April 2020



Move your workload to Azure
and feel the peace of mind of
knowing you'll get it right –
and done in **RECORD TIME**



Agenda

01

Your needs

02

Your Options

03

Our Approach

Gaining the competitive edge

Transitioning the right workloads to the cloud in the right way is business critical.

But what's the best way to do this?



And how do you do this:

- Quickly?
- Securely?
- Guaranteed availability?

Your needs

Agility provided by cloud based workloads

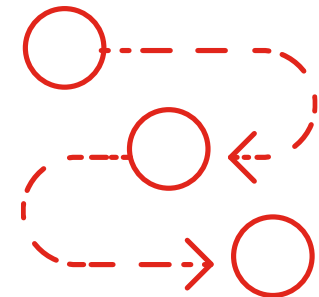
Speedy transition

Guaranteed uptime

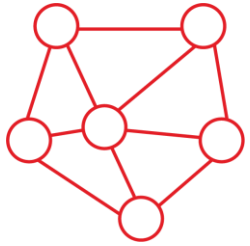
Watertight security

Easy and low cost ongoing management

Vendor/Partner confidence



Key considerations



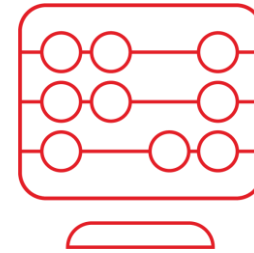
Networking

- Secure, granular model
- Design principles of disabled by default, access only where required
- Detailed logging and auditing
- Next generation security capabilities built in



Security

- Enshrine company policies, procedures and controls
- Protect administrative access, including ensuring access only from trusted locations
- Report non-compliance in real time
- Adhere to encryption and data sovereignty policies



Design architecture

- Guidelines for all future deployments
- Built in disaster recovery and high availability
- Security principles



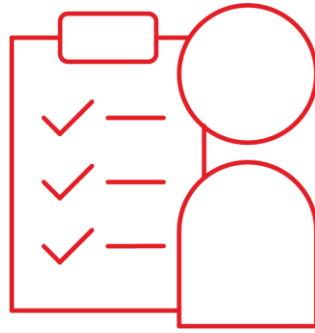
Ongoing management

- Simplify portal administration
- Consistent backup and recovery
- Automated security management
- Leverage DevOps and automation
- Detailed reporting to avoid "bill shock"

Your options



Do it yourself



Engage expert consultant



Pre-configured environment

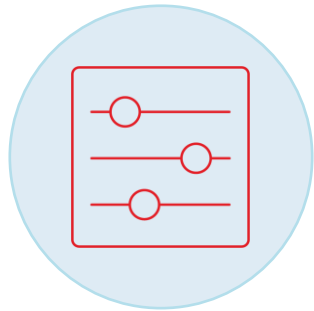
Our approach



The TDL Production Ready Cloud Platform is the gift that keeps on giving. It provides the guard rails that IT teams can follow to deploy future, additional workloads to Azure rapidly and with full confidence the framework will ensure the right outcome.



5 key benefits



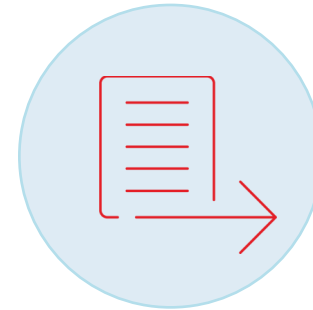
Design
framework



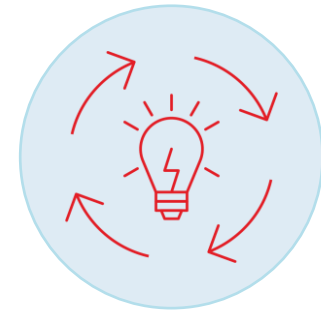
Security and
Compliance



Governance

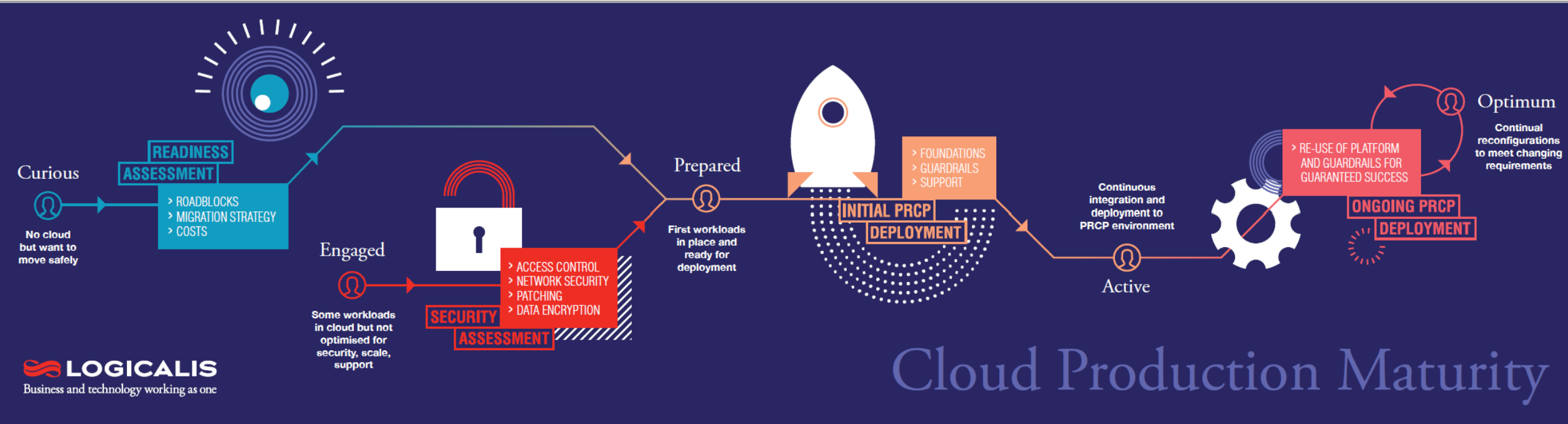


Ongoing
Management

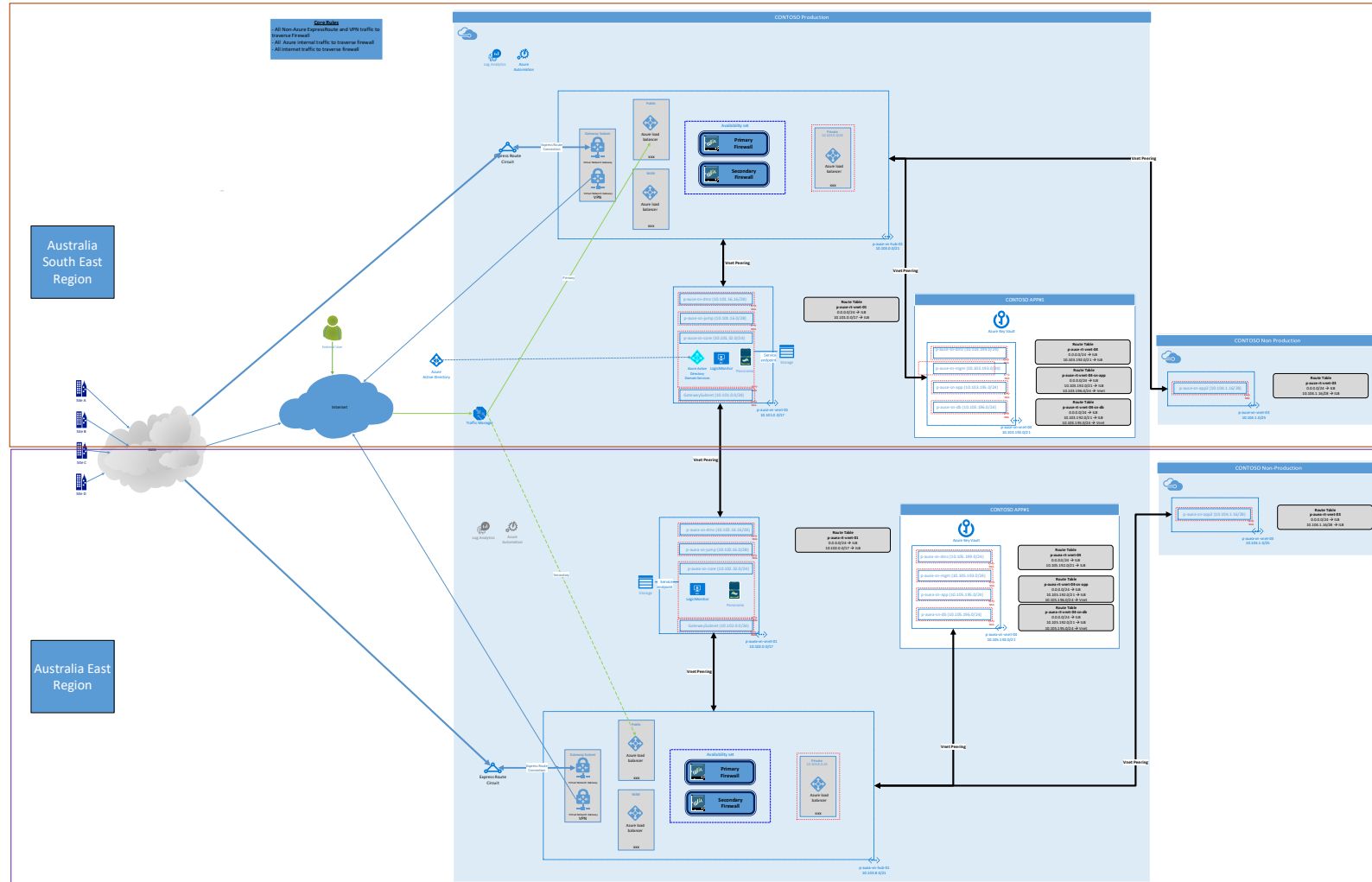


Availability

Cloud Journey



High Level Design



Infrastructure Security and Compliance



Australian Government Certified Cloud Services List (CCSL)

Microsoft is included in the Australian Certified Cloud Services List based on an IRAP assessment and certification by the ASD.

Microsoft and CCSL

Microsoft has undergone an IRAP assessment and been certified on the CCSL by ASD for Azure, Dynamics 365, and Office 365. For each assessment, Microsoft engaged an ASD-accredited assessor who examined the security controls and processes used by Microsoft's IT operations team, physical datacenters, intrusion detection, cryptography, cross-domain and network security, access control, and information security risk management of in-scope services. The IRAP assessments found that the Microsoft system architecture is based on sound security principles, and that the applicable Information Security Manual (ISM) controls are in place and fully effective within our assessed services.

- In 2014, Azure was launched as the first IRAP-assessed cloud service in Australia, hosted from datacenters in Melbourne and Sydney. These two datacenters give Australian customers control over where their customer data is stored, while also providing enhanced data durability in the event of a disaster through backups at both locations.
- In early 2015, Office 365 became the first cloud productivity service to complete this assessment.
- In April 2015, the ASD announced the CCSL certification of both Azure and Office 365, and in November 2015, of Dynamics 365.
- In June 2017, ASD announced the recertification of Microsoft Azure and Office 365 for a greatly expanded set of services for Unclassified DLM information.
- In April 2018, ASD announced the certification of Azure and Office 365 at the Protected classification. Microsoft is the first and only public cloud provider to achieve this level of certification.

Their certification provides assurance to public sector customers in government and their partners that Microsoft has appropriate and effective security controls in place for the processing, storage, and transmission of sensitive and official information that holds Dissemination Limiting Markings (DLMs) or is classified at the Protected level. This includes the majority of government, healthcare, and education data in Australia.

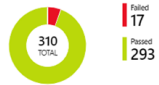
- Learn about the [benefits of CCSL on the Microsoft Cloud](#).

Infrastructure Security and Compliance

Security Center - Regulatory Compliance (Preview)

Showing 3 subscriptions

Regulatory compliance assessment



Regulatory standards compliance status



Regulatory compliance

View your compliance posture relative to the standards and regulations that are important to you. Remediate assessments to watch your compliance posture improve.

[Learn more >](#)

Azure CIS PCI DSS 3.2 ISO 27001 SOC TSP All

Under each applicable Compliance Control is a set of assessments run by Security Center that are associated with that Control. If they are all green, it means those assessments are currently passing; this does not ensure you are fully compliant with that control. Furthermore, not all controls for any particular regulation are covered by Security Center assessments, and therefore this report is only a partial view of your compliance status.

ASSESSMENT

Configure IP restrictions for Web Application (Preview)	ISO 27001	SOC TSP		
Use the latest supported PHP version for Web Application (Preview)	ISO 27001			
Require secure transfer to storage account (Preview)	Azure CIS	ISO 27001		
Remediate vulnerabilities in security configuration on your machines	Azure CIS	ISO 27001		
Troubleshoot missing scan data on your machines	ISO 27001			
Disable unrestricted network access to storage account (Preview)	ISO 27001			
Enable diagnostic logs in Key Vault (Preview)	Azure CIS	PCI DSS 3.2	ISO 27001	SOC TSP

RESOURCE TYPE

TOTAL RESOURCES

Web applications	51 of 51
Web applications	50 of 51
Storage accounts	32 of 78
Virtual machines	32 of 84
Virtual machines	28 of 84
Storage accounts	23 of 43
Key vaults	21 of 21

OS SECURITY CONFIGURATION

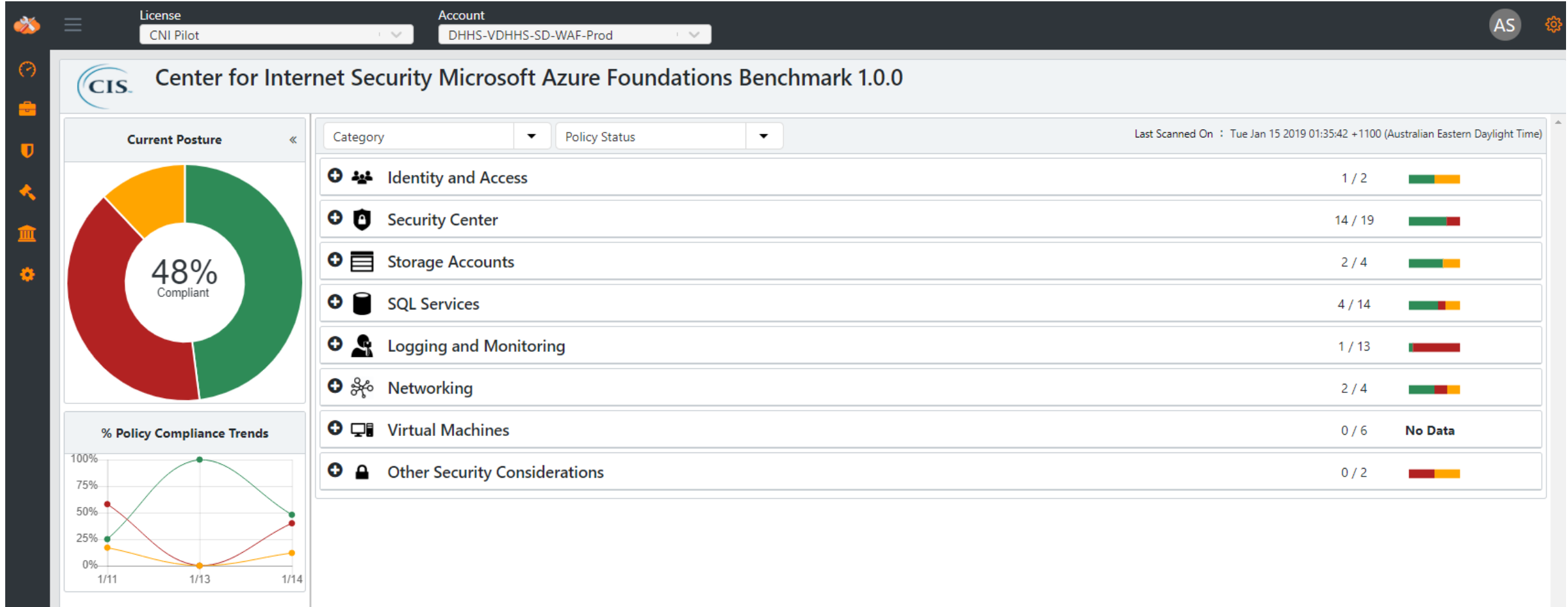
[CCE-4236-6] Accepting source routed packets should be disabled for all interfaces. (net.ipv4.conf.all.accept_source_route = 0) (Linux)	PCI DSS 3.2	SOC TSP
[CCE-4236-6] Accepting source routed packets should be disabled for all interfaces. (net.ipv6.conf.all.accept_source_route = 0) (Linux)	PCI DSS 3.2	SOC TSP
[CCE-4133-5] Ignoring bogus ICMP responses to broadcasts should be enabled. (net.ipv4.icmp_ignore_bogus_error_responses = 1) (Linux)	PCI DSS 3.2	SOC TSP
[CCE-3644-2] Ignoring ICMP echo requests (pings) sent to broadcast / multicast addresses should be enabled. (net.ipv4.icmp_echo_ignore_broadcasts = 1) (Linux)	PCI DSS 3.2	SOC TSP
[CCE-3561-8] IP forwarding should be disabled. (net.ipv4.ip_forward = 0) (Linux)	PCI DSS 3.2	SOC TSP
[CCE-5229-0] MSS: (DisableIPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing) (2008)	PCI DSS 3.2	SOC TSP
[CCE-24452-5] MSS: (DisableIPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing) (2012)	PCI DSS 3.2	SOC TSP

RESOURCE TYPE

TOTAL RESOURCES

VMs & computers	0 of 84
VMs & computers	0 of 84
VMs & computers	0 of 84
VMs & computers	0 of 84
VMs & computers	0 of 84
VMs & computers	0 of 84
VMs & computers	0 of 84

Infrastructure Security and Compliance



Next steps

1. Understand interest

2. Approve proposal to proceed

3. Design Workshops

4. Detailed Framework Design

5. Implementation and handover



A person in a light blue long-sleeved shirt and tan pants stands on a rocky peak, looking out over a vast mountain range at sunset. The sky is a mix of orange and yellow, and the mountains are silhouetted against the light. The person is seen from behind, standing on a dark, jagged rock formation.

We are architects of change

Together we own the possible