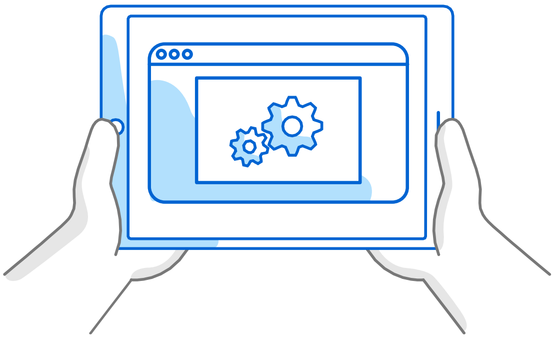
Managed Cloud Health Check
Overview

Telstra Purple's Managed Cloud Heath Check gives you a report into the health of your Azure and/or AWS public cloud environment and helps provide visibility and insight into your potential security, cost and compliance exposures. This complimentary, obligation free service leverages the experience and expertise of Telstra Purple and includes recommendations to achieve and maintain a secure, well managed cloud environment.

The Process

- Assessment of your existing public cloud environment against Microsoft Azure and/or AWS best practice standards to identify deltas and risks in security, cost and compliance for compute, identity and access, data and networking
- A report detailing high impact exposures and recommendations to remediate*
- Security risk reporting detailing currency of patching and existing backups and frequency and retention policies where native cloud provider tools are used, and security best practice recommendations
- Cost optimisation recommendations evaluating right sizing relative to utilisation and plan selection
- Compliance alignment to regulatory standards, where relevant, and operational excellence recommendations

The Value



- Complementary assessment and recommendations from Telstra Purple, the cloud experts you can trust
- Understand key areas of risk against critical business drivers
- Quick turn around on your obligation free assessment, report and consultation
- Opportunities to optimise your environment for security, cost and compliance

* Recommendations are general in nature and may require additional investigation based on your cloud environment configuration and specific business requirements

For additional information on how you can receive a complementary Managed Cloud Health Check, please contact your Telstra Representative or **Contact us - Telstra Purple**

Telstra Purple

Managed Cloud Health Check
How To

To access Telstra Purple's Managed Cloud Health Check and your personalised insights and recommendations, follow these simple steps:

Let's Get It Done …

- **Prerequisites**
  - An existing Microsoft Azure or AWS environment;
  - For AWS customers, have either Business or Enterprise Support to allow access to Trusted Advisor*;
  - If you require regulatory compliance reporting, have Conformance Packs (AWS) or Compliance Offerings (Azure) enabled;
  - Provide us with secure, limited access to the virtual machines running in your environment; and
  - Sign a Managed Cloud Health Check Application Form

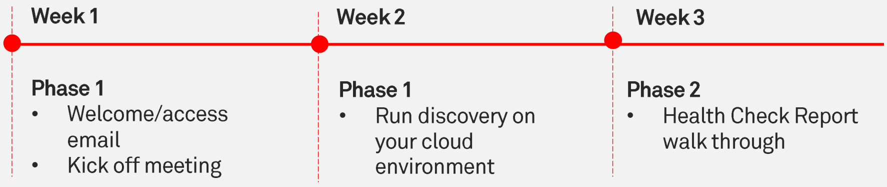
- **Phase 1 – Kick off meeting and environment access**
  - We'll email your technical contacts an ARM template (for Microsoft Azure) or CloudFormation template (for AWS) which delegates 'read onlyr' access to your environment
  - Join us for an initial meeting where we'll answer any questions you may have and confirm details in order to undertake the assessment
  - Our Telstra Purple Engineers will run discovery on your cloud environment

- **Phase 2 – Reporting and Consultation**
  - Allow 1 week for collection of data and compilation of your customised Health Check report
  - A session with our Telstra Purple experts to walk you through the report and discuss key call outs and recommendations
  - If you'd like further information on any of the recommendations, we can provide more detailed information on how we can help you resolve any identified issues

* There may be a small cost from your cloud provider for enabling this service

Timeline

The anticipated timeframe is 2-3 weeks, dependent on your availability



Week 1

Phase 1
- Welcome/access email
- Kick off meeting

Week 2

Phase 1
- Run discovery on your cloud environment

Week 3

Phase 2
- Health Check Report walk through

For additional information on how you can receive a complementary Managed Cloud Health Check, please contact your Telstra Representative or **Contact us - Telstra Purple**

Managed Cloud Health Check
Environment Access

Security is our top priority and Managed Cloud Health Check complies with Telstra's organizational wide Security Governance Framework which leverages a number of controls within industry practices and standards such as ISO/IEC 27001:2013 (AS ISO/IEC 27001:2015), AS ISO 31000:2018, PSPF, ASD, ISM, NIST, PCI DSS. It uses a proactive governance approach to the security of its identities, devices, access, applications, networks, infrastructure and data

Access

We require permission to run reports for the environments you delegate. Access to your environment will be granted using the principle of least privilege required to run reports on your behalf.

Microsoft Azure

To securely access your Microsoft Azure environment we use Azure Lighthouse. Azure Lighthouse is an Azure Resource Manager capability called resource management which enables businesses to delegate permission to service providers over selected scopes, including subscriptions and resource groups.

To grant us access to your subscription/s you need either Global Administrator or Owner access. We provide you with an Azure Lighthouse ARM template which delegates the following permissions to your Azure subscription/s.

Telstra Purple Security Group Name	Role
CUST - DMS Engineer - Global Read Only	Reader

AWS

To securely access your AWS environment we use AWS Identity and Access Management (IAM). IAM is a web service that helps to securely control access to AWS resources and it controls who is authenticated (signed in) and authorised (has permissions) to use resources.

To grant us access to your account/s you need Account Administrator access. We provide you with a CloudFormation template which delegates the following permissions to your account/s.

Telstra Purple Security Group Name	Role
CUST - DMS Engineer - Global Read Only	Reader

For additional information on how you can receive a complementary Managed Cloud Health Check, please contact your Telstra Representative or **Contact us - Telstra Purple**