{{r org\_name }} audit report

{{ month\_year }}

# Contacts

### {{r member\_name }}

|  |  |
| --- | --- |
| Contact 1 | Contact 2 |
| {{r contact1\_name }} | {{r contact2\_name }} |
| {{r contact1\_role }} | {{r contact2\_role }} |
| {{r contact1\_email }} | {{r contact2\_email }} |
| {{r contact1\_phone }} | {{r contact2\_phone }} |

### Jisc, Cybersecurity division

|  |  |
| --- | --- |
| Contact 1 | Contact 2 |
| Jisc Cyber Security Professional Services | Leah Honer |
| [professional.cyberservices@jisc.ac.uk](mailto:professional.cyberservices@jisc.ac.uk) | Professional security services manager |
|  | [leah.honer@jisc.ac.uk](mailto:leah.honer@jisc.ac.uk) |
|  | 07776 957936 |

### Jisc, Cyber security assessors

|  |  |
| --- | --- |
| Contact 1 | Contact 2 |
| Paul Knee | Ben Chapman |
| Security specialist | Security specialist |
| [paul.knee@jisc.ac.uk](mailto:paul.knee@jisc.ac.uk) | [ben.chapman@jisc.ac.uk](mailto:ben.chapman@jisc.ac.uk) |
| 07435 984771 | 07586 549064 |

|  |  |
| --- | --- |
| Contact 3 | Contact 4 |
| Adam Maxwell | Charlotte King |
| Security specialist | Cyber security services group manager |
| [adam.maxwell@jisc.ac.uk](mailto:adam.maxwell@jisc.ac.uk) | [charlotte.king@jisc.ac.uk](mailto:charlotte.king@jisc.ac.uk) |
| 07825 176624 | 07776 769046 |

*“All modern software contains vulnerabilities; either software defects that require patches to remedy, or configuration issues that require administrative activity to resolve.”*

*“For this reason, organisations should have a vulnerability management process which enables them to know what vulnerabilities are present within their IT estate on a regular basis. Executive staff should ideally be as aware of the major vulnerabilities in their IT estate as they are of their financial status.”*

****NCSC Vulnerability Management Process****

# Disclaimer

A vulnerability assessment is considered a snapshot in time. The findings and recommendations reflect the information gathered during the assessment and not any changes or modifications made outside of that period.

Time-limited engagements do not allow for a full evaluation of all security controls. The Jisc Professional Services Team prioritised the assessment to identify the weakest security controls an attacker would exploit. Jisc recommends conducting similar assessments on an annual basis by internal or third-party assessors to ensure the continued success of the controls.

After testing has concluded, you should ensure any test accounts are revoked and any IP whitelist rules added for the test are removed.

# Table of contents

[Contacts 2](#__RefHeading___Toc6996_3152444580)

[Disclaimer 3](#__RefHeading___Toc7004_3152444580)

[Table of contents 4](#__RefHeading___Toc7006_3152444580)

[Executive Summary 5](#__RefHeading___Toc7008_3152444580)

[Scope 6](#__RefHeading___Toc7010_3152444580)

[Conclusions and Recommendations 7](#__RefHeading___Toc7012_3152444580)

[Summary of Findings 8](#__RefHeading___Toc7018_3152444580)

[Detailed Findings 9](#__RefHeading___Toc7020_3152444580)

[Appendix A: Useful resources 12](#__RefHeading___Toc7064_3152444580)

[Scanning 12](#__RefHeading___Toc7066_3152444580)

[SSL and TLS  12](#__RefHeading___Toc7068_3152444580)

[HTTP security headers  12](#__RefHeading___Toc7070_3152444580)

[CIS security benchmarks 13](#__RefHeading___Toc7072_3152444580)

[Operating System Benchmarks (Hardening) 13](#__RefHeading___Toc7074_3152444580)

[Database Benchmarks (Hardening) 13](#__RefHeading___Toc7076_3152444580)

[Application Benchmarks (Hardening) 13](#__RefHeading___Toc7078_3152444580)

# Executive Summary

The professional service team at Jisc is pleased to present this cloud audit report for {{r org\_name }}.

The engagement took place between the {{ start\_day }} and {{ end\_day }} {{ month\_year }} reviewing the configuration of your cloud setup against CIS Benchmarking defined controls, using automated and manual checks.

The overarching goal of this engagement was to identify areas for improvement and provide advice on how to implement any recommendations changes. Below are the findings for each level of check. It is strongly recommended that you review each of the findings and take the appropriate action where necessary. There are some controls listed below that require manual review on a regular basis and should be incorporated into administrative tasks. Before enabling any Level 1 or Level 2 controls it is strongly recommended that you ensure the change will not have a negative effect on service.

|  |  |
| --- | --- |
| **Risk** **Rating** | **Number of Findings** |
| **Non-Compliant** | {{ num\_failed }} |
| **Compliant** | {{ num\_passed }} |
| **Information** | {{ num\_warning }} |

# Scope

The list of services covered by this assessment included:

{%p for item in scope %}

* {{ item }}

{%p endfor %}

# Summary of Findings

A total of {{ num\_total }} findings were identified.

|  |  |  |
| --- | --- | --- |
| **Finding** | **Risk Rating** | **Affected Service** |
| {%tr for issue in issues.failed %} | | |
| {{ issue.title }} | **Failed** | {% for s in issue.services %}{{ s }}  {% endfor %} |
| {%tr endfor %} | | |
| {%tr for issue in issues.passed %} | | |
| {{ issue.title }} | **Passed** | {% for s in issue.services %}{{ s }}  {% endfor %} |
| {%tr endfor %} | | |
| {%tr for issue in issues.warning %} | | |
| {{ issue.title }} | **Information** | {% for s in issue.services %}{{ s }}  {% endfor %} |
| {%tr endfor %} | | |

# Detailed Findings

# Non-Compliant

{% for issue in issues.failed %}

## {{ issue.title }}

|  |  |
| --- | --- |
| {%tr for service in issue.services %} | |
|  | {{ service }} |
| {%tr endfor %} | |

### Description

{{r issue.description }}

### Rationale

{{r issue.rationale }}

### Solution

{{r issue.remediation }}

### References

{{r issue.reference }}

### Impact

{{r issue.impact }}

{% endfor %}

# Compliant

{% for issue in issues.passed %}

## {{ issue.title }}

|  |  |
| --- | --- |
| {%tr for service in issue.services %} | |
|  | {{ service }} |
| {%tr endfor %} | |

### Description

{{r issue.description }}

### Rationale

{{r issue.rationale }}

### Solution

{{r issue.remediation }}

{% if issue.reference %}

### References

{{r issue.reference }}

{% endif %}

### Impact

{{r issue.impact }}

{% endfor %}

# Information

{% for issue in issues.warning %}

## {{ issue.title }}

|  |  |
| --- | --- |
| {%tr for service in issue.services %} | |
|  | {{ service }} |
| {%tr endfor %} | |

### Description

{{r issue.description }}

### Rationale

{{r issue.rationale }}

### Solution

{{r issue.remediation }}

### References

{{r issue.reference }}

### Impact

{{r issue.impact }}

{% endfor %}

# **Appendix A: Useful resources**

## Scanning

* OpenVAS is a free vulnerability scanner that can be deployed for use internally and externally: <http://openvas.org/>
* Tenable Nessus and Rapid7 Nexpose are paid products that both offer similar functionality and a free trial, which would be suitable for occasional use (eg: quarterly):  
  [tenable.com/](https://www.tenable.com/) and [rapid7.com/products/nexpose/](https://www.rapid7.com/products/nexpose/)
* PingCastle is a free-to-use Active Directory audit tool that can quickly identify issues in the AD configuration and group policy: [pingcastle.com/](https://www.pingcastle.com/)

## SSL and TLS

* For SSL maintenance, Qualys’ online SSL test can provide clear and detailed information about an internet-facing site’s SSL configuration: [ssllabs.com/ssltest/analyze.html](https://www.ssllabs.com/ssltest/analyze.html)
* Similarly, the tool sslscan can be run locally to identify the configuration of SSL services: <https://github.com/rbsec/sslscan>
* The following article contains practical information on configuring SSL/TLS on a variety of servers: <https://hynek.me/articles/hardening-your-web-servers-ssl-ciphers/>
* The SSL Labs “SSL and TLS Deployment Best Practices” guide contains information about which cipher suites and configurations to use: <https://github.com/ssllabs/research/wiki/SSL-and-TLS-Deployment-Best-Practices>
* The OWASP Transport Layer Protection Cheat Sheet provides a variety of high level information about designing and using TLS and SSL: <https://github.com/OWASP/CheatSheetSeries/blob/master/cheatsheets/Transport_Layer_Protection_Cheat_Sheet.md>
* IISCrypto is a free tool that can be used to centrally manage SSL/TLS cipher suites, which can greatly reduce the burden of keeping configurations and in line with best practices: [nartac.com/Products/IISCrypto/](https://www.nartac.com/Products/IISCrypto/)

## HTTP security headers

* It is considered best practice to send specific HTTP security headers, which can help control a browser’s behaviour in order to protect users against common attacks. The following resource details these headers and their possible values: [keycdn.com/blog/http-security-headers](https://www.keycdn.com/blog/http-security-headers)

## CIS security benchmarks

### Operating System Benchmarks (Hardening)

* [CIS Microsoft Windows Desktop Benchmarks (cisecurity.org)](https://www.cisecurity.org/benchmark/microsoft_windows_desktop/)
* [CIS Microsoft Windows Server Benchmarks (cisecurity.org)](https://www.cisecurity.org/benchmark/microsoft_windows_server/)
* [Debian Family Linux (cisecurity.org)](https://www.cisecurity.org/benchmark/debian_family/)
* [Fedora Family Linux (cisecurity.org)](https://www.cisecurity.org/benchmark/fedora_family_linux/)

### Database Benchmarks (Hardening)

* [PostgreSQL (cisecurity.org)](https://www.cisecurity.org/benchmark/postgresql/)
* [CIS Microsoft SQL Server Benchmarks (cisecurity.org)](https://www.cisecurity.org/benchmark/microsoft_sql_server/)

### Application Benchmarks (Hardening)

* [CIS Microsoft IIS Benchmarks (cisecurity.org)](https://www.cisecurity.org/benchmark/microsoft_iis/)
* [CIS Microsoft Exchange Server Benchmarks (cisecurity.org)](https://www.cisecurity.org/benchmark/microsoft_exchange_server/)