ICT Audit

FINAL

APPENDIX 2b

# South Lakeland District Council

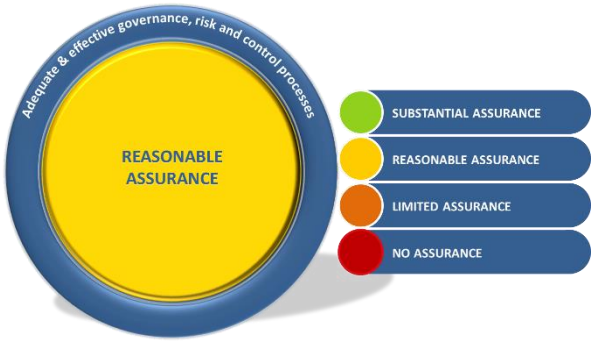
## ICT Review of Network Security and Cybercrime

## 2019/20

September 2020

# Executive Summary

## OVERALL ASSURANCE ASSESSMENT




## OVERALL CONCLUSION

**Appropriate operational cyber security arrangements are in place at South Lakeland District Council, however, the framework within which the cyber security controls function can be strengthened.**

- **Policies are in need of review and document control applied.**
- **The Council does not apply critical patches in line with best practice although this is mitigated to some degree; this risk should be periodically reviewed.**
- **The migration of the remaining Windows 7 computers to Windows 10 is not yet complete with Windows 7 support having ceased on 14th January 2020.**
- **The Council has robust technical measures in place, however, the single firewall represents a single point of failure.**

## SCOPE

Organisations are increasingly reliant on ICT systems for everyday operations and service delivery. This review assessed the arrangements in place for maintaining the integrity of the computer network. This included server configuration and patching, threat detection, change control, remote access, user administration and desktop control policies as well as examining supporting policy and procedural documentation. The review also considered the arrangements for the pro-active identification, prioritisation and mitigation against cyber-crime.

## ACTION POINTS

| Urgent | Important | Routine | Operational |
|---|---|---|---|
| 0 | 5 | 3 | 3 |

# Management Action Plan - Priority 1, 2 and 3 Recommendations

| Rec. | Risk Area | Finding | Recommendation | Priority | Management Comments | Implementation Timetable (dd/mm/yy) | Responsible Officer (Job Title) |
|---|---|---|---|---|---|---|---|
| 1 | Directed | The Information Security Policy requires a full review to bring it up to date to ensure it is fit for purpose with revisions to include, but not be limited to, references to legislation and standards and roles and responsibilities. Other policies also require review. Document control should also be used to provide a framework to ensure polices are regularly reviewed and maintained. | It be ensured that all ICT policies and procedures are subject to regular review, utilising document control, to provide a defined framework in which the Network Security and Cybercrime controls operate. | 2 | *Paul Mountford has agreed to lead on setting up regular reviews of IT policies and procedures.* | *31/10/20* | *Infrastructure Lead* |
| 2 | Compliance | A random sample of ten staff members was selected and evidence requested to confirm that signed Authorised User Agreements to comply with the Information Security Policy and Internet and Email Acceptable Use Policy were held, however, only two were located at the time of audit. The Council should ensure that it can evidence employee's acceptance of these policies by holding signed Authorised User Agreements on file for all staff. | It be ensured that signed Authorised User Agreements are obtained and kept on file for all members of staff. | 2 | *HR have agreed to take over the responsibility for issuing and storing signed Authorised User Agreement forms from 7th September.* | *07/09/20* | *Infrastructure Lead* |

**PRIORITY GRADINGS**

| | | |
|---|---|---|
| 1 | **URGENT** | Fundamental control issue on which action should be taken immediately. |
| 2 | **IMPORTANT** | Control issue on which action should be taken at the earliest opportunity. |
| 3 | **ROUTINE** | Control issue on which action should be taken. |

| Rec. | Risk Area | Finding | Recommendation | Priority | Management Comments | Implementation Timetable (dd/mm/yy) | Responsible Officer (Job Title) |
|---|---|---|---|---|---|---|---|
| 4 | Compliance | All mobile devices are encrypted including laptops, however, desktop computers are not currently encrypted. As the Council has the facility to also encrypt desktop computers, this should be put in place to mitigate against the loss of data and subsequent potential reputation loss in the event of theft. | Encryption be applied to desktop computers to mitigate against the loss of data and subsequent potential reputation loss in the event of theft. | 2 | *Agreed.* | *Completed* | *Infrastructure Lead* |
| 5 | Compliance | Laptops are configured with a local firewall operative although desktops are not. Enabling the local firewall on desktop machines may help to contain the spread of malware in the event a machine is compromised and should be put in place. | The local firewall be enabled on Desktop PCs to help to contain the spread of malware in the event a machine is compromised. | 2 | *Agreed.* | *Completed* | *Infrastructure Lead* |
| 7 | Compliance | The Council does not block the downloading of harmful file types. While users are unable to install applications without administrator privileges, file sharing sites are blocked and the firewall and anti-virus software scan for suspicious files, it still presents a possible vector for unwanted and potentially dangerous software to be present on the Council's network. The blocking of file types including, but not limited to, executables, installers, batch files and visual basic scripts would provide some mitigation of this risk and should be implemented. | The blocking of the download of file types including, but not limited to, executables, installers, batch files and visual basic scripts be implemented. | 2 | *Agreed.* | *Completed* | *Infrastructure Lead* |

PRIORITY GRADINGS

| | | |
|---|---|---|
| 1 | URGENT | Fundamental control issue on which action should be taken immediately. |
| 2 | IMPORTANT | Control issue on which action should be taken at the earliest opportunity. |
| 3 | ROUTINE | Control issue on which action should be taken. |

| Rec. | Risk Area | Finding | Recommendation | Priority | Management Comments | Implementation Timetable (dd/mm/yy) | Responsible Officer (Job Title) |
|---|---|---|---|---|---|---|---|
| 3 | Compliance | The Council has been migrating its existing stock of Windows 7 computers to Windows 10 due to the upcoming end of life (EOL), and subsequent lack of support including security patches, on 14th January 2020. At the time of audit, however, approximately 30 to 40 computers were yet to be migrated including two computers which have not been migrated due to issues with a specialised parking application, for which the Council is awaiting resolution by the software vendor. The IT team is confident that the remaining Windows 7 computers will be migrated before EOL, however, it should be ensured that mitigations are put in place if, due to unresolved issues, Windows 7 computers are still in operation at the Council once support for Windows 7 ends. | It be ensured that mitigations are put in place if, due to unresolved issues, Windows 7 computers are still in operation at the Council once support for Windows 7 ends. | 3 | *Extended support purchased from Microsoft.* | *Completed* | *Infrastructure Lead* |
| 6 | Compliance | A log of firewall rule changes has been introduced, however, as part of the Change Request process, these requests should have been logged via the Service Desk but no field to record the Service Desk reference is provided. Providing the Service Desk reference would allow rule changes to be followed back to the original request and should be included. | A Service Desk reference be added to the firewall rule changes log to allow rule changes to be followed back to the original request. | 3 | *Agreed.* | *Completed* | *Infrastructure Lead* |

PRIORITY GRADINGS

| | | |
|---|---|---|
| 1 | URGENT | Fundamental control issue on which action should be taken immediately. |
| 2 | IMPORTANT | Control issue on which action should be taken at the earliest opportunity. |
| 3 | ROUTINE | Control issue on which action should be taken. |

| Rec. | Risk Area | Finding | Recommendation | Priority | Management Comments | Implementation Timetable (dd/mm/yy) | Responsible Officer (Job Title) |
|---|---|---|---|---|---|---|---|
| 8 | Compliance | Servers are patched centrally using System Center Configuration Manager (SCCM) on a four week cycle following Microsoft's monthly release which typically involves a test group being patched during the first week, and subsequent devices being patched on a phased approach with all devices receiving the patch by the end of week four. While this cautious approach mitigates against the disruption to live servers used by staff and stakeholders, it falls outside the best practice timescales of 14 days for the application of critical patches. It is noted that internet facing servers are set to patch immediately and the IT team monitor incoming patches and would take action if they felt the application of a critical patch out of phase was required. Nonetheless, the Council should ensure that it continues to review the risk of applying critical updates outside of best practice against the risk of disruption to live servers. | It be ensured that the Council continues to review the risk of applying critical updates outside of best practice against the risk of disruption to live servers. | 3 | *If we are alerted to a critical update, then we would look to test and apply this immediately. Our Patch Management Policy and Procedure have been updated to reflect this.* | *Completed* | *Infrastructure Lead* |

PRIORITY GRADINGS

| | | |
|---|---|---|
| 1 | URGENT | Fundamental control issue on which action should be taken immediately. |
| 2 | IMPORTANT | Control issue on which action should be taken at the earliest opportunity. |
| 3 | ROUTINE | Control issue on which action should be taken. |

# Operational Effectiveness Matters

| Ref | Risk Area | Item | Management Comments |
|---|---|---|---|
| 1 | Directed | Consideration be given to achieving Cyber Essentials Certification once the Council is satisfied that all appropriate controls are in place. | *Agreed, we will consider this.* |
| 2 | Directed | The introduction of Phishing simulation software to educate and test end users through automated attack simulations be considered. | *Agreed, we will consider this.* |
| 3 | Compliance | Consideration be given to mitigating the risk of disruption due to firewall appliance failure. | *We have added additional firewall resilience since the audit was completed by adding a duplicate hardware appliance to cope with hardware failure, we now have a resilient pair of firewalls.* |

ADVISORY NOTE

Operational Effectiveness Matters need to be considered as part of management review of procedures.

# Detailed Findings

## Introduction

1. This review was carried out in December 2019 as part of the planned internal audit work for 2019/20. Based on the work carried out an overall assessment of the overall adequacy of the arrangements to mitigate the key control risk areas is provided in the Executive Summary.

## Background

2. Robust and secure ICT networks are critical in ensuring that South Lakeland District Council's systems maintain their integrity to enable staff to deliver services to customers and stakeholders.

## Materiality

3. South Lakeland District Council places considerable reliance on the management of its computer systems for day to day operations and to achieve its business objectives.

## Key Findings & Action Points

4. The key control and operational practice findings that need to be addressed in order to strengthen the control environment are set out in the Management and Operational Effectiveness Action Plans. Recommendations for improvements should be assessed for their full impact before they are implemented.

## Scope and Limitations of the Review

5. Organisations are increasingly reliant on ICT systems for everyday operations and service delivery. This review assessed the arrangements in place for maintaining the integrity of the computer network. This included server configuration and patching, threat detection, change control, remote access, user administration and desktop control policies as well as examining supporting policy and procedural documentation. The review also considered the arrangements for the pro-active identification, prioritisation and mitigation against cyber-crime.

6. The definition of the type of review, the limitations and the responsibilities of management in regard to this review are set out in the Annual Plan.

## Disclaimer

7. The matters raised in this report are only those that came to the attention of the auditor during the course of the internal audit review and are not necessarily a comprehensive statement of all the weaknesses that exist or all the improvements that might be made. This report has been prepared solely for management's use and must not be recited or referred to in whole or in part to third parties without our prior written consent. No responsibility to any third party is accepted as the report has not been prepared, and is not intended, for any other purpose. TIAA neither owes nor accepts any duty of care to any other party who may receive this report and specifically disclaims any liability for loss, damage or expense of whatsoever nature, which is caused by their reliance on our report.

## Risk Area Assurance Assessments

8. The definitions of the assurance assessments are:

| | |
|---|---|
| **Substantial Assurance** | There is a robust system of internal controls operating effectively to ensure that risks are managed and process objectives achieved. |
| **Reasonable Assurance** | The system of internal controls is generally adequate and operating effectively but some improvements are required to ensure that risks are managed and process objectives achieved. |
| **Limited Assurance** | The system of internal controls is generally inadequate or not operating effectively and significant improvements are required to ensure that risks are managed and process objectives achieved. |
| **No Assurance** | There is a fundamental breakdown or absence of core internal controls requiring immediate action. |

## Acknowledgement

9. We would like to thank staff for their co-operation and assistance during the course of our work.

## Release of Report

10. The table below sets out the history of this report.

| | |
|---|---|
| **Date draft report issued:** | 21st January 2020 |
| **Date management responses received:** | 2nd September 2020 |
| **Date final report issued:** | 2nd September 2020 |