VISIT NUMBER: 610181

DATE OF OPENING MEETING: 26/01/2022

THIS REPORT HAS BEEN PREPARED BY:

REGIONAL ASSESSOR: Jesse Culleton

CONTACT NUMBER: 07974 014 210

EMAIL: Jesse.culleton@nqa.com

APPLICABLE STANDARD(S):

ISO 27001:2013
### Client Information

<table>
<thead>
<tr>
<th>Primary Contact:</th>
<th>Laurel Kindy &amp; James Heathcote</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address:</td>
<td>The Granary, Abbey Mill Business Park, Godalming, Surrey GU7 2QW</td>
</tr>
<tr>
<td>Contact Tel:</td>
<td>01483239240</td>
</tr>
<tr>
<td>Contact Email:</td>
<td><a href="mailto:laurel.kindy@unily.com">laurel.kindy@unily.com</a> &amp; <a href="mailto:james.heathcote@unily.com">james.heathcote@unily.com</a></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Billing Contact:</th>
<th>As above</th>
</tr>
</thead>
<tbody>
<tr>
<td>Billing Tel:</td>
<td>As above</td>
</tr>
<tr>
<td>Billing Email:</td>
<td>As above</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Audit Conducted at:</th>
<th>Head Office (multi-site certification)</th>
<th>Participating / Temporary Site (multi-site certification)</th>
<th>Single Site Certification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit Conducted as:</td>
<td>Fully On-Site</td>
<td>Split On-Site / Remote</td>
<td>Fully Remote</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>System integration (integrated audits only):</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Additional information on integration (if required):</td>
<td></td>
</tr>
<tr>
<td>Certificate expiry date(s):</td>
<td>UKAS (80199) expiry 26/02/2024</td>
</tr>
<tr>
<td>Required changes to EAC or NQA Codes applied:</td>
<td>No changes required</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>At this location</th>
<th>Across all locations (Multisite)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total employees</td>
<td>118</td>
<td></td>
</tr>
<tr>
<td>Repetitive or parallel workers</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Energy engaged employees</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Energy consumption</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Energy uses</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Energy sources</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Energy data only applicable for ISO 50001 audits. Further guidance available in ASR 47:2.1*

**The date of the next audit is:** 25/01/2023 for 26/01/2023
AUDIT REPORT PART A - EXECUTIVE SUMMARY

Audit Information

Audit duration (in days): 2 days remote surveillance

Scope of certification: 'The provision of intranet as a service to commercial clients in accordance with the Statement of Applicability Version 1.0 dated 17.01.2018'

Scope is appropriate.

Confirmation that audit objectives have been fulfilled: All objectives met.

If no, which objectives have not been met. Note that customers with installation/service activities within their scope must receive a minimum of one on-site visit once per cycle. Failure to achieve this may result in this activity being removed from the client’s scope of certification.

NQA Audit Team

<table>
<thead>
<tr>
<th>Lead Assessor</th>
<th>Client</th>
<th>Position</th>
<th>Attendance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jesse Culleton</td>
<td>James Heathcote</td>
<td>Information Security Manager</td>
<td>Opening and Closing</td>
</tr>
<tr>
<td>Member 1</td>
<td>Michael Harper</td>
<td>Sam Hassani</td>
<td>Opening</td>
</tr>
<tr>
<td>Member 2</td>
<td>Lyk Calligeris</td>
<td>Director of Operations</td>
<td>Closing</td>
</tr>
</tbody>
</table>

* Mandatory attendance at OHSAS18001 / ISO45001 Audits. If these mandatory positions are not present at closing meeting, record and justify reasons in the Executive Summary.

Details of Changes

<table>
<thead>
<tr>
<th>Type of action or change required</th>
<th>Action Required</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Name Change:</td>
<td>☐</td>
<td></td>
</tr>
<tr>
<td>Change of Address:</td>
<td>☐</td>
<td></td>
</tr>
<tr>
<td>Scope Change:</td>
<td>☐</td>
<td></td>
</tr>
<tr>
<td>Contact Change:</td>
<td>☐</td>
<td></td>
</tr>
<tr>
<td>Number of Employees Change:</td>
<td>☐</td>
<td></td>
</tr>
<tr>
<td>Major NCs Raised:</td>
<td>☐</td>
<td></td>
</tr>
<tr>
<td>Special Visit Recommended:</td>
<td>☐</td>
<td></td>
</tr>
<tr>
<td>Other:</td>
<td>☐</td>
<td></td>
</tr>
</tbody>
</table>
Executive Summary

This Remote Surveillance audit was undertaken to evidence conformance within the requirements of ISO/IEC 27001:2013 and was conducted over 2 working days. The ICT used in carrying out the Assessment was as follows:

- MS Teams was used for video conferencing and screen sharing facilities throughout. Telephone and email systems were also used
- Assessment objectives were fully achieved via these means
- ICT systems used were fully effective in achieving the Assessment objectives

The organisation’s context is well defined, leadership has been effectively demonstrated and commitment levels are evident.

This is reflected in the levels of compliance with requirements and operational control evident at the organisation during the audit process.

The availability of documented information to demonstrate that the system is well implemented and well understood throughout the organisation is acceptable.

This audit has involved a review of system administration activities, a review and sample of site activities at The Granary, Abbey Mill Business Park, Godalming, Surrey GU7 2QW, as well as review of job related records.

It was fully evident that the key policy commitments are being adhered to.

Grateful thanks are passed to all the participants for their time, assistance and hospitality during this audit.

It should be noted that this audit report is based on a sample basis, a fully comprehensive audit has not been undertaken.

<table>
<thead>
<tr>
<th>Major NCs</th>
<th>Zero</th>
<th>Minor NCs</th>
<th>Zero</th>
<th>OFIs</th>
<th>Zero</th>
<th>AoCs</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zero</td>
<td></td>
<td>Zero</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Is there any conflict of interest which exists between the Auditor(s) and the client, and are there any situations known to them that present themselves, or NQA, with a potential conflict of interest in respect to the audit undertaken.

No.
### Audit Conclusion

- This visit was Satisfactory: Continuation or granting of certification is recommended
- No findings have been identified
- Any findings are as detailed on the following page(s).

### Audit Follow-up Actions

The following post-audit action(s) shall be taken by the client: No action required.

Please note that certification will not be granted, reissued or revised until all outstanding Non-Conformance responses have been submitted, and in the case of Major Non-Conformances, the evidence of corrective action has been provided to, and accepted by, NQA.

For further information, useful guidance and further support for responding to audit findings, please visit [https://www.nqa.com/en-gb/clients/non-conformities](https://www.nqa.com/en-gb/clients/non-conformities)

### Management system performance, such as trends in audit findings that require further investigation at the next recertification audit.

**Mandatory completion at the Head Office Audit of Surveillance Year 2**

Detail that the previous Recertification (or Stage 2), Surveillance 1 and Surveillance 2 results have been reviewed and whether there are any trends in non-conformities or other issues which require further investigation at the next Recertification audit.
### Audit Findings

<table>
<thead>
<tr>
<th>Ref No.</th>
<th>Clause No.</th>
<th>Details of any finding(s) raised.</th>
<th>Type (Major NC, Minor NC, OFI or AoC)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**End of Findings**

**Note:** Responses to findings must be sent using the Corrective Action Plan form, as applicable, to caps@nqa.com within the timeframes stated on Page 5.

### Closure of Findings from Previous Audit:

**Report No. 490801, Dated 25/01/2021**

<table>
<thead>
<tr>
<th>Ref No.</th>
<th>Detail of finding and client action:</th>
<th>Outcome (Closed or Escalated)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Clause Summary

<table>
<thead>
<tr>
<th>Clause No.</th>
<th>Summarise Action(s) Taken to Prevent Recurrence</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>NC01 5.3</td>
<td><em>The company is not fully compliant with the clause detailed, in that:</em> Roles and responsibilities have not been defined for the following roles:  - (Global Head of People)  - (Director of Operations) Within the RACI table, both roles have been identified as Responsible and Accountable for areas of the Information Security Management system (ISMS). <strong>Finding:</strong> this was amended during the audit process and was reviewed and closed prior to the closing meeting.</td>
<td>Minor NC Closed</td>
</tr>
<tr>
<td>OFI 01 N/A</td>
<td>It may benefit the organisation to review the Key type within the management action log to ensure they use the correct identification keys are used to reduce confusion. Sampled Ref 33 has been identified as IA (internal audit action) by C S but in fact should have been raised as F (Feedback). Also the completion dates updated.</td>
<td>OFI Closed</td>
</tr>
<tr>
<td>OFI 02 N/A</td>
<td>It would be beneficial to clarify the target and timescales and define how the results will be evaluated for all of the IS Objectives to ensure timely recording, improvement actions required and to better determine fulfilment.</td>
<td>OFI Closed</td>
</tr>
<tr>
<td>NC02 A.18.1.1</td>
<td>Whilst the Register of Legal Obligations and Responsibilities lists relevant legislative requirements (related to information security), the organisation’s approach to meet these requirements has not been explicitly identified nor documented as required by ISO 27001 Annex A Control A.18.1.1</td>
<td>Minor Closed</td>
</tr>
</tbody>
</table>
### Findings: the organisation has updated the information recorded and added new column to the register listing the responsibilities, review date and links to the ISMS

| NC03 | 6.1 | The organisation will need to ensure that the IS Risk Management policy is embedded and used to identify Risks and Risk Treatment plan identified within the Risk Register and within the risk management framework. **Finding:** full risk management process completed by organisation to ensure the risks and risk treatment plans are available. | Minor | Closed |

| NC04 | 6.1.2.A 1 | The organisation need to ensure the risk criteria for the ‘impact’ is conducted on all identified risks within the Risk Register. The impact criteria are not clearly defined within the business must be identified to highlight the negative affects to the business when scoring Low, Medium and High against confidentiality / integrity / availability. **Finding:** reviewed and documented within the report. | Minor | Closed |

| NC05 | 6.1.2 E | Residual Risks scoring will need to be included within the organisations Risk Register to identify if the risk has been accepted. Risk acceptance by the risk owner will need to be identified as per the management action log. **Finding:** reviewed and documented within the report. | Minor | Closed |

| OFI 03 | N/A | Whilst there have been only a couple of insignificant outages over the last 12 months – with the longest downtime of 2 hours with users unable to access sites due to a CDN endpoint issue – the Company may consider it beneficial to treat and record these real-time DR events at Information Security Incidents. | OFI | Closed |

| NC06 | A.17 | The following deficiencies were noted with the Business Continuity Plan (Issue 1.2 dated 12/10/20):  
- Whilst a number of primary/failover locations are listed, SE Asia to East Asia and SE Australia to East Australia are not included  
- Notifications and Analytics Unily Services that will not be available are not listed (section 4.1)  
- There is no testing strategy included which defines the regular testing intervals for this BCP scenario  
- Section 10.1 refers to more detailed procedures which are not listed in the appendices  
**Finding:** review of the organisations BCP plan was conducted updated with all information. | Minor | Closed |
Opening and Closing Meetings

Opening and closing meetings were performed in accordance with Form 335. The objective of the audit was to confirm that the management system had been established and implemented in accordance with the requirements of the audit standards.

Confirmed no changes to system scope since the organisations stage one remote visit.
- No unusual operations scheduled during this audit.
- No changes to company operations since previous audit.
- No major customer complaints or environmental / health and safety complaints or issues with delivering contractual requirements have occurred since previous audit.
- Discussed site visit requirements, required a minimum of once per audit cycle, to address any remote activities within scope.
- Discussed approach to audit and availability of personnel. Confirmed system scope, discussed and clarified business operations occurring on and off site and within the system scope.
- Discussed and justified any inapplicable clauses.
- Reviewed certificates.
- No changes of significance to management structure since previous audit.
- Reviewed previous report. No unusual activities scheduled. No issues arising with adhering to Audit Plan as prepared.

Findings closed out as per previous page
Process/audit area: Organisational Context (External / Internal issues /interested parties / boundaries and scope / process identification) A.5 information security policies / A.6 information security organisation & A.18 legal compliance

Auditees: James Heathcote
Auditor (if applicable): Jesse Culleton & Michael Harper

Evidence to support audit conclusion:

The following documents were reviewed/sampled as part of audit process:

- Information Security Management System Manual (Issue 1.5 dated 16/1/21 – Private)
- Register of Legal Obligations and Responsibilities (Issue 1.4 dated 16/1/21 – Private)
- Interested Parties, Authorities and Special Interest Groups (Issue 1.3 dated 16/1/21 – Restricted)
- 27001 Key Documentary Requirements spreadsheet (dated 24/1/18)

The ISMS Manual has recently been updated to reflect the Unily re-branding (as clarified within the Company Overview section) and internal organisational changes.

The organisation’s structure and integration was seen represented by an organogram within section 4.4 of the ISMS Manual.

Relevant internal and external issues were seen listed for assessment/treatment within the Information Security Risk Register and Treatment Plan spreadsheet.

The Needs and Expectation of Interested Parties was seen referenced within section 4.2 of the ISMS Manual and included a hyperlink to the Interested parties table, Reference: ISMS DOC.2, Issue No: 1.4, Issue Date: 10/11/2021 and classified as Restricted.

Sample of Interested Parties:

<table>
<thead>
<tr>
<th>Interested Party</th>
<th>Information Security Requirements</th>
</tr>
</thead>
</table>
| Directors        | • To ensure that the business continues to function in a profitable manner without hindrance and bureaucracy.  
|                  | • To ensure business information is kept confidential, available and reliable.  
|                  | • Oversee the overall running of the business.  
|                  | • Responsible for managing costs within the business.  
|                  | • Responsible for managing customer service.  
|                  | • Responsible for the growth of the company.  |
| Managers         | • To protect confidential employee information.  
|                  | • To protect client confidentially.  
|                  | • To ensure employment processes are followed.  
|                  | • To ensure training has been carried out from a quality and personal development point of view.  
|                  | • To ensure all relevant HR documentation is up to date.  
|                  | • To ensure records are maintained and kept up to date.  |
## Employees
- To protect client confidentially.
- To ensure employment processes are followed.
- To ensure all internal Policies and Procedures are followed.
- To take responsibility for their own training.
- To ensure that clients requests are adhered to all at times.

## Contractors
- To protect client confidentially.
- To ensure contractor processes are followed.
- To ensure all internal Policies and Procedures are followed.
- To take responsibility for their own training.
- To ensure that clients requests are adhered to all at times.

## Accountant
- To ensure that reports are given to the Directors in a timely fashion.
- To ensure that accounts are kept up to date
- To ensure that accounts are easily accessible for the Directors/Managers

## Solicitor
- To protect client confidentially.
- To ensure that clients requests are adhered to all at times.

## Clients
- Data to be used ethically in accordance with consent arrangements

## Hosting Services
- To protect client confidentiality
- To ensure hosting and related support services are delivered to a high standard.
- To ensure the charges are fair and in line with industry standards.

## UK Government
<table>
<thead>
<tr>
<th>Legal and regulatory authorities expect their requirements to be consistently and continually met. Data protection laws and regulatory requirements are particularly relevant to Unily including:</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Computer Misuse Act 1990</td>
</tr>
<tr>
<td>- Copyright (Computer Programs) Regulations 1992</td>
</tr>
<tr>
<td>- Data Protection Act 1998</td>
</tr>
<tr>
<td>- GDPR 2018 \ UK GDPR</td>
</tr>
<tr>
<td>- Human Rights Act 1998 (esp. Article 8)</td>
</tr>
<tr>
<td>- Electronic Communications Act 2000</td>
</tr>
<tr>
<td>- The Copyright, Designs and Patents Act 1988</td>
</tr>
<tr>
<td>- The Companies Act</td>
</tr>
<tr>
<td>- Privacy and Electronic Communications (EC Directive) Regulations 2003</td>
</tr>
<tr>
<td>- Equality Act 2010</td>
</tr>
<tr>
<td>- The Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011</td>
</tr>
<tr>
<td>- Defamation Act 2013</td>
</tr>
<tr>
<td>- The Electronic Communications Code (Conditions and Restrictions) (Amendment) Regulations 2013</td>
</tr>
<tr>
<td>- Data Retention and Investigatory Powers Act 2014</td>
</tr>
</tbody>
</table>

## US Government
- US Privacy Act of 1974
- Californian Consumer Privacy Act (CCPA) 2020
- Equal Employment Opportunity Policy
- Non-Discrimination and Anti-Harassment Policy

## Australian Government
- Privacy Amendment (Private Sector) Act 2000
- Commonwealth Privacy Act 1988
Within section 5 of the interested parties’ document, all special interest groups and authorities have been documented with links to website.

Sample of Special interest Groups and Authorities:

<table>
<thead>
<tr>
<th>Name</th>
<th>Subject</th>
<th>Web site</th>
</tr>
</thead>
<tbody>
<tr>
<td>UK Government</td>
<td>Running a Business</td>
<td><a href="https://www.gov.uk/browse/business">https://www.gov.uk/browse/business</a></td>
</tr>
<tr>
<td>Qualys</td>
<td>Vulnerability &amp; Security for Web Applications</td>
<td><a href="https://qualysguard.qg2.apps.qualys.eu">https://qualysguard.qg2.apps.qualys.eu</a></td>
</tr>
<tr>
<td>BT (British Telecom)</td>
<td>Data Bearer, Connectivity issues</td>
<td><a href="https://business.bt.com/products/broadband">https://business.bt.com/products/broadband</a></td>
</tr>
<tr>
<td>Umbraco</td>
<td>Core of Unily Product, Security Updates, Best Practices</td>
<td><a href="https://umbraco.com">https://umbraco.com</a></td>
</tr>
<tr>
<td>SendGrid</td>
<td>Used for SMTP messaging within the Unily platform</td>
<td><a href="https://sendgrid.com/policies/security/">https://sendgrid.com/policies/security/</a></td>
</tr>
<tr>
<td>Elastic</td>
<td>Core of Unily Product, Security Updates, Best Practices</td>
<td><a href="https://www.elastic.co/community/">https://www.elastic.co/community/</a></td>
</tr>
<tr>
<td>Microsoft Group</td>
<td>Best Practises, Security &amp; Vulnerabilities, Emerging Product features, Client Impacting changes</td>
<td><a href="https://portal.office.com">https://portal.office.com</a></td>
</tr>
<tr>
<td>Microsoft Partner Centre</td>
<td>Microsoft Gold Partner</td>
<td><a href="https://partner.microsoft.com/">https://partner.microsoft.com/</a></td>
</tr>
</tbody>
</table>

The legal register document was seen recently updated with clarification to BREXIT (modal clauses and operating procedures reviewed and updated as necessary) and GDPR (data transfer aspects). The COO has been working with local external lawyers to review/update contracts and handling of data internally (GDPR).
Unily acts as a data processor= s/w/processing of customer data / and as a data controller for internal staff information. James Heathcote is also the nominated Data Protection Officer for the organisation.

The Privacy Notice is available at the bottom of the homepage of both the Unily and Unily .com websites.

Within the Register of Legal Obligations and Responsibilities, ISMS Doc.1 issue 1.5 dated 16122021, all identified legal and regulatory required have been documented with the following headings:

- Key provisions
- Owner
- Reviewed date
- Clause/Annex A control ref

Sample of identified legal compliance:

- General Data Protection Regulations 2018
- UK GDPR
- California Privacy Act 2020
- Network and Information Systems
- Regulations 2018
- China Personal Information Protection Law 2021 (PIPL)
- Copyright Designs and Patents Act 1988
- Computer Misuse Act 1990

The organisation continues to have an annual SOC 2 assessments undertaken are undertaken by Linford & Co LLP (law firm) encompassing a 5-day data review. The Type II SOC 2 Controls relevant to security, availability and confidentiality report dated 01/04/2020 to 01/03/2021 was evidenced with no findings raised and no follow-up actions required.

The Pentest organisation conducted an External Infrastructure and Web Application Assessment. The corresponding report (dated 12/11/2021) was seen to highlight 1 low risk item which has now been mitigated.

The Microsoft Secure Centre application is continually running in the background, providing an ongoing technical compliance review, and was seen to show a current effectiveness of IS controls score of 88%. It was affirmed that Managers are involved in internal audits when checking that IS policies and procedures are up to date and reflect current working practices.

**Conclusion of the overall effectiveness of the process:** Process/ Audit Area is satisfactory - best practice(s) identified
<table>
<thead>
<tr>
<th>Process/audit area:</th>
<th>Leadership (Process based approach, risk based thinking, policy, identification of roles and responsibilities)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auditees:</td>
<td>James Heathcote / Lyk Calligeris / Mark Sahal</td>
</tr>
<tr>
<td>Auditor (if applicable):</td>
<td>Jesse Culleton &amp; Michael Harper</td>
</tr>
</tbody>
</table>

**Evidence to support audit conclusion:**

Undertook Leadership interview with James Heathcote, Information Security Manager, and Changes within the board with new board members joining due to new investors. As discussed this will not change the ISMS Changes to the management structure.

CHIEF Operations Officer (COO) Mark Sahal who was added within the ISMS in November 2021 who takes part in the management review. New starters and leavers was discussed and has been documented due to the pandemic and finding new jobs due to be able to work from home.

Investment into the ISMS systems was discussed with ServiceNow managing and being used for the joiners and leaver process which went live in January 2022.

The office has not required any changes. Internal processes have been reviewed for client site with the introduction of PIMS which allows for the organisation to maintain access to customer’s sites and reduce risks.

An increase in risks relating to threats globally due to the increase of IT threats worldwide and phasing attacks. The organisation has subscribed to Microsoft Threat Experts which give assistance and consultation to threats.

Fully discussed, assessed and reviewed:

- Accountability for the effectiveness of the management system,
- The Policy and system objectives,
- The integration of the management system requirements into the core business processes,
- The use of the process approach and risk-based thinking,
- The resources provided and availability,
- The means of communicating the importance of the management system and of conforming to the management system requirements,
- The means of ensuring that the management system achieves its intended results,
- The means of engaging, directing and supporting people to contribute to the overall effectiveness of the management system,
- The promotion of improvement,
- The support provided to other relevant management roles to demonstrate leadership as it applies to their areas of responsibility,

Leadership and commitment levels have therefore been adequately demonstrated.

Documented within the Information Security Management system Manual, ISMS Doc 0, Issue 1.5 dated 16/01/2021 and classified as Private, the management structure has been reviewed to include new roles within the business.
A Sample of Organisation Chart was undertaken during the remote audit process.

The 27001 Key Documentary Requirements spreadsheet was seen to provide cross-references to ISO 27001 clauses and controls for ISMS documents. The Controlled Document List spreadsheet was also evidenced as listing all of the IS Policies within the ISMS. ISMS documentation was seen stored within a SharePoint site accessible to all staff and all relevant policies are reviewed annually as part of the internal audit schedule.

Section 5.3 of the ISMS Manual was seen to define IS roles and responsibilities including:

- Members of the Information Security Steering Group, viz: CTO, Global Head of People, Director of Operations and the IS Manager
- RACI table showing the responsibilities (R=Responsible, A=Accountable, C=Consulted, I=Informed) of the Information Security Steering Group, Director of Operations, HR Managers, IS Manager/Admin/Auditor, Department Managers and Staff against the clauses and Annex A controls of ISO 27001
- Further details of the key roles, responsibilities and authorities for the: Information Security Steering Group; CTO; Information Security Manager/Administrator/Auditor; Department Managers; Operations Team and Staff

A Documented Information Security Policy, ISMS Doc.3, issue 1.2 dated 23/06/2020 and classified as Public. The organisation IS Policy has been signed by Sam Hassani on the 23/06/2020 and reviewed on the 17/06/2021 with no changes documented within the change history record table.

The IS policy is made available to all internal employees via the Intranet system and will read during the induction process for all new starters. All external parties can request to view the policy as classified as public. All visitors to site will read and sign during the visitor sign in process.

ISMS responsibilities have been identified in order to ensure its effective management and development. The information steering group is details as follows:

Employee Contracts together with job descriptions have been defined to outline each role within the organization together with their related responsibilities and authorities; ensuring that that the appropriate personnel are in place to cover the entire organisation and strategy of the business.

Unily has defined and allocated all ISMS responsibilities in order to ensure its effective management and development. The information steering group is details as follows.

Overall responsibility for the management of the various areas of the ISMS is shown in the following RACI table. This defines the type of responsibility of each role in each area according to whether the listed role is:

```
Sam Hassani (CTO)

Victoria Martindale (Global People Director)
Lyk Calligeris (Director of Operations)
James Heathcote (Information Security Manager)
```
Overall responsibility are documented and recorded using a RACI table to ensure all persons within the organisation know if they are: -
- R = Responsible
- A = Accountable
- C = Consulted
- I = Informed

An Information Security Steering group is implemented within the organisation to ensure all information relating the ISMS is reviewed, appropriate and communicated throughout the organisation. All roles from top management down to staff are documented to ensure all IS responsibilities are identified.

Roles and responsibilities for all roles within the organisation have been documented and include:

- **The Information Steering Group**
  - The Information Security Steering Group oversees the operation of the ISMS as a representative of top management within Unily and has overall responsibility for its effectiveness. The group is made up of the members of the Senior Management Team. This group has the following responsibilities:
    - Establish and maintain the ISMS policy, objectives and plans
    - Communicate the importance of meeting the objectives and the need for continual improvement throughout the organization
    - Maintain an awareness of business needs and major changes
    - Ensure that information security requirements are determined and are met with the aim of minimizing risk and maintaining effective controls for Unily and for our customers
    - Determine and provide resources to plan, implement, monitor, review and improve information security and management e.g., recruit appropriate staff, manage staff turnover
    - Oversee the management of risks to the organization and its services

### Roles and Responsibilities

<table>
<thead>
<tr>
<th>ISO/IEC 27001 Area</th>
<th>Information Steering Group</th>
<th>Chief Operations Officer</th>
<th>Chief Technology Officer</th>
<th>Director of Operations</th>
<th>Director of Finance</th>
<th>Director of Client Services</th>
<th>Global People Director</th>
<th>Global Head of Engineering</th>
<th>Information Security Manager</th>
<th>Office Manager</th>
<th>Information Security Admin</th>
<th>Information Security Auditor</th>
<th>Department Managers</th>
<th>Staff</th>
</tr>
</thead>
<tbody>
<tr>
<td>Context</td>
<td>A/R</td>
<td>A/R</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>C</td>
<td>C</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td>C</td>
<td>I</td>
<td></td>
</tr>
<tr>
<td>Leadership</td>
<td>A/R</td>
<td>A/R</td>
<td>A</td>
<td>A/R</td>
<td>A</td>
<td>R</td>
<td>A</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td>C</td>
<td>I</td>
<td></td>
</tr>
<tr>
<td>Planning</td>
<td>A/R</td>
<td>A/R</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>R</td>
<td>A</td>
<td>R</td>
<td>I</td>
<td>C</td>
<td>I</td>
<td>C</td>
<td>I</td>
<td></td>
</tr>
<tr>
<td>Support</td>
<td>A/R</td>
<td>A/R</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>R</td>
<td>A</td>
<td>R</td>
<td>C</td>
<td>I</td>
<td>C</td>
<td>I</td>
<td></td>
</tr>
<tr>
<td>Operation</td>
<td>A/R</td>
<td>A/R</td>
<td>A/R</td>
<td>R</td>
<td>A/R</td>
<td>R</td>
<td>C</td>
<td>R</td>
<td>I</td>
<td>R</td>
<td>R</td>
<td>C</td>
<td>I</td>
<td></td>
</tr>
<tr>
<td>Performance evaluation</td>
<td>A/R</td>
<td>A/R</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>R</td>
<td>A</td>
<td>R</td>
<td>C</td>
<td>C</td>
<td>R</td>
<td>R</td>
<td>I</td>
<td></td>
</tr>
<tr>
<td>Improvement</td>
<td>A/R</td>
<td>A/R</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>R</td>
<td>A</td>
<td>R</td>
<td>A</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td></td>
</tr>
<tr>
<td>Annex A Controls</td>
<td>A/R</td>
<td>A/R</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>R</td>
<td>A</td>
<td>R</td>
<td>A</td>
<td>R</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td></td>
</tr>
</tbody>
</table>
- Conduct management reviews of information security, at planned intervals, to ensure continuing suitability, adequacy and effectiveness
- Select auditors and ensure that internal audits are conducted in an objective and impartial manner
- Establish a continual improvement mentality with respect to information security for Unily;
- Review major information security incidents
- Ensure that arrangements that involve external organizations having access to information systems and services are based on a formal agreement that defines all necessary security requirements

The Information Security Steering Group has the authority to approve significant expenditure on information security-related matters, recruit additional resources for the management of information security, approve high-level policies for information security and initiate high-level incident management actions.

- **Chief Technology Officer – Sam Hassani**
  - Has overall responsibility for ISMS including authorisation of the Information Security Policy Statement. The CTO requires that all directors, managers and staff be aware of this policy and adhere to its inclusions. The CTO has authority for approving all processes, procedures and policies on behalf the board.

- **Chief Operations Officer – Mark Sahal**
  - Is responsible for the day to day operations of business. Works directly with legal advisors to ensure relevant processes and activities conform to global laws applicable to business. Manages the team responsible for Contracts and Agreements. Coordinates departments and managers to ensure business objectives are met, provides communication to all staff and contractors.

- **Director of Finance – Chris Jackman**
  - Has overall responsibility for all financial operations and financial reporting across the business. This covers day to day operations ensuring business continuity, complying with relevant law and reporting, both internally and externally to the board. Working with other key management across the business, Finance produces the business plan which incorporates the long-term strategic aspirations and focus for the company for the coming years.

- **Information Security Manager – James Heathcote**
  - The Information Security Manager is the primary role with a dedicated focus on information security and related issues and has the following responsibilities.
    - Reporting to the Information Security Steering Group on all security related matters on a regular and ad-hoc basis when required
    - Communicate the information security policy to all relevant interested parties where appropriate, including customers
    - Implement the requirements of the information security policy
    - Manage risks associated with access to the service or systems
    - Ensure that security controls are in place and documented
• Quantify and monitor the types, volumes and impacts of security incidents and malfunctions
• Define improvement plans and targets for the financial year
• Monitor achievement against targets
• Establish and maintain a continual improvement action list
• Report on improvement activities
• Identify and manage information security incidents according to a process;
• Attend management review meetings on a regular basis.

The Information Security Manager also has the authority to declare information security incidents, approve limited expenditure on information security-related matters and review the operation of controls within all business areas.

- Information Security Administrator – James Heathcote
  o The Information Security Administrator is a technical role involved in the implementation and maintenance of many of the controls used to manage risk and has the following responsibilities:
    ▪ Ensure that security controls are in place and documented;
    ▪ Manage the day to day maintenance of controls, including:
    ▪ Access control (user account lifecycle)
    ▪ Testing and implementing security patches
    ▪ Vulnerability scanning
    ▪ Software operation e.g. IDS, IPS, firewalls, DLP
    ▪ System and network hardening
    ▪ Remote access
    ▪ Cryptographic key management
    ▪ Log management
    ▪ Identify and manage information security incidents according to a process

The Information Security Administrator’s authorities are to take action to prevent an information security incident from occurring or escalating, where possible and to maintain information security records in accordance with defined policies and procedures.

- Information Security Auditor – James Heathcote
  o The Information Security Auditor fulfils the internal audit requirements of the ISO 27001:2013 standard and is generally responsible for checking that the ISMS is effectively implemented and maintained. Responsibilities are as follows:
    • Plan, establish, implement and maintain an audit programme including the frequency, methods, responsibilities, planning requirements and reporting
    • Define the audit criteria and scope for each audit
    • Conduct internal audits at planned intervals
    • Ensure the audit process is objective and impartial
    • Report the results of audits to relevant management
    • Retain documented information as evidence of the audit programme and the audit results
The Information Security Auditor has the authority to investigate information security-related procedures and controls in order to assess their suitability and effectiveness and report findings to relevant management.

Unily has also defined the following roles with Information Security Responsibilities and authorities:

- **Department Managers**
  - Department Managers may be heads or supervisors of operational units within the organization and are responsible for:
    - Reviewing and managing employee competencies and training needs to enable them to perform their role effectively within the information security space
    - Ensuring that employees are aware of the relevance and importance of their activities and how they contribute to the achievement of information security objectives.
  
  Department Managers have the authority to arrange training and awareness activities for the employees under their direction, within budget constraints and take action to prevent an information security incident from occurring or escalating, where possible.

- **Operations Team**
  - Due to the often technical nature of information security issues, engineers have an important part to play in the ISMS. Their responsibilities include:
    - The operation of processes such as incident and change management
    - The provision of technical expertise in matters of information security
    - The implementation of technical controls
    - System administration e.g., user creation, backups
    - Security monitoring e.g., network intrusions
    - System provisioning
  
  Engineers have the authority to take action to prevent an information security incident from occurring or escalating, where possible.

- **Staff**
  - The responsibilities of the staff are defined in a variety of organization-wide policies. All members of staff have the following main responsibilities:
    - Ensure they are aware of and comply with all information security policies of the organization relevant to their business role
    - Report any actual or potential security breaches
    - Contribute to risk assessment where required
  
  Staff have the authority to take action to prevent an information security incident from occurring or escalating, where possible.

**Conclusion of the overall effectiveness of the process**: Process / Audit Area is satisfactory
<table>
<thead>
<tr>
<th>Process/audit area:</th>
<th>Performance Evaluation and Improvement Processes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auditees:</td>
<td>James Heathcote</td>
</tr>
<tr>
<td>Auditor (if applicable):</td>
<td>Jesse Culleton &amp; Michael Harper</td>
</tr>
</tbody>
</table>

**Evidence to support audit conclusion:**

**Management Review**


**Sampled:**

- Procedure – ISG Review Template, Doc ISMS form.9, - issue 1.1 dated 22/01/2021 – classified as Restricted

The organisations has set up a reoccurring steering Group meeting which will be held quarterly.

The organisation has determined all information that requires is monitoring and measuring via the security objectives, opportunities for improvements and all risk relating to the daily operations of the business. All monitoring and measuring of objectives, risks and improvements is discussed during the fortnightly meetings, management review meetings, Ticketing analysis and trends and SLA and open incidents.

Minutes of most recent meeting, held 04/11/2021. Attended by:

- L Calligeris – Director of Operations
- C Jackman – Finance Director
- V Martindale – HR Director
- L Kindy – Office Manager
- J Heathcote
- R skilton – Head of Client Services
- M Harding – Head of Product engineering
- T Moxon – Senior Product engineers
- M George – senior product engineers

Confirmed that all mandatory input and output requirements have been achieved. Detail includes:

1. The status of action from previous management reviews
2. Changes to internal and external issues
3. Feedback from IS performance including trends
4. Feedback from interested Parties
5. Results of Risk Assessment and status of risk treatment plans
6. Opportunities for improvement
7. Any other business
8. Date of next meeting

The organisation also holds Hall Towns meetings to review the business and performance (customer satisfaction), employee engagement survey, diversity and inclusion, internal alignment and priorities which is reported to all employees within the business via the organisations Intranet system (Rockstarrs), the last town hall was held on the October 2021.

The next meeting is planned for February 2022.
**Internal Audits**

Reviewed internal audit processes, sampled as follows:

- Procedure - Information Security Management system Manual, ISMS Doc 0, Issue 1.5 dated 16/01/2021 and classified as Private (Section 9.2 Internal audits)
- Audit Schedule, 2021/2022, ISMS REC.7, issue 1.2 dated 11/12/2020
- Initial Audit Report, ISMS form.0, issue 1.0 dated 04/11/2017 and classified as restricted

A review of the Audit schedule 2019/2020 Programme internal audits against procedural requirements and system arrangements. The organisation has a documented 2021/2022 schedule is available and will be used to conduct all internal audits throughout the year.

All internal audits will be reported within the initial Audit report, ISMS Form.0, issue 1.0 dated 04/07/2017 which is classified as restricted.

**Sample of Internal Audits:**

- Report No: 2021/12
- Date: 18/12/2021
- Scope & Type of Audit: Full audit of clauses 4 to 10 and the associated controls A5 to A18 as detailed below.
- Site: The Granary, Abbey Mill Business Park, Lower Eashing, Godalming, Surrey, GU7 2QW
- Auditor: J Heathcote
- Finding: Zero

All audits undertaken by James Heathcote, internal auditor, with the exception of system administration processes, undertaken by Sam Hassani to provide impartiality.

**Non Conformity and Corrective Action**

Reviewed Non Conformity and Corrective Action processes, sampled as follows:

- Management Action log, ISMS Rec.7, issue 1.1 dated 22/01/2018, classified as private (Live data)

Methods used for collecting information and identifying areas of improvement are:

- Internal audits
- Internal and 3rd party feedback
- Penetrations tests
- Vulnerability assessments
- Business Continuity Plans tests
- IT Operations logs

Since the organisation previous visit, a total of 6 actions logged which included:
Confirmed that the corrective action as sampled have been effective in addressing the non-conformity and in preventing its recurrence.

Continual improvement is monitor via the risks & opportunities analysis, Information Security Policy and objectives. All continual improvement is monitored via several dashboards within the service desk system with all changes to the clients system and services monitored and recorded within the dashboard against the documented SLAs and requests.

Objectives

The Information Security Objectives spreadsheet (Issue 1.4 dated 22/01/2022- Restricted) is used by the organisation and documents all objectives using the following headings:

- Objective
- Target
- Plan of how objectives are to be achieved
- Responsibility
- Comments

The Organisation has a total of 5 IS objectives recorded and include:

<table>
<thead>
<tr>
<th>Objectives</th>
<th>Target</th>
</tr>
</thead>
<tbody>
<tr>
<td>To achieve and retain certification to ISO 27001:2013 and SOC2</td>
<td>2017-</td>
</tr>
<tr>
<td>Ensure % of internal audits completed on time</td>
<td>&gt;95%</td>
</tr>
<tr>
<td>Trend of number of security incidents reported per quarter decreasing</td>
<td>0</td>
</tr>
<tr>
<td>Ensure % of system/network uptime per month/quarter</td>
<td>99.95%</td>
</tr>
<tr>
<td>Review and Investigate Microsoft Azure Security Centre Alerts &amp; Recommendations weekly</td>
<td>&gt;95%</td>
</tr>
<tr>
<td>Ensure % of Security Incidents resulting in Data Breaches are notified to clients within 48 hours</td>
<td>100%</td>
</tr>
<tr>
<td>Review Security Incidents daily, both ServiceNOW &amp; Azure Sentinel</td>
<td>&gt;95%</td>
</tr>
<tr>
<td>Achieve Greater than % Baseline for Microsoft Security Centre Secure Score</td>
<td>&gt;80%</td>
</tr>
<tr>
<td>Ensure % Patch Compliance for Servers and Desktops within 14 days of release</td>
<td>100%</td>
</tr>
<tr>
<td>Ensure security risks and recommendations from Penetration \ Vulnerability reports are analysed within 7 day</td>
<td>95%</td>
</tr>
<tr>
<td>Ensure all major product releases are independently tested and verified</td>
<td>Qlty</td>
</tr>
<tr>
<td>Ensure % of Security Vetting performed on sensitive roles</td>
<td>100%</td>
</tr>
<tr>
<td>Ensure % of staff complete mandatory staff training within 4 weeks</td>
<td>100%</td>
</tr>
<tr>
<td>Ensure assets are removed securely when appropriate</td>
<td>100%</td>
</tr>
<tr>
<td>Ensure premises are secure % of time</td>
<td>100%</td>
</tr>
<tr>
<td>Ensure % unsuccessful client site production deployments</td>
<td>0%</td>
</tr>
</tbody>
</table>

As discussed, the organisations objectives are discussed, documented and reviewed during the management review meeting (ISG)

Conclusion of the overall effectiveness of the process: Process / Audit Area is satisfactory
Process/audit area: Planning

Auditees: James Heathcote
Auditor (if applicable): Jesse Culleton & Michael Harper

Evidence to support audit conclusion:

As discussed, the Organisation has reviewed the IS risk register and treatment plan as part of the minor NCRs raised during the reassessment visit in 2021. Information Security Risk Register and Treatment Plan spreadsheet, IMS REC.2 1.2 dated 06/02/2021 – and classified as Restricted

The Information Security Risk Management Policy was seen to define a Risk Management Framework covering:

- Risk Assessment
- Risk Mitigation
- Risk Communication
- Risk Monitoring and Review

Risk values are calculated by multiplying Impact Scores by Likelihood Scores. Impact and Likelihood are rated Low, Medium or High with respective numerical values of 1, 2 or 3. Criteria for L/M/H Likelihoods was seen defined in terms of occurrence in time periods.

Numerical Risk Values are calculated and will score between 1 and 9. Risks scoring 2 or below are considered acceptable (requiring no further action). All other risks (scoring 3 or more) will require review and one of the risk treatment types assigned.

Risk assessments are conducted annually (the most recent being undertaken in January 2021), or whenever significant change occurs, as identified by the Senior Management Team.

The Information Security Risk Register and Treatment Plan spreadsheet was seen to list risks with the following column fields defined and completed:

- Asset
- Risk description
- Risk Owner
- C I A (1 or 0)
- Score
- Likelihood (1 to 3)
- Risk Score
- Status
- Action
- Control
- Acceptance
- Accept date
- Accepted by
- Short Term Mitigation / Risk Treatment Plan
- Control Reference
- Risk Treatment Type (Treat/Transfer/Terminate)
A total of 135 risks, with a total of 4 high risk (Red), 4 medium risks (Amber), 34 (3 score). As discussed, all risks with a score above 3 will be treated, Transfer or Terminate. This terminology is now used consistently within the Risk Register and the Management Action Log and a unique Log. No. is assigned to correlate entries in each of these documents.

The risk owner’s approval of the treatment plan for each TREAT/TRANSFER/TERMINATE IS risk was seen recorded in the Management Action Log in the Authorised By column. The Verified By and Date Corrective Action Verified as Completed columns in the Log record the results of (completed) IS risk treatment.

**Sample of Risk Register,**

- **Asset:** Unily
  - **Risk description:** risk of exploit / damage to reputation / financial penalty due to outdated libraries,
  - **Risk owner:** Tech Operations
  - **Risk Score:** 6
  - **Status:** Treat
  - **Action:** Ensure secure process exists update libraries
  - **Accepted by:** M H
  - **Residual risk score:** 6
  - **Log No:** 30

- **Asset:** Premises
  - **Risk description:** environmental disaster
  - **Risk owner:** Facilities
  - **Risk Score:** 1
  - **Status:** accept
  - **Action:** Ensure all equipment is taken home
  - **Residual risk score:** 1
  - **Log No:** N/A

Within the management action log, all risks requiring a risk treatment and actions will be documented and allows for the organisation to conduct a full risk assessment and root cause analysis to allow for corrective action to be taken and the risk to be treated, Transfer or Terminated.

The Statement of Applicability, ISMS REC.3 issue 1 dated 17/01/2018 with the last review conducted on the 22/01/2022 with no changes made. Within the SoA all information is documented using the following headings:

- **Control Ref**
- **Control**
- **Control description**
- **Applied**
- **Justification for exclusion**
- **Control / implemented**
- **Business requirement or best practice**
- Risk assessment
- Contractual or Regulatory

Confirmed, the Organisation has No exclusions were justified and all controls have been implemented.

As discussed, all risk assessment have been documented against the Annex A controls within the risk register and risk treatment spreadsheet and sampled; (A.8.1.2 & A.7.1.1).

**Conclusion of the overall effectiveness of the process:** Process / Audit Area is satisfactory
AUDIT REPORT PART B – AUDIT REPORT

<table>
<thead>
<tr>
<th>Process/audit area:</th>
<th>Physical and Environmental Security A.11</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auditees:</td>
<td>Laurel Kindy / James Heathcote</td>
</tr>
<tr>
<td>Auditor (if applicable):</td>
<td>Jesse Culleton &amp; Michael Harper</td>
</tr>
</tbody>
</table>

**Evidence to support audit conclusion:**

Brightstarr, trading as Unily, occupy the first floor and a large part of the ground floor of a converted old building on an island in the River Wey near Godalming, Surrey. The ground floor is also used by other organisations but these do not share the Brightstarr/Unily office space.

The organisation continues to offer working from home as the organisation had in place a mobile working process in place prior to the pandemic. MS Teams was used by the organisation which allowed for remote working to be imbedded from the first lockdown.

A full remote audit of the office area was conducted via using Teams on a mobile phone.

**Entrance**
- 2 entrances, a staff entrance for the ground floor and a visitors entrance to the reception on the first floor.
- CCTV signage was visible
- Door entry system – staff have key fobs
- Anti-pass back system so if staff don’t fob in they can’t fob out. This reduces risk of tailgating.
- A Ring door bell was fitted to the ground floor
- Keypad entry system
- Doors also have physical keys
- Inside the building there is a reminder to close windows when leaving the office empty
- Windows are secured with anti-tamper locks
- Ground floor shutters are closed out of hours

**Visitors process:**
- Visitors enter by ground floor and take stairs to first floor
- Speak to reception via intercom
- Double doors to the outside are locked, then there’s a small lobby, followed by a set of fire doors.
- Reception can see all visitors as they enter
- Sign reminding visitors to sign in
- Visitors have to sign in to iPad system acknowledging
- who they are meeting, Name, Company, car reg, covid questions, visitor agreements
- Visitors have to sign out when leaving the building
- Visitor must wear visitor lanyards & be escorted throughout the building
- Copies of Visitor & Info Sec policy in reception

It is not a Brightstarr policy to require staff to wear staff ID badges. The staff directory has photos of everyone which is considered adequate for identification.

Covid precautions
- Screens, hand sanitisers, door system used for track and trace

Legal and H&S notices displayed by Multifunction Printer, which was clear of unclaimed documents
Cross hatch shredder for shredding of ordinary documents. Shredded paper is disposed of by Laurel.

Financial data is shredded annually by Shred-it.
- Evidence: Shred-it invoice #9504161487
- Fire extinguishers all around the office.
- Last serviced 10/21
- Fire Risk Assessment dated 11 October 2021 by Camden Council Safety Division

Finance & HR cupboard is secured. It contains:
- Confidential docs in locked cupboards
- Fire proof safe which holds contracts
- There are very limited keys to the safe.

Server room is secured. It contains:
- Enough networking equipment to connect the office to the cloud
- Equipment is supported by UPSs, which are tested annually and are maintained by Schneider Electric. Evidence: Smart-UPS 1500, Health OK, Next Battery Replacement date 08/11/2023
  (possibly US date format) Smart-UPS 2200, Next Battery Replacement date 27/Sept/2022

A Clear Desk Policy is in place and appears to be working effectively.
Staff have their own pedestals but can’t lock them and shouldn’t leave anything in them overnight due to flexible working.
- Evidence: Asset Management Policy (v1.8, 01/11/2021), Section 7.0

Air conditioning is maintained by Brightstarr/Unify.
Cabling is secured & wireless access is on VLANS. Equipment is protected by anti-tamper screws.
Internal CCTV is backed up to the cloud (System Sampled). It is GDPR compliant and the retention period is covered in the Asset Management Policy.
Evidence: Asset Management Policy (v1.8, 01/11/2021), Section 13

Downstairs is similar to upstairs.
- Comms cabinets are high up the wall and are locked.
- There is a kitchenette with information boards.

**Contingency plans for river flooding**
- Monitoring from Environmental Health authority
- Covered in BCP & Risk
- People can work effectively from home

**Evidence:** IS Risk Register and Risk Treatment Plan (Environmental disasters). Risk Score is 1, they are accepting the risks. There is no corresponding action log as it has a low score.

**Evidence:** Business Continuity Plan (v1.5, 11/03/2021)

**Conclusion of the overall effectiveness of the process:** Process / Audit Area is satisfactory
<table>
<thead>
<tr>
<th>Process/audit area:</th>
<th>Operational Process – Client Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auditees:</td>
<td>Rachael Skilton</td>
</tr>
<tr>
<td>Auditor (if applicable):</td>
<td>Michael Harper</td>
</tr>
<tr>
<td>Evidence to support audit conclusion:</td>
<td>Rachael is Director of Client Services. She oversees the implementation and customer successes teams in EMEA and North America. The process takes customers post sale through implementation to contract renewal.</td>
</tr>
<tr>
<td></td>
<td>Limited information is passed from sales. This includes licences and standard documentation which is tailored to the customer depending in where their data sits and customer’s goals.</td>
</tr>
<tr>
<td></td>
<td>Her team works with sales on forecasting so they can see what’s about to be signed and plan resources accordingly. Head of implementation appoints a team of an implementation manager and a consultant.</td>
</tr>
<tr>
<td></td>
<td>From post sales to implementation there are five stages with gate reviews between each stage. Stages involve review and sign off. To launch a new product there is a Checklist for Launch followed by a table top review with teams then a period of stability before going live.</td>
</tr>
<tr>
<td></td>
<td>A Customer Success Manager is introduced to the customer. They set up site analytics with the customer. Handover from implementation to the CSM takes place after two weeks.</td>
</tr>
<tr>
<td></td>
<td>The control for this process is the Project Management Policy (ISMS DOC.21, v1.1, 14/08/2021)</td>
</tr>
<tr>
<td></td>
<td>Information on the customer is stored in the product, in Salesforce CRM, and in Service Now (SNOW).</td>
</tr>
<tr>
<td></td>
<td>The access staff have to information depends on their profile. This is set when people join the company via a New Starter Request in Service Now. Access to groups is largely based on the Department people are members of.</td>
</tr>
<tr>
<td>Examples</td>
<td>MC. Based in New York Office. Is a member of US Implementation and US Staff?</td>
</tr>
<tr>
<td></td>
<td>As a member of US Implementation he has access to Salesforce.</td>
</tr>
<tr>
<td></td>
<td>RD. Based in the UK. Is a developer.</td>
</tr>
<tr>
<td></td>
<td>Has access to Visual Studio but NOT to Salesforce.</td>
</tr>
<tr>
<td></td>
<td>This is controlled by the Human Resource - Security document (ISMS DOC.6, v1.2, 03/12/2021)</td>
</tr>
<tr>
<td></td>
<td>For customer data Brightstarr acts as a data processor only. The product may have PII but the client is data controller. This is covered by the SOC audit.</td>
</tr>
<tr>
<td></td>
<td>Only client’s information is stored in their product.</td>
</tr>
<tr>
<td></td>
<td>James demonstrated the new PIMS tool that has been developed in house at Brightstarr.</td>
</tr>
<tr>
<td></td>
<td>The process is:</td>
</tr>
<tr>
<td></td>
<td>Unily Site Access Request</td>
</tr>
<tr>
<td></td>
<td>Decide if you want access to the customer’s staging site or production site</td>
</tr>
</tbody>
</table>
Enter the client name
For Production enter the Service Now number for the issue being investigated if admin access is needed
Choose Read Only or Admin
Enter the site
Site access is time limited for support but not for the implementation team who might need to spend a lot of time on the site developing it.

This is documented in the Intranet (RockStarrs) but not yet written up as a policy or process. The purpose of this Personal Identity Management System is to control access to customer’s sites and to audit who accessed the site, for how long, when and why. If something goes wrong Brightstarr can check who made a change leading up to the incident.

**Conclusion of the overall effectiveness of the process:** Process / Audit Area is satisfactory
Process/audit area: A.7 HR Support including, competency, awareness and resources

Auditees: James Heathcote / Victoria Martindale / Chrissy Stapleton

Auditor (if applicable): Jesse Culleton & Michael Harper

Evidence to support audit conclusion:

As discussed during the remote audit process with Victoria Martindale (Global People Director) and Chrissy Stapleton (HR Manager), the organisation’s HR process has not changed over the past year. Recruitment conducted via various avenues but firstly conducted via Team Trailer system is used to approve all recruitment requests which will track all applicants allowing for the organisation to monitor and screen all applicants for the role. Other recruitment sites used included LinkedIn, Recruitment sites and referrals from employees. An initial call will be held with the candidate prior to the secondary interview process starting. This will be with department managers and assistance given by the HR department.

All roles and responsibilities have been documented within the set templates used for advertising the role and a job description unless a bespoke role where a new template is required.

Sample of Job descriptions:

- Job title: talent Acquisition Partner
  - Issue 1, approved via Team Tailor – C J
  - Line manager: Global People Director

The interview process will be undertaken via telephone and/or MS Teams call with secondary peer interview. This is dependent on the role.

All recruits will undergo a full background screening check which are conducted by the organisation’s 3rd party supplier HireRight. Checks will include:

- Passport
- Driving licence
- Proof of address
- Right to work
- 2 x references
- DBS checks

A T&Cs will then be sent to the candidate to electronically sign via DocuSign and return to the organisation with all details of employment mentioned. All T&Cs will be held within the personnel fill within the HR system in the OneDrive (SharePoint). Restricted access to the HR drive in place and evidenced.

All new access to the Drive will be requested via ServiceNow system access request.

All new employees will have a new starter form completed via ServiceNow system and a ticket raised to arrange for the account to be set using the automatic set up for the department the recruit will be working in. This will include the online system (RockStars) with HR will conducted an introduction to the office and induction to office and fire Safety tours etc. All IT equipment will then be issued and access granted to the employee.
All training and awareness are completed online within the Rockstarrs intranet system with a mandatory reading tab on the first screen which has to be completed before the employee can access the rest of the system.

This includes the introduction to the ISO, document location and key policies. A PowerPoint presentation will then be accessible – Information Security Management System Awareness Training ISO27001:2013. This PowerPoint presentation meets the requirements of the international standard for awareness. An e-learning system is currently being reviewed and will be used to include a training package for all employees to complete to evidence competency.

Within the CMS section of the Rockstarrs system, the organisation is able to monitor all employees that have completed the mandatory training for information security for all annual refresher training completed. The organisation new Traliant system being put in place at present will be fully in place and reviewed during the next surveillance visit.

Sample of Training and awareness:

- Training: Data Privacy, GDPR & Information Security
- Total assessment (Global): 222
- Completed assessments: 208
- Uncompleted: 14

A review of the uncompleted training was undertaken and only 3 within UK.

All new starters will have a ticket raised via the department and/or HR department to grant access to emails, files etc. Mandatory information will have to be added to the ticket before it can be submitted within ServiceNow. All starters and leavers information will be recorded onto the Employee Info with password protection.

Within Section 4 – disciplinary & Grievance procedures within the Unily UK Employee handbook, issue 1.5 date 05/07/2021, disciplinary levels have been documented and include:

- **First Formal Warning** - For minor offences or if conduct or performance does not meet acceptable standards, a First Formal Warning is given by the employee’s immediate manager, or other nominated manager, and confirmed in writing
- **Final Formal Warning** - For offences of serious misconduct, or if conduct or performance does not improve, or if different or more serious problems arise, a Final Formal Warning is given by the employee’s immediate manager, or other nominated manager, and confirmed in writing.
- **Dismissal with Notice** - If despite a Final Formal Warning, conduct or performance does not improve, or if different or more serious problems arise, the employee will be dismissed with notice by their immediate manager. The Company, at its discretion, may dismiss the employee with pay in lieu of notice as an alternative to dismissal with notice.

Ordinarily formal warnings will remain valid on an individual’s disciplinary record for the following:

- First Formal Warning 6 months
- Final Formal Warning 12 months
Within the last 12 months, no disciplinary have occurred in relation to IT and/or the ISMS.

A new leaver’s process has been implemented by the Organisation. Within the ServiceNow, the leaver’s information will be completed with all information including last working day date, equipment returned and removal of access to systems. A ticket will be raised within ServiceNow to ensure all access rights are remove

| **Conclusion of the overall effectiveness of the process:** Process / Audit Area is satisfactory |
### Process/audit area:
Operational Process – Sales & Consultancy

<table>
<thead>
<tr>
<th>Auditees</th>
<th>Mark Sahal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auditor (if applicable)</td>
<td>Jesse Culleton &amp; Michael Harper</td>
</tr>
</tbody>
</table>

**Evidence to support audit conclusion:**

Mark Sahal is the Chief Operating Officer. He talked through the sales process.

Opportunities are created by inbound event such as a potential customer reaching out to Brightstarr and is captured by forms on the website. The contact details go into the Outreach application. The information is passed to Business Development. The information has to be freely offered and is publicly available rather than personal identification information.

Typical information is:
- Name,
- Phone number,
- Company,
- Additional information

Prior to entering the information potential clients have to read the cookie notice. There is a privacy statement on the website [https://www.unily.com/legal/privacy-policy](https://www.unily.com/legal/privacy-policy) which explains what Brightstarr do with the data and the name of the Data Protection Officer. The DPO is registered with the Information Commissioner’s Office.

Warm leads (which might lead to sales) are passed to the Salesforce application. A salesman manages the warm lead to closure. Sales are entered into Service Now. Non sales data stays in Hub Spot for prospects and are sent marketing emails about once a month until they ask to be removed.

Customers are assigned to a sales manager and all sales staff can see all customers in Salesforce. There is no PII to protect.

**Conclusion of the overall effectiveness of the process:** Process / Audit Area is satisfactory
**Process/audit area:** (A.8 Asset Management / A.9 Access Control / A.10 cryptography / Malware & A.13 Communication Security)

**Auditees:** James Heathcote

**Auditor (if applicable):** Jesse Culleton & Michael Harper

### Evidence to support audit conclusion:

A review of the following documents was undertaken during the remote audit process:

- Asset Management policy, ISMS Doc.5, issue 1.8 dated 01/11/2021 and classified as Private
- Acceptable Use Policy, ISMS Doc.8, issue 1.2 dated 16/01/2021 and classified as Restricted
- Access Control Policy, ISMS Doc.9, issue 1.4 dated 04/11/2021 and classified as Restricted
- Cryptographic controls Policy, ISMS Doc.11, issue 1.1 dated 23/10/2020 and classified as Restricted
- Cryptographic controls register, ISMS rec.5 issue 1.3 dated 08/03/2021 and classified as Private
- Network and information transfer policy, ISMS Doc.14, issue 1.5 dated 12/12/2021 and classified as Restricted

As discussed during the remote audit process, the organisation has a documented Asset Management policy, (ISMS Doc.5). All assets are held within InTune (now called Endpoint). Hardware tokens are used to access the asset management system, all assets are assigned ownership. All device compliance and configuration are documented within the main dashboard.

A total of 285 devices are recorded within Endpoint using the following headings:

- Managed by
- Ownership
- Compliance
- OS
- OS Version
- Last logged in

**Sample of Assets:**

- Device: DESKTOP-0KA1NOD
- Owner: L S
- Serial Number: 8ZD1(XXX)
- OS: Windows
- Device: IPhone
- Owner: D M
- Serial Number: F17WKEHQH(XXX)
- OS: iOS

Within PRTG, all equipment held within the comm room are recorded and sampled during the remote audit process. The infrastructure is listed within the device management tab including the health and location of the asset.

Sampled assets within PRTG:

- Item: APC SMART UPS 2220
  - REF: BSUKMGMTUP01
  - Location: GU7 2QW

- Item: PH01 – Physical Server
  - REF: BSUKMGMTVH01
  - Location: GU7 2QW

HR is responsible for ensuring that all users’ sign User Agreements that set out requirements for acceptable use of information assets and in which they also explicitly accept the Acceptable Use Policy. These User Agreements also explicitly accept Unily’s Rules for Use of E-mail. The Information Security Manager is responsible for monitoring compliance.

All disposals of media will be recorded within the asset register with disposal certificates recorded. And all disposals recorded within the waste disposal register

Sample of disposal records:

- Date: 11/02/2020
- Facility ID: GBRHO0000049
- Work Order: Confidential waste
as documented, the organisation has identified all data retention with the following chart used:

<table>
<thead>
<tr>
<th>Data Source</th>
<th>Retention Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Teams Chats (General)</td>
<td>14 days</td>
</tr>
<tr>
<td>Teams Rooms (Collaboration)</td>
<td>1 year review</td>
</tr>
<tr>
<td>Outlook emails (Online)</td>
<td>1 year</td>
</tr>
<tr>
<td>Outlook emails (Archive)</td>
<td>Indefinitely for the employment of the user, 30 days after termination unless litigation held</td>
</tr>
<tr>
<td>OneDrive Personal Documents</td>
<td>Indefinitely for the employment of the user, 30 days after termination unless litigation held</td>
</tr>
<tr>
<td>SharePoint General Documents</td>
<td>Reviewed after 6 years, archived if no longer required or deleted</td>
</tr>
<tr>
<td>Finance Materials</td>
<td>End of current financial year + 7 years</td>
</tr>
<tr>
<td>HR Materials</td>
<td>6 years following cessation of employment</td>
</tr>
<tr>
<td>HR Recruitment</td>
<td>Unsuccessful kept for 1 year</td>
</tr>
<tr>
<td>CCTV footage</td>
<td>30 days</td>
</tr>
<tr>
<td>Accident Books, reports</td>
<td>3 years from last entry</td>
</tr>
<tr>
<td>Contracts with customers, suppliers and agents</td>
<td>Expiry of termination + 3 years</td>
</tr>
<tr>
<td>Source Code</td>
<td>Indefinite</td>
</tr>
<tr>
<td>Infrastructure Security Logs</td>
<td>90 days ingested into SIEM</td>
</tr>
<tr>
<td>Unily Client data</td>
<td>Expiry or termination of the contract + 35 days</td>
</tr>
<tr>
<td>Unily Application Audit Logs</td>
<td>Expiry or termination of the contract + 35 days</td>
</tr>
<tr>
<td>Unily IIS Logs</td>
<td>Archived after 30 days, Expiry or termination of the contract + 35 days</td>
</tr>
<tr>
<td>Unily IDP Logs</td>
<td>Client responsibility to keep Authentication logs, we retain ours for 90 days</td>
</tr>
</tbody>
</table>

Access control

A documented access control policy, (ISMS Doc.9). Unily’s policy regarding access control must ensure that the measures implemented are appropriate to the business requirement for protection and are not unnecessarily strict. The policy therefore must be based upon a clear understanding of the business requirements as specified by the owners of the assets involved. These requirements may depend on factors such as:

- The security classification of the information stored and processed by a particular system or service
- Relevant legislation that may apply e.g. the Data Protection Act, GDPR
- The regulatory framework in which the organization and the system operates
- Contractual obligations to external third parties
- The threats, vulnerabilities and risks involved
- The organization’s appetite for risk

Privileged access rights such as those associated with administrator-level accounts must be identified for each system or network and tightly controlled. In general, technical users; such as IT support staff should not make day to day use of user accounts with privileged access. Separate “admin” user account should be created and used only when the additional privileges are required. These accounts should be specific to an individual. Generic admin accounts should not be used as they provide insufficient identification of the user.
A request for access to the organization’s network and computer systems must first be submitted to the Operations Team for approval. Once approved, the user will be added via the ServiceNow system and a ticket generated. The principle of segregation of duties will apply so that the creation of the user account and the assignment of permissions are performed by different people.

Sample of Access Ticket:

- Ticket: SCTASK0012882
- Employee: L O
- State: Completed 18/01/2022
- Action: create an account and assign access
- Date: 24/01/2022
- Department: Customer Services

Once the ticket has been completed, this will automatically create a procurement workflow to create a hardware task and issue equipment.

Each user account will have a unique user name that is not shared with any other user and is associated with a specific individual and not by role or job title. Generic user accounts should not be created as they provide insufficient allocation of responsibility.

An initial strong password should be created on account setup and communicated to the user via secure means. The user is required to change this password on first use of the account.

When an employee leaves the organization under normal circumstances, their access to computer systems and data must be suspended at the close of business on the employee’s last working day. It is the responsibility of the line manager to request the suspension of the access rights via the Operations Team.

Weekly access rights reviewed via a build in capability, every week an email is received to review the privilege groups and records all review history for all access.

Strong passwords are essential against unauthorised access. A variety of ways to improve the security of user authentication are available, including various forms of multi-factor authentication and strong password techniques.

Unily’s policy is to make use of additional authentication methods based on a risk assessment considering:

- The value of the assets protected
- The degree of threat believed to exist
- The cost of the additional authentication method(s)
- The ease of use and practicality of the proposed method(s)
- Any other relevant controls in place

The use of multi-factor authentication methods should be justified on the basis of the above factors and securely implemented and maintained where appropriate.

Whether single or multi-factor authentication is used, the quality of user passwords should be enforced in all networks and systems globally using the following parameters:
### Parameter | Value
---|---
Minimum length | 14
Maximum length | 24
Re-use cycle | Cannot be the same as any of the previous 3 passwords
Characters Required | Must contain upper and lowercase characters
Number of numerals to include “1”  
Special Characters | New password cannot share more than three characters in the same position as the old password
Password similarity | Change Frequency | At least every 70 days
Account lockout | On 3 incorrect logon attempts
Account lockout action | Account must be re-enabled by Operations Engineering Team
Other controls | Must not have 5 consecutive characters from username
Must not be a palindrome  
Must not contain any character more than twice consecutively
Cannot contain banned words such as brightstarr or unily

Any exceptions to these rules must be authorised by the Information Security Manager.

Unily classifies information into four levels; confidential, restricted, private and public, as noted in the table below. Classification is included in the document footer, which is manually set to appear on all pages of an internal document, or on the media on which it is recorded. Any external information received is classified by its owner.

<table>
<thead>
<tr>
<th>Classification</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confidential</td>
<td>Applies to information that is specifically restricted to the Senior Management Team and specific professional advisers. Material tagged as confidential automatically alerts end users if shared with external parties and requires the user to acknowledge and provide business justification if sending externally. Emails sent that are tagged as Confidential are automatically encrypted with Office 365 encryption (OME) to users both internally and externally.</td>
</tr>
<tr>
<td>Restricted</td>
<td>Applies to information that is specifically restricted to the Senior Management Team, line managers and those identified with specific requirements within their roles.</td>
</tr>
<tr>
<td>Private</td>
<td>This classification covers all information assets that have value but which do not need to fall within either of the other categories.</td>
</tr>
<tr>
<td>Public</td>
<td>This is information which can be released outside Unily.</td>
</tr>
</tbody>
</table>

Confidential information must be marked ‘Confidential’, and its circulation must be kept to a minimum with the names of the people to whom it is limited identified on the document. Confidential information sent by e-mail is encrypted, digitally signed and sent only to the e-mail addresses of identified recipients.

A Cryptographic control register is held by the organisation, (ISMS Rec.5). It is vital that cryptographic keys are protected from modification, loss, destruction and unauthorized disclosure. A lifecycle approach has been adopted by Unily covering the following:

- Key generation
- Distribution of keys to point of use
- Storage at point of use
- Backup as protection against loss
- Recovery in the event of loss
- Updating keys once expired
- Revoking if compromised
AUDIT REPORT PART B – AUDIT REPORT

- Archiving once expired
- Destroying when no longer required
- Logging and auditing of key management related activities

These points will take account of the specific circumstances in which encryption will be used.

In principle, private asymmetric keys and symmetric keys shall only exist in the following secure forms:

- As cleartext within the memory of a hardware-based encryption device
- As ciphertext outside the memory of a hardware-based encryption device
- As two or more key fragments either in cleartext or ciphertext, managed using dual control with split knowledge

As documented within the organisations Cryptographic controls register, ISMS rec.5 will list all encryption software and includes:

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Owner</th>
<th>Strength of encryption</th>
<th>Storage of encryption keys</th>
</tr>
</thead>
<tbody>
<tr>
<td>Laptop\PC Drives</td>
<td>Microsoft</td>
<td>AES-CBC 128bit</td>
<td>TPM</td>
</tr>
<tr>
<td>Laptop\Apple Devices</td>
<td>Apple</td>
<td>AES-XTS 128 bit</td>
<td>TPM</td>
</tr>
<tr>
<td>Removable Media</td>
<td>Microsoft</td>
<td>AES-128 bit</td>
<td>TPM</td>
</tr>
<tr>
<td>BYOD Mobiles</td>
<td>Microsoft</td>
<td>AES-128 bit</td>
<td>TPM</td>
</tr>
<tr>
<td>SSL Transport (Web)</td>
<td>Microsoft</td>
<td>SHA-256 RSA \ 2048</td>
<td>Private Key managed by Unily</td>
</tr>
<tr>
<td>Azure Storage Containers</td>
<td>Microsoft</td>
<td>AES-256 bit</td>
<td>Managed by Microsoft</td>
</tr>
<tr>
<td>Azure SQL Databases</td>
<td>Microsoft</td>
<td>AES-256 bit</td>
<td>Managed by Microsoft</td>
</tr>
<tr>
<td>Password Vault</td>
<td>Keeper</td>
<td>AES-256 bit</td>
<td>Client\Server Salted Hash</td>
</tr>
<tr>
<td>VoIP Communications</td>
<td>Teams</td>
<td>AES-256 bit GCM Mode</td>
<td>Managed by Microsoft</td>
</tr>
<tr>
<td>SharePoint Document Libraries</td>
<td>Microsoft</td>
<td>AES-256 bit</td>
<td>Managed by Microsoft</td>
</tr>
<tr>
<td>Email Encryption</td>
<td>Microsoft</td>
<td>AES-256 bit</td>
<td>Managed by Microsoft</td>
</tr>
<tr>
<td>Azure REDIS Cache</td>
<td>Microsoft</td>
<td>AES-256 bit</td>
<td>Managed by Microsoft</td>
</tr>
</tbody>
</table>

Encryption software sampled but will not be documented within report.

It is vital that cryptographic keys are protected from modification, loss, destruction and unauthorized disclosure. A lifecycle approach has been adopted by Unily covering the following:

- Key generation
- Distribution of keys to point of use
- Storage at point of use
- Backup as protection against loss
- Recovery in the event of loss
- Updating keys once expired
- Revoking if compromised
- Archiving once expired
- Destroying when no longer required
- Logging and auditing of key management related activities

These points will take account of the specific circumstances in which encryption will be used. In principle, private asymmetric keys and symmetric keys shall only exist in the following secure forms:
As cleartext within the memory of a hardware-based encryption device
- As ciphertext outside the memory of a hardware-based encryption device
- As two or more key fragments either in cleartext or ciphertext, managed using dual control with split knowledge

Malware

All incidents will have alert sent to the operations team and automation built into malware system and use the playbooks to action/quarantine file. Classification of threat will be completed and full lockdown of device conducted.

<table>
<thead>
<tr>
<th>Device compliance status</th>
<th>Devices</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compliant</td>
<td>262</td>
</tr>
<tr>
<td>In grace period</td>
<td>2 ▲</td>
</tr>
<tr>
<td>Not evaluated</td>
<td>0</td>
</tr>
<tr>
<td>Not compliant</td>
<td>21 ●</td>
</tr>
<tr>
<td>Total</td>
<td>285</td>
</tr>
</tbody>
</table>

Discussed non-compliant systems and due to extended leave and once returned will be updated before use. All malware actions will be alerted via email allowing for the organisation to review the alerts and action if required.

Sample of Malware action:

- Date: 27/01/2022
- Alerts: 1
- Title: malware detection
- Severity: Medium
- Status: Resolved
- Category: Malware

Within the organisation Network and Information transfer policy (ISMS Doc.14), the organisation has identified their network via a diagram (sampled during audit process but will not be documented due to being shared with external parties (i.e. customers)

Risk assessments are carried out for each network service and appropriate controls, including authentication, encryption and network connection are selected. The risk assessment is reviewed in line with the review requirements of the ISMS. The identified controls are included in the external party agreement/internal SLA which are managed in line with The Operating Procedures for IT Management.

Systems are separated by domain name. The business systems are managed by one domain and our cloud provided infrastructure for customers is managed by a dedicated\isolated domain accessible only by support engineers and authorised developers. The CTO and Operations Teams controls the domains directly.
<table>
<thead>
<tr>
<th><strong>VLANS, firewalls and NSGs separate environments based on audience and security requirements.</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Conclusion of the overall effectiveness of the process:</strong> Process / Audit Area is satisfactory</td>
</tr>
</tbody>
</table>
Process/audit area: A,16 IS Incident Management & A.17 BCP

Auditees: James Heathcote / Hugh Wilkinson / Tim Malhans

Auditor (if applicable): Jesse Culleton & Michael Harper

Evidence to support audit conclusion:

The following documents were reviewed/sampled as part of these audit areas:

- Information Security Incident Management Policy, ISMS Doc.1.7, Issue 1.43 dated 22/06/2021 and classified as Public

As discussed during the remote audit process with Tim Malhans (Head of Service Delivery), the organisation uses ServiceNow to report all incident tickets which all employees can report directly via ServiceNow and 3 avenues used by clients which include

- Email
- Self-service portal
- Telephone to support

The following are typical weaknesses and/or incidents that fall within the scope of this procedure, this list is not exhaustive:

- Breach of Physical security
- Breach of information security
- Loss or theft of property
- Data/information missing, lost or incorrect
- Financial irregularities
- Requests for Right to be forgotten
- Request for Data Subject access

Within the Ticket, the reporter will be required to supply all information. Each ticket will be review on receipt via level one assessment and be given a priority rating.

All information security events and weaknesses are, immediately upon receipt assessed and categorized by the Information Security Manager. Initially, there are four categories; events, vulnerabilities, incidents and unknowns.

- 'Events' are occurrences that, after analysis, have no or very minor significance on information security.
- 'Vulnerabilities' are weaknesses that, after analysis, clearly exist as significant weaknesses compromising information security.
- 'Incidents' are occurrences of events / series of events that have a significant probability of compromising Unilys information security.
- 'Unknowns' are those reported events or weaknesses that, after initial analysis, are still not capable of allocation to one of the four categories.

Within the ServiceNow system the dashboard allows for the organisation to have a visual look at tickets including incident and service request.
Sample of Incident:

- Ticket: INC0249376
- Company: B(XX)
- Application: Front End
- Type: Incident
- Issue: Some image are missing when accessing form different browser
- Priority: 3 – moderate
- Date: 11/01/2022
- Status: Closed

- Ticket: INC0249343
- Company: B(X)
- Application: forms
- Type: Incident
- Issue: documents submitted through forms are not downloading correctly
- Priority: 3 – moderate
- Date: 20/01/2022
- Status: Closed

All tickets will have the documented resolution steps undertaken to close the tickets.

It was explained that Daily Operations Meetings cover IS related tickets logged within the ServiceNow tool with a unique INC number.

Sample of Priority One Ticket:

- Ticket: INC0248403
- Company: S
- Application: Front End
- Date: 16/12/2021
- Issue: sire appears to be loading but not resolving site appears to be down.
- Priority: 1 – critical
- Status: Closed

A.17 INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT

documentation reviewed during the remote audit process include;

- Business Continuity Plan, ISMS Doc.18 (Issue 1.5 dated 11/03/2021 and classified as Private)

As discussed during the remote audit process with Hugh Wilkinson, due to the organisation BC & DR plans cover clients and availability of services. The organisation has conducted in May 2020 and covers the following identified incidents:
In response to a major disruptive incident that has resulted in the organization’s Incident Response Procedure being activated;
- As a recovery for a smaller, more localised event which although not serious enough to result in activation of the Incident Response Procedure, requires action to address its impact.

An initial briefing will then be held at which the plan owner will:
- Explain why the plan has been activated
- Describe the impact of the incident
- Outline what needs to be achieved by the team
- Allocate tasks according to the checklists detailed in the plan
- Address any questions the team may have
- Set out the method and frequency of communication within the team

Sample of BCP Test:
- Date: 07/05/2021
- Doc Ref: ISMS-DOC-17-5
- Test: loss of data centre
- Plan Ref: A17.2

As discussed, the organisation clients RTO is set as 12 hours and during the test, it took the organisation an hour to complete and return to normal.

Lessons learnt have been documented within section of the BCP and during the test, a single lessons learnt was documented:

Sample of Lesson learnt:
- Ref: 1
- Lesson: added step to ensure DB is scaled prior to restarting the site
- Recommendation: Step clarified in BCP
- Person Responsible: HW
- Timescale : Completed

It was explained that one of the main BC risks identified for the business was the unavailability of platform equipment to host and run the Unily product for clients to use. Whilst the IT infrastructure is hosted in the Azure cloud environment and owned by Microsoft, Brightstarr retain full remote control over this hardware and virtual machines.

The Business Continuity Plan was reviewed and seen to address the DR event of recovering the IT systems at an alternative Microsoft Data Centre and to provide user access to them. Also included were details of:
- Scope, Objectives, and Integrated Services not covered
- Activation Criteria and Procedures
- Implementation Procedure
AUDIT REPORT PART B – AUDIT REPORT

- Roles, Responsibilities and Authorities
- Communication Requirements and Procedures
- Internal and External Interdependencies and Interactions
- Resource Requirements
- Restoration of Normal Service
- Appendices of Contact details and Logging Forms

Business Team Recovery Checklist is used within the organisation during the activation of a BCP/DR:

<table>
<thead>
<tr>
<th>Task</th>
<th>Target Completion Date/ Time</th>
<th>Actual Completion Date/ Time</th>
<th>Signature</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confirm receipt of ticket</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Convene with relevant parties for remediation</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Allocate manual tasks to appropriate teams</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Communicate with clients</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Verify actions completed, issue MIR</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The IT Recovery Team consists of the following people:

<table>
<thead>
<tr>
<th>Name</th>
<th>Title</th>
<th>Role In Plan</th>
</tr>
</thead>
<tbody>
<tr>
<td>SH</td>
<td>Chief Technology Officer</td>
<td>Plan Owner</td>
</tr>
<tr>
<td>HW</td>
<td>Head of Operations Engineering</td>
<td>Server Specialist</td>
</tr>
<tr>
<td>JH</td>
<td>Head of Information &amp; Security</td>
<td>Security Specialist</td>
</tr>
<tr>
<td>MJ</td>
<td>Head of Deployments</td>
<td>Application Specialist</td>
</tr>
<tr>
<td>RG</td>
<td>Senior Operations Engineer</td>
<td>Database Specialist</td>
</tr>
</tbody>
</table>

The IT Recovery Team is responsible for:

- Recovering services in Microsoft Data Centre.
- Setup and configuration of Unily once fail over to secondary data centre is complete.

Conclusion of the overall effectiveness of the process: Process / Audit Area is satisfactory
**Use of Registration Marks and Logos**

<table>
<thead>
<tr>
<th>Use of Registration Mark (if used) is in accordance with the Rules of Registration</th>
<th>Yes</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>Detail if required</em></td>
<td></td>
</tr>
<tr>
<td>Use of Logo correct</td>
<td></td>
</tr>
</tbody>
</table>

**Example of the current NQA logos:**

ISO 9001 (UKAS Accredited)  
ISO 9001 (UKAS Accredited) with ‘UKAS Tick and Crown’

More information can be found at: [https://www.nqa.com/en-gb/clients/logo-library](https://www.nqa.com/en-gb/clients/logo-library)

If there are inaccuracies, errors or queries regarding this report or audit findings, please contact NQA Head Office on 0800 052 2424 within five working days of the closing meeting.

**End of Audit**
Audit Plan

This plan relates to the next Surveillance visit.

Relevant Standard/Supporting Documentation ISO27001:2013

<table>
<thead>
<tr>
<th>Member/Role</th>
<th>Lead auditor – J Culleton</th>
<th>Member/Role</th>
<th>Lead Auditor – J Culleton</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date</td>
<td>Day One – 25/01/23</td>
<td>Date</td>
<td>Day Two – 25/01/23</td>
</tr>
<tr>
<td>Time</td>
<td>Location/Department/Function</td>
<td>Time</td>
<td>Location/Department/Function</td>
</tr>
<tr>
<td>0900</td>
<td>Opening Meeting - Close out of previous findings / review of previous report</td>
<td>0900</td>
<td>Opening Meeting and reflection of Day One</td>
</tr>
<tr>
<td>0930</td>
<td>Site Tour (A.11 Physical &amp; Environmental Security)</td>
<td>0930</td>
<td>IT Support (Internal)</td>
</tr>
<tr>
<td>12.00</td>
<td>LUNCH</td>
<td>1200</td>
<td>LUNCH</td>
</tr>
<tr>
<td>1300</td>
<td>Leadership (Policy, roles and responsibilities)</td>
<td>1300</td>
<td>Development Department A.14</td>
</tr>
<tr>
<td>1400</td>
<td>Planning (Risk and opportunities, Risk Treatment and objectives)</td>
<td>1500</td>
<td>Incident Management A.16 &amp; BCP A.17</td>
</tr>
<tr>
<td>1500</td>
<td>Performance evaluation (Internal audit, management review) Improvement (Nonconformities and continual improvement)</td>
<td>1530</td>
<td>Report Writing and collation of information</td>
</tr>
<tr>
<td>1530</td>
<td>Report Writing</td>
<td>1630</td>
<td>Closing Meeting</td>
</tr>
<tr>
<td>1600</td>
<td>Closing Meeting</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Completed by Jesse Culleton
Timings and content may be subject to change

The objectives of the audit will be:
- To confirm that the management system had been established implemented and maintained in accordance with the requirements of the audit standard.
- To evaluate the ability of the management system to ensure the client organisation meets applicable statutory, regulatory and contractual requirements. Note: A management system certification audit is not a legal compliance audit.
- To evaluate the effectiveness of the management system to ensure it is continually meeting its specified objectives
- To identify as applicable, areas of the management system for potential improvement.

The audit scope describes the extent and boundaries of the audit, such as physical locations, organisational units, activities and processes to be audited.

Where the initial or re-certification process consists of more than one audit (e.g. covering different locations), the scope of an individual audit may not cover the full certification scope, but the totality of audits shall be consistent with the scope in the certification document.
## AUDIT REPORT PART D – AUDIT MATRIX

**Relevant Standard/Supporting Documentation:** ISO27001: 2013

- This audit programme is to be prepared by the Lead Auditor at the completion of the Stage 2 audit or the Recertification audit. It should be replicated in all subsequent surveillance visit reports.
- Where an element(s) of the programme cannot be completed at a given visit the programme shall be amended and up-issued accordingly to ensure coverage at the following visit.
- Site visits are to be included in the programme with a clear indication as to the processes intended to be sampled.

<table>
<thead>
<tr>
<th>Type of visit</th>
<th>Recertification</th>
<th>Surveillance 1</th>
<th>Surveillance 2</th>
<th>Recertification</th>
<th>Surveillance 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Visit Due Date (MM/YY)</td>
<td>2021</td>
<td>2022</td>
<td>2023</td>
<td>2024</td>
<td>2025</td>
</tr>
<tr>
<td>Mandatory Elements / Selected Processes</td>
<td>Processes to be audited during visits are to be indicated with a cross (X). All processes are to be audited during a three-year certification cycle excluding the re-certification visit.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Context of the organization</td>
<td>✓</td>
<td>✓</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Leadership</td>
<td>✓</td>
<td>✓</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Planning</td>
<td>✓</td>
<td>✓</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Support</td>
<td>✓</td>
<td>✓</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Performance evaluation</td>
<td>✓</td>
<td>✓</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Improvement</td>
<td>✓</td>
<td>✓</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Use of marks and references to certification / Client website</td>
<td>✓</td>
<td>✓</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Site Tour (A.11) Physical and Environmental Security</td>
<td>✓</td>
<td>✓</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Operations Processes (specify from scope)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• HR (Competency, A.7)</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>• Client support (Portals &amp; PIMS)</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>• IT Support (Internal)</td>
<td>✓</td>
<td></td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>• Development Department A.14</td>
<td>✓</td>
<td></td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>• Operations - Consultancy (A.6)</td>
<td>✓</td>
<td></td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>• Operations - Finance</td>
<td>✓</td>
<td></td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>• Operations – Sales A.13</td>
<td>✓</td>
<td></td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>• Incident Management A.16 &amp; BCP A.17</td>
<td>✓</td>
<td>✓</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

Audit trails will be developed based upon identified risk throughout the audit and as such timings and content may be subject to change. Where the client operates shifts, the activities that take place during shift working shall be considered when developing the audit programme.
ONGOING SUPPORT SERVICES

Training promotions and complimentary e-learning
As an NQA client, enjoy discounted training courses and complimentary access to our portfolio of e-learning courses.

Support through free webinars
Join one of our many free webinars discussing standards, improvement and industry topics. Use our webinars to help you improve your knowledge and understanding and engage with our subject matter experts.

PR and marketing support
Help to promote your press releases, blogs and case studies along with complimentary vehicle stickers for vans and HGV’s. Use the NQA Certified logo to promote your certification.

InTouch and legal updates
Registration to a monthly e-zine from NQA. Translating the language of standards, management systems and certification through articles covering best practices, tools and techniques and alerts on latest environmental and health & safety legislation.

Trusted partners
Our Associate Partner Programme is designed to put you in touch with third party independent consultants and software providers that can support you through every step of your certification journey.

NQA certified clients are authorized and encouraged to use NQA logos to promote their certification achievements.

Access all NQA logos here: https://www.nqa.com/en-gb/clients/logo-library

NQA, Warwick House, Houghton Hall Park, Houghton Regis, Dunstable, Bedfordshire LU5 5ZX, United Kingdom
T: 0800 052 2424 E: info@nqa.com @nqaglobal

www.nqa.com