|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Location | Glasgow Sentinel Office |  | Discussion | Management review 2024 |
| Attendees | |  |  | | --- | --- | | ***Name*** | ***Title*** | | ***Grant Nairn*** | *Chief Information Officer* | | ***Andrew Norrie*** | *Head of IT Operations* | | ***Aidan Glendye*** | *Head of Applications* | | ***Robert Clark*** | *ATS Senior Delivery Manager* | | ***Darren Johnson*** | *Enterprise Architect* | | ***Grant Leitch*** | *Head of Programme Delivery* | | ***Jim McGlynn*** | *Head of Global Processes* | | | Date | 20th September |
| Location | Glasgow |
|  |  |
|  |  |
| Absent | N/A | | Report no. 240409 | 1 |
|  |  |
| Copy to | ATS Leadership | | Chairmen | Grant Nairn |

Agenda

[**Introduction** 2](#_Toc181284979)

[**1.** **Review actions from previous management reviews and provide action updates** 3](#_Toc181284980)

[**2.** **Fulfilment of information security objectives** 3](#_Toc181284981)

[**3.** **Internal and External Audit** 5](#_Toc181284982)

[**4.** **Review of internal and external issues** 5](#_Toc181284983)

[**5.** **Nonconformities and corrective actions** 6](#_Toc181284984)

[**6.** **Risk Management** 7](#_Toc181284985)

[**7.** **Monitoring and Measurement of the ISMS** 8](#_Toc181284986)

[**8.** **Adequacy of resource for maintaining an effective Information Security Management System.** 9](#_Toc181284987)

[**9.** **Opportunities for continual improvement** 10](#_Toc181284988)

[**10.** **Feedback from interested parties/ relevant communication with interested parties.** 10](#_Toc181284989)

[**11.** **Communication** 10](#_Toc181284990)

[**12.** **Internal Customer Satisfaction** 11](#_Toc181284991)

[**13.** **Conclusion** 11](#_Toc181284992)

|  |
| --- |
| **Introduction** |

Information Security has a significant effect on day-to-day business of Aggreko.

Management recognizes the imperative to ensure that our assets, data and information are kept secure for our internal and external systems, and that we must enhance customer satisfaction through the process of continuous improvement.

This report is to evaluate the performance of the AGGREKO Information Security Management System to ensure effectiveness, adequacy, and compliance. The review includes all processes that contribute to the meeting our customer’s requirements, protecting our data and information, risks and continuous improvement.

|  |  |  |
| --- | --- | --- |
| 1. **Review actions from previous management reviews and provide action updates** | | |
| **No.** | | **Subject** |
|  | | 2024 is the first year of the UK Audit and therefore no minutes from last minutes are available. |
| 1. **Fulfilment of information security objectives** | | | |
| **No.** | **Subject** | | |
|  | **Evaluation & Effectiveness**  The ISMS policies are published on the [Information Security Management System - Home (sharepoint.com)](https://aggreko.sharepoint.com/sites/InformationSecurityManagementSystem?xsdata=%3D%3D&sdata=aEozQzRmc3hSNGRBVmIvekZ3ZXBKQ2FQRnFFQTRwVTFtMXIrOXFXZkNIdz0%3D&ovuser=5cb01ea2-4160-4f87-afc6-5e72e6b82ad1%2CDenis.Gallacher%40aggreko.com&OR=Teams-HL&CT=1720175258902&clickparams=eyJBcHBOYW1lIjoiVGVhbXMtRGVza3RvcCIsIkFwcFZlcnNpb24iOiI0OS8yNDA1MzEwMTQyMSIsIkhhc0ZlZGVyYXRlZFVzZXIiOmZhbHNlfQ%3D%3D)  The policies were signed off by Grant Nairn (Group CIO) and Darren Johnston (Head of Architecture) September 2024. Communication has been done via email to ATS. Various training sessions were complete over 2024 to create awareness and communication. An email was sent from the CIO to confirm that the Information Security Management SharePoint is available. The implementation has been driven by the Information Security Team. | | |
|  | **Realisation of objectives**  ISMS objectives are captured as part of our operational reporting within ATS, and governance framework. List current IS objectives and provide update on how they are being met:   * **Confidentiality, Integrity, and Availability.** All Aggreko employees and contractors will identify and protect all information assets, by ensuring appropriate security controls are in place to protect the confidentiality, integrity and availability of that asset. This is underpinned by effective information security risk management and privacy by design.   + IS risk management framework is established, and risks are being assessed. Security design requirements have been recently established by the Secure Development Standard and the IT Infrastructure Security Standard. Training has been carried out on these and is available on the ISMS site. * **Security Capability.** Responsibility and accountability for information security in Aggreko is defined and resourced appropriately so that security is effectively managed, and an incident response capability is in place.   + ISMS creation and maintenance supports this objective, as management clause documentation and IS policy and standards completed recently outline IS roles and responsibilities, outlining necessary requirements for security in Aggreko. * **Protection of Assets.** All Aggreko data assets will be identified, risk assessed and protected from theft, abuse, misuse and any form of potential damage.   + An Information Asset registry is being created to meet ISO 27001 requirements and support IS Control application. * **Role-Based Access Controls.** All Aggreko staff will be granted systems and data access in line with their role-based needs. Access granted will be recorded centrally and reviewed and adjusted quarterly by line management.   + Privileged access reviews are completed monthly, the IS team continues to ensure access requests are assessed for sufficient business justification before granting approval. * **Security Awareness.** All Aggreko colleagues, contractors and individuals with access to Aggreko’s infrastructure and information assets, will, upon joining and at least annually, undertake appropriate security awareness training based on their role.   + Aggreko’s yearly security awareness training material is nearly complete with a target of mid-November for publishing to employees. * **Commercial Control.** Operational resilience requirements are identified and built into all critical products and systems to ensure that Aggreko can continue its commercial activities in the event of significant information security incidents.   + A Third-Party Supplier Security Standard has been recently approved and published which sets out high level requirements for IS within supplier relationships. Supporting processes are in process. * **Management Control.** Aggreko will establish, maintain and continually improve an effective Information Security Management System in line with ISO27001:2022.   + Efforts to achieve ISO27001 are continuing as a gap assessment and internal audit have been completed of the ISMS, and the first and second stage ISO 27001 audits are due in October and November. * **Legality.** Aggreko will comply with all relevant security legal, statutory, regulatory and contractual obligations. This will be subject to frequent monitoring and review.   + A IS Legal Register has been created to fulfil requirements of ISO27001 and ensure Aggreko is able to comply with legal requirements. | | |

***Conclusion***

*ISMS policy & objectives are up to date and comply with the standards. The measurement and management of these objectives are being reported via the Operations Service Forum and Vulnerabilites / Asset Management Forum.*

|  |  |  |  |
| --- | --- | --- | --- |
| 1. **Internal and External Audit** | | | |
| **No.** | **Subject** | | |
|  | Internal ISO27001 – Audit | There were no Major NCs detected, only minor NC’s and observations. These were discussed with the auditor and agreement was made that some corrections were to be made, but others were not critical to effective functioning of the ISMS. The auditor advised that these can be taken under recommendations for Continuous Improvement. | |
|  | ITGC Audit Executed in 2023 | **External:**   * EY - ATS   **Internal:**   * Service Performance Mangement * Applications * Infrastructure | **Key Items**  Minor   * B1.1 A full population user access review has not been conducted for Salesforce or CloudSuite * B1.2 Reviews of SOC reports by management are not formally documented (repeat finding) Housekeeping |

***Conclusion***

*Findings are reviewed by Management and corrections take place within three months. We have corrected various minor nonconformities and were practicable the observations. The ITGC audit provided a view to enhance our controls. Full population reviews are now conducted, and SOC reporting now has a defined process which supports the Service Owners and Information Security. The reports are attached and were reviewed at the meeting.*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1. **Review of internal and external issues** | | | | |
| **No** | **Subject** | |  |  |
|  | External | There is a strong possibility the Digital Resilience Bill will be brought into legislation within the next year, which may affect the ISMS. The Legal and Information Security Team will be informed of developments and changes required. There is currently no other external factors consideration. | | |
|  | Internal | The Information Security team is subject to staff attrition with a position required to be filled by the end of September. A Security Team lead has been identified to start with Aggreko, while we continue to work on hiring additional analysts. | | |

***Conclusion***

*We must continue to monitor external changes and effectiveness of our internal environment to support the ISMS, this is critical ensure its effectiveness. The issue of staff must be addressed as part of this report and corrective action is underway, as per the adequacy of resources which is discussed further in this report.*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1. **Nonconformities and corrective actions** | | | | |
| **No.** | **Subject** | |  |  |
| 5.1 | Internal | The deadline for ATS teams reporting nonconformities and risks has passed. The IS team is in process of assessing risk/ noncompliance entries. Forty-Nine nonconformities have been raised internally against our standards and risks. | | |
| 5.2 | Internal | No Major NCs detected as part of our internal / external audits. | | |
| 5.3 | Internal | Minor nonconformities detected and corrected on management and some controls. Majority have been corrected, please see attached internal audit report. | | |
| ***Conclusion***  *Nonconformities and corrective actions are key to the effective functioning and enhancement of the system. In order to meet, maintain and enhance our objective’s these must be corrected. The minor NCs detected from our audits and internal response to the Standards will need to be corrected and managed via the Risk and Continuous Service Improvement processes. In some instances, there may be a valid reason for the NCs, and these will remain. These were reviewed as part of the meeting.* | | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| 1. **Risk Management** | | | |
| **No. Subject** | | |  |
|  | Risk status | The information Security Risk Management Framework is in its infancy and currently there are 253 risks in register, 214 open, 39 closed, 12 open ones have been assessed. The first risk governance forum has been completed on 10/10; screenshot of current top ten assessed risks attached below. No risks have lapsed treatment timelines yet. | |
|  | Key Risks | Key risks have been identified below and have been discussed at the latest risk forum: | |
|  | Risk Dashboard | There is not a risk dashboard to support the SLT in understanding the risk within their respective areas. This will be enhanced on the basis of risks by department to provide additional focus areas, once the data integrity has been improved. | |

***Conclusion***

*The risk-based approach is critical to our ISMS, while we are a smaller organisation we must ensure best practice is in place and risks are being addressed in a timely manner to keep us secure. A key focus before the end of the year is to focus on Risks. While they are well mitigated on the environment through various controls, a renewed focus will support the protection of data and information for our key and critical systems.*

|  |  |  |
| --- | --- | --- |
| 1. **Monitoring and Measurement of the ISMS** | | |
| **No Subject** | | |
| 7.1 | Governance | A governance framework has been implemented for the ISMS. All meetings are now set with a term of reference to ensure the effectiveness of the ISMS. While this is not a specific requirement of the standard a separate document has been created advising all teams of their responsibilities. Over and above a Management Standard has been created with training to support the ATS Senior Leadership Team. A copy has been attached and was reviewed at this meeting. |
| 7.2 | Service Operations | The Service Operations Forum has been updated to include all monitoring, measurement and metrics agreed for the ISMS. The first review identified improvements to the Asset, Change and Vulnerability Management processes and demonstrated their effectiveness. Based on this, the sample copy below has supported raising some additional risks and identifying key continuous improvement initiatives. |

***Conclusion***

*A key focus before the end of the year is to focus on Asset and Vulnerabilities. While we continue to see improvements, as a collective organisation we need to ensure we are being effective in reducing the associated risks.*

|  |  |  |
| --- | --- | --- |
| 1. **Adequacy of resource for maintaining an effective Information Security Management System.** | | |
| **No Subject** | | |
| 8.1 | Internal | There are changes to the current Security Team due to attrition, we are currently in the hiring process with a new Information Security Lead starting in Jan 2024. Additional staff are being hired to support the effectiveness of the management system. All Security Operations Teams remain in place, with support from the Service Performance team. This will support sustainable performance and ensure continuous improvement. In addition, there is varying expertise within Aggreko ATS that will continue to support and uphold the standards and controls agreed.  There will be a full induction and continuity from the remaining teams to educate and support any new Information Security Team members. |
| 8.2 | Internal | Sufficient training has been provided to all teams on the Information Security Management System, which includes standards and controls. The annual security training is due to take place in Jan 2025, which includes reviewing and acknowledging the Information Security Policy. Reporting will take place to identify and confirm all individuals have completed their annual training. |

***Conclusion***

*Resources and knowledge are key to the success of the ISMS. There is sufficient resource to continue the ISMS and monitor its effectiveness in its current form, however additional security headcount is required to support the overall improvement, sustainability and management of the ISMS.*

|  |  |  |
| --- | --- | --- |
| 1. **Opportunities for continual improvement** | | |
| **No.** | **Subject** | |
| 9.1 | Vulnerability Management | Due to new technologies, we have found that additional vulnerabilities have been identified and are in the process of remediating these. This also in part due to Line Managers turning on old end point devices, which has spiked the numbers.  There are a few key process areas which can be enhanced and as part of continuous improvement we will develop these. We are seeing a downward trend and that will support a more secure environment. |
| 9.2 | Asset Management | We have identified several assets which were being brought online after a long period, which has spiked our vulnerability score. We are now instituting a new policy, with a wider communication to Line Managers, that no device can rejoin the network after 45 days without a rebuild. |
| 9.3 | Change Management | Changes which fail due to security must be logged in a checkbox rather than a text field to clearly identify the issues. We completed an end-end review of all changes in the last 3 months and there were no clear security failures. There will be a check box added to our ITSM solution to clearly identify a security change that has failed. |
| 9.4 | Audits | As discussed, we have identified several improvements that can be made to the ISMS, these are based on observations within the attached reports. We discussed these at length and will add to our continuous improvement actions to enhance the overall ISMS. |

***Conclusion***

*The ISMS must be continuously improved to ensure that it is effective and keeping our data, information and assets safe. The enhancement of these processes will bring us in line with some of the non-conformities identified and improve our estate.*

|  |  |  |  |
| --- | --- | --- | --- |
| 1. **Feedback from interested parties/ relevant communication with interested parties.** | | | |
| **No.** | **Subject** |  |  |
| 10.1 | Feedback | The ISMS is still under establishment, feedback will be provided from the Management Team. | |

***Conclusion***

*Feedback from interested parties is critical to improve the system. The ISMS has recently been developed, we will monitor and make modifications based on feedback received by our stakeholders and interested parties.*

|  |  |  |
| --- | --- | --- |
| 1. **Communication** | | |
| **No.** | **Subject** | |
| 11.1 | Internal | Communication is done from top down and bottom up. Through various governance meetings, awareness and training we have successfully informed ATS of the Information Security System which can be seen as part of the number of times that articles have been viewed on the site. Risk and non-conformance engagement has been excellent as demonstrated by the number which have been raised. |

***Conclusion***

*Good communication is an essential tool in achieving productivity and maintaining strong working relationships at all levels of an organisation. We need to ensure that lines of communication are kept open at all times. Actively seek and encourage progress reports and project updates. This is particularly important when dealing with remote staff.*

|  |  |  |  |
| --- | --- | --- | --- |
| 1. **Internal Customer Satisfaction** | | | |
| **No.** | **Subject** | |  |
| 12.1 |  | Customer Satisfaction Survey  Our internal metrics for customer satisfaction for all of ATS, including security, remains above industry standard of 75% | |
| 12.2 | ATS Survey | The employee survey is a key measurement to ensure that our employees are being supported and gives them a chance to voice their feedback. Comments may be made as part of the ISMS. We have had consistently positive results as we have enhanced our security posture. | |

|  |
| --- |
| 1. **Conclusion** |
| **Conclusion**  Looking at the content of the yearly review of the ISMS systems, we can conclude that while there is room for improvement the Management Systems covered are suitable, adequate and effective.  **Agreement**  All the attendees hereby declare to agree with the content of the ISMS Management Review 2024 and the comments made on this review as noted above. |

Date 20th September 2024 Submitted too: Aggreko Technology Service – Grant Nairn CIO