Information Security Management System

Monitoring, Measure & Performance Evaluation

**Aggreko Technology Services**

**Change Record**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Author** | **Change Reference** | **Version** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Peer Review**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version no.** | **Date** | **Signatory** | **Title** | **Digital Signature** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**Approval**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version no. | Date | Signatory | Title | Digital Signature |
|  |  |  |  |  |

**Terms of reference**

|  |  |  |
| --- | --- | --- |
| **Name** | **Acronym** | **Description** |
| Aggreko Technology Services | ATS | Aggreko’s Information Technology Department |
| Information Security Management System | ISMS | Security Management system governing management activities and controls as prescribed by ISO27001 |
| Information Security | Infosec | Aggreko’s information security department |
|  |  |  |
|  |  |  |

Table of Contents

[1. Purpose 3](#_Toc170834125)

[2. Scope 3](#_Toc170834126)

[3. Requirements 3](#_Toc170834127)

[4. Active and Reactive Monitoring 3](#_Toc170834128)

[5. Key Information Security Performance Measures 3](#_Toc170834129)

[5.2 Monthly Key Performance Indicators 4](#_Toc170834130)

[5.3 Quarterly Key Performance Indicators 5](#_Toc170834131)

[6. Information Security Analysis 6](#_Toc170834132)

[7. Recording data and results 6](#_Toc170834133)

[8. Related Documentation 6](#_Toc170834134)

[9. Key Performance Data 6](#_Toc170834135)

[10. Legal & Other Requirements 6](#_Toc170834136)

[11. Summary process flow chart – Monitoring, Measurement and Performance Evaluation 7](#_Toc170834137)

# Purpose

The purpose of this procedure is to ensure the correct level of monitoring and measuring are used to make sure the ISMS plans have been implemented and assess how well the ISMS risks are being controlled and if we are achieving our aims.

# Scope

The scope of this procedure applies to all management, employees, and contractors within ATS. The full cooperation and assistance of personnel are required to ensure appropriate resources are available to support the ISMS.

# Requirements

Monitoring is a key step in any management process and forms the basis of continuous improvement. If monitoring is not carried out correctly, the effectiveness of the Information Security Management System can be undermined and there is no reliable information to inform managers of how well the IS risks are controlled.

Monitoring the performance of an organisation is also an important step when formulating the direction of strategic activities. It is important to know where the strengths and weaknesses of the organisation lie, and as part of the “Plan-Do-Check-Act” cycle, measurement plays a key role in quality and productivity improvement activities.

Monitoring performance information sustains the operation and development the IS Management system, supporting the IS objectives and control of risks by:

* Providing information on how the system operates in practice.
* Identifying areas where remedial action is required.
* Providing a basis for continual improvement.
* Providing feedback and motivation.

The monitoring process can gather information through:

* Direct observation of conditions and people’s behaviour.
* Talking to people elicit facts and their experiences as well as gauging their views and opinions.
* Examining written reports, documents and records.

# Active and Reactive Monitoring

There are many different types of monitoring by they can be generally categories as either ‘active’ or ‘reactive’:

* **Active methods:** Monitoring the design, development and implementation of operational or project management activities. This tend to be preventative, for example: before making changes such opening Firewall ports, there are information security checks in place to ensure there no impact to our data and no risks to our environment. Similarly new projects are checked for any potential security implications and if utilising a supplier, the RFP process will ensure they can meet our standards.
* **Reactive methods:** monitor evidence of poor Information Security practices but can help to identify potential opportunities to improve our practices, which can also be transferred to the rest of the business. For example, investigating incidents or security incidents can identify overall improvements to our infrastructure and expose potential risks.

Aggreko Technology Services will use both performance measures as part of our monitoring.

# Key Information Security Performance Measures

The measurement of processes and controls, which have been put in place will be reviewed as part of our monthly and quarterly governance that will support the Information Security Management System. Based on risk, these have been broken down into monthly and quarterly reviews.

Key performance indicators that are monitored, measured and analysed to ensure that we remain proactive and identify opportunities for improvement with reactive methods. This will be used to support the technological controls and ensure that we address any information, asset and data risks.

## 5.2 Monthly Key Performance Indicators

These key performance indicators are reviewed and analysed monthly as they are critical to protecting our Information and Data assets. This ensures that the fundamental controls, with the greatest risk, are monitored at an increased frequency. This supports immediate action to reduce and / or mitigate risk within our tolerances and facilitates rapid continuous improvement.

|  |  |  |
| --- | --- | --- |
| **Area Title** | **Description** | **Measure** |
| **Risks Management** | Monitors the identification of risks and treatments plans. | No of risks raised No of treatment plans Mean Time to Resolve |
| **Non-Conformance** | Monitors addressing the resolution of non-conformities to reduce risk | No of non-conformities Mean time to resolve |
| **Access Control** | Access to networks and network services | Review of sample user accounts and verification of access rights, which match requirements of the templated form.  Record no. of conformities vs. non-conformities. |
| Review of user access rights | Record no. of accounts automatically disabled every quarter. Record no. of unused privileged system accounts that require disabling every quarter. Record no. of unused document management system accounts that require disabling every quarter. |
| **Operational Security** | Change management | No of unauthorised changes.  No of security related changes.  No of failed security related changes.  No of incidents caused by change, related to security.  Record no. of conformities vs. non-conformities. |
| Controls against malware | Record number of malware infections on a quarterly basis and increase / decrease in trends. |
| Management of technical vulnerabilities | Conduct regular documented reviews of third-party reports to ensure that procedures are carried out in line with expectations. No of devices with software vulnerabilities N-1 over 15 days.  % of devices with the latest OS patch standard  Mean time to resolve vulnerabilities.  Record no. of conformities vs. non-conformities. |
| Reporting information security Incidents & Events | No of incidents report No. of events reported Mean time to respond. Mean time to resolve  Security Incident Reviews – completed within 5 days of the incident occurring. |
| Service Request Management |  |
| Antivirus Rate | No of devices without Antivirus check-in |

## 5.3 Quarterly Key Performance Indicators

These key performance indicators are reviewed and analysed quarterly as they are critical to protecting our Information and Data assets. This ensures that the fundamentals of the Information Security Management System are effective but deemed a reduction in risk in relatively to the monthly reviews.

|  |  |  |
| --- | --- | --- |
| **Area Title** | **Description** | **Measure** |
| **Information Security Policies** | Policies for information security | 80% of new or updated to policies to be read and accepted within 2 weeks. 100% of new or updated to policies to be read and accepted within 4 weeks. |
| Review of the policies for information security | 100% of policies to be reviewed within 4 weeks of the reminder date. |
| **Organisation of Information Security** | Mobile device policy | % of devices detected as compliant with policy. No target score defined, but trend is tracked. |
| **Human Resources Security** | Screening | Conduct quarterly audits by taking a sample of staff files and checking that all necessary background checks have been conducted and recorded. Target is 100% of all records should be correct. |
| Information security awareness, education and training | 80% of all modules are taken within 2 weeks of being notified. 100% of all modules are taken within 4 weeks of being notified. 70% first time pass rate for all modules with knowledge reviews. % of click throughs of staff in phishing tests is tracked. |
| Disciplinary process | Track no. of breaches that are caused by internal staff, and split into intentional vs. accidental. |
| **Asset Management** | Inventory of assets | Conduct quarterly audits of the asset register by taking a sample set of assets and checking that the corresponding information on the asset register and in the fixed asset list is correct. Record no. of conformities vs. non-conformities. |
| Return of assets | Conduct quarterly audits of the asset register by taking a sample set of assets and checking that the corresponding information on the asset register is correct and that items are accounted for. Record no. of conformities vs. non-conformities. |
| **Physical and Environmental Security** | Supporting utilities | Record number of power failures on a bi-annual basis and the length of disruption for each failure. |
| Unattended user equipment | Record number of non-compliances on a quarterly basis by conducting an office walkthrough. |
| Clear desk and clear screen policy | Record number of non-compliances on a quarterly basis by conducting an office walkthrough. |
| **System Acquisition, Development and Maintenance** | System change control procedures | No of unauthorised project changes.  No of security project related changes.  No of failed security project related changes.  Record no. of conformities vs. non-conformities’. |
| **Information Security Incident Management** | Reporting information security events | No. of events reported in last quarter. Mean time to address root cause. |
| **Information Security Aspects of Business Continuity Management** | Availability of information processing facilities | No. of issues raised from DR tests & the time to resolve. |
| **Compliance** | Intellectual property rights | Record number of IP violations every quarter. |
| Independent review of information security | Number of external audits completed. |
| Compliance with security policies and standards | Annual audit. |
| Technical compliance review | Results of penetration testing, showing the number of high , medium & low issues. Track previously open findings to closure, e.g. still open at next test or now closed. |

# Information Security Analysis

The key performance data reviewed will be discussed as part of our governance structure for the Information Security System. Although we will conduct yearly management reviews where all reports will be collated the monthly and quarterly review output will be reviewed and / or attended by the Senior Leadership Team. The key meetings that allow us to review these datasets and address risks are as follows:

* Service Operations Review – A monthly review forum where we report on all stated KPI’s.
* Risk Management Review – The risks, treatment plans and non-conformities are discussed, and we address any challenges / issues.
* Quarterly IT Process Review – A quarterly review forum for the effectiveness of processes and their effectiveness.
* Vulnerability Review – Monthly meeting to discuss the status of the vulnerabilities discovered on the estate as well as remediation.

Output from these meetings and the Key Performance Indicators, will result in action taken to mitigate risks, secure our information and assets. These will be analysed by the Information Security Department and all Services Owners.

Any support required or outcomes that cannot be addressed by the teams involved in these reviews will be discussed with the Senior Leadership Team who will support any requests to proactively resolve any challenges with the Information Security Management System and any associated process.

The output from all the governance forums will form support the end of year Management Review which will take place.

# Recording data and results

The output from all reviews and their associated data records shall be sufficient to facilitate subsequent corrective and preventative actions. This will also be recorded on the Information Security SharePoint to support auditing, review and a history of record.

# Related Documentation

* Information Security Policy
* Security reporting

# Key Performance Data

* Service Operations Forum
* Risk Reporting System
* NCR Reporting System

# Legal & Other Requirements

* ISO27001: 2022 Information Security Management System
* ISO27005: Risk Management
* The Data Protection Act (2018)
* General Data Protection Regulation (EU) 2016/679
* The Freedom of Information Act (2000)
* The Computer Misuse Act (1990)
* The Human Rights Act (1998)
* The Copyright, Designs and Patents Act (1988).
* The Regulation of Investigatory Powers Act (2000)
* The Electronic Communications Act (2000)
* Privacy and Electronic Communications Regulations (2003)

# Summary process flow chart – Monitoring, Measurement and Performance Evaluation

|  |  |
| --- | --- |
| **Process Flow and Chart** | **Procedure / Action** |
|  | 1. **Information Security**   Identify the key activities across BAU, Project and Security Incidents for critical business applications. Agree risk control and non-conformance activities. |
| 1. **Information Security**   Analyse these key activities, management arrangements and resource to identify key performance data within each standard / procedure. |
| 1. **Information Security / Security Operations**   Establish the goals and measurements for success and effectiveness of the Information Security Management System. |
| 1. **Information Security / Security Operations**   Assign responsibility for collecting and analysing the data for presenting back the findings at the various agreed governance forums. |
| 1. **Information Security / Service Owners / Security Operations**   Act on the findings and ensure that agreed risks / non-conformance is documented. Document all reporting to support demonstrating compliance. |