| | |
|---|---|
| **Company** | [Company Name] |
| **Document** | ISO 27001 RASCI Matrix |
| **Classification** | Internal |
| | Used to track who is accountable and who does the work. |

**Version Control**

| Version | Document Changes | Last Modified By | Date |
|---|---|---|---|
| **0.1** | | | |
| | | | |
| | | | |

**Guidance - delete this section**

**This is the BASIC version of the RASIC Matrix. In most cases you would use the basic version but I include the full detailed RASCI Matrix for if you need it. You would amend it to fit your requirements and style and remove the columns that you do not need. You have both version of the standard so remove the tabs at the bottom that you are not using.**

# [Company] : ISO 27001:2022 ISMS RASCI Matrix

**Classification: Confidential**

| ISO27002:2022 - ISMS Accountability | | Responsible Named Person<br>(The person who is ultimately responsible for the completion of a task) | Accountable Named Person<br>(The person who is ultimately accountable for the success or failure of a task) |
|---|---|---|---|
| **4** | **Context of the organisation** | <Insert persons name> | <Insert persons name> |
| 4.1 | Understanding the organisation and its context | <Insert persons name> | <Insert persons name> |
| 4.2 | Understanding the needs and expectations of interested parties | <Insert persons name> | <Insert persons name> |
| 4.3 | Determining the scope of the information security management system | <Insert persons name> | <Insert persons name> |
| 4.4 | Information security management system | <Insert persons name> | <Insert persons name> |
| **5** | **Leadership** | <Insert persons name> | <Insert persons name> |
| 5.1 | Leadership and commitment | <Insert persons name> | <Insert persons name> |
| 5.2 | Policy | <Insert persons name> | <Insert persons name> |
| 5.3 | Organisational roles, responsibilities and authorities | <Insert persons name> | <Insert persons name> |
| **6** | **Planning** | <Insert persons name> | <Insert persons name> |
| 6.1 | **Actions to address risks and opportunities** | <Insert persons name> | <Insert persons name> |
| 6.1.1 | General | <Insert persons name> | <Insert persons name> |
| 6.1.2 | Information security risk assessment | <Insert persons name> | <Insert persons name> |
| 6.1.3 | Information security risk treatment | <Insert persons name> | <Insert persons name> |
| 6.2 | **Information security objectives and planning to achieve them** | <Insert persons name> | <Insert persons name> |
| 6.2 | General | <Insert persons name> | <Insert persons name> |

|  |  |  |  |
|---|---|---|---|
| 6.3 | When the organization determines the need for changes to the information security management system, the changes shall be carried out in a planned manner. | <Insert persons name> | <Insert persons name> |
| **7** | **Support** | <Insert persons name> | <Insert persons name> |
| 7.1 | Resources | <Insert persons name> | <Insert persons name> |
| 7.2 | Competence | <Insert persons name> | <Insert persons name> |
| 7.3 | Awareness | <Insert persons name> | <Insert persons name> |
| 7.4 | Communication | <Insert persons name> | <Insert persons name> |
| 7.5.1 | Documented information General | <Insert persons name> | <Insert persons name> |
| 7.5.2 | Creating and updating | <Insert persons name> | <Insert persons name> |
| 7.5.3 | Control of documented information | <Insert persons name> | <Insert persons name> |
| **8** | **Operation** | <Insert persons name> | <Insert persons name> |
| 8.1 | Operational planning and control | <Insert persons name> | <Insert persons name> |
| [redacted] | [redacted] | <Insert persons name> | <Insert persons name> |
| [redacted] | [redacted] | <Insert persons name> | <Insert persons name> |
| **9** | **Performance evaluation** | <Insert persons name> | <Insert persons name> |
| 9.1 | Monitoring, measurement, analysis and evaluation | <Insert persons name> | <Insert persons name> |
| 9.2 | **Internal Audit** | <Insert persons name> | <Insert persons name> |
| [redacted] | [redacted] | <Insert persons name> | <Insert persons name> |
| [redacted] | [redacted] | <Insert persons name> | <Insert persons name> |
| 9.3 | **Management review** | <Insert persons name> | <Insert persons name> |
| 9.3.1 | General | <Insert persons name> | <Insert persons name> |
| [redacted] | [redacted] | <Insert persons name> | <Insert persons name> |
| [redacted] | [redacted] | <Insert persons name> | <Insert persons name> |
| **10** | **Improvement** | <Insert persons name> | <Insert persons name> |
| 10.1 | Continual improvement | <Insert persons name> | <Insert persons name> |
| [redacted] | [redacted] | <Insert persons name> | <Insert persons name> |

# [Company] : ISO 27001:2022 ANNEX A RASCI Matrix

**Classification: Confidential**

| ISO27002:2022 - Annex A Controls | | Responsible Named Person<br>(The person who is ultimately responsible for the completion of a task) | Accountable Named Person<br>(The person who is ultimately accountable for the success or failure of a task) |
|---|---|---|---|
| **5** | **Organisational Controls** | | |
| 5.1 | Policies for information security | <Insert persons name> | <Insert persons name> |
| 5.2 | Information security roles and responsibilities | <Insert persons name> | <Insert persons name> |
| 5.3 | Segregation of duties | <Insert persons name> | <Insert persons name> |
| 5.4 | Management Responsibilities | <Insert persons name> | <Insert persons name> |
| 5.5 | Contact with Authorities | <Insert persons name> | <Insert persons name> |
| 5.6 | Contact with special interest groups | <Insert persons name> | <Insert persons name> |
| 5.7 | Threat intelligence | <Insert persons name> | <Insert persons name> |
| 5.8 | Information security in project management | <Insert persons name> | <Insert persons name> |
| 5.9 | Inventory of information and other associated assets | <Insert persons name> | <Insert persons name> |
| 5.10 | Acceptable use of information and other associated assets | <Insert persons name> | <Insert persons name> |
| [redacted] | [redacted] | <Insert persons name> | <Insert persons name> |
| [redacted] | [redacted] | <Insert persons name> | <Insert persons name> |
| [redacted] | [redacted] | <Insert persons name> | <Insert persons name> |
| [redacted] | [redacted] | <Insert persons name> | <Insert persons name> |
| [redacted] | [redacted] | <Insert persons name> | <Insert persons name> |

| | | | |
|---|---|---|---|
| 5.16 | Identity Management | <Insert persons name> | <Insert persons name> |
| 5.17 | Authentication information | <Insert persons name> | <Insert persons name> |
| 5.18 | Access rights | <Insert persons name> | <Insert persons name> |
| 5.19 | Information security in supplier relationships | <Insert persons name> | <Insert persons name> |
| 5.20 | Addressing information security within supplier agreements | <Insert persons name> | <Insert persons name> |
| 5.21 | Managing information security in the ICT supply chain | <Insert persons name> | <Insert persons name> |
| 5.22 | Monitoring, review and change management of supplier services | <Insert persons name> | <Insert persons name> |
| [redacted] | [redacted] | <Insert persons name> | <Insert persons name> |
| 5.24 | Information security incident management planning and preparation | <Insert persons name> | <Insert persons name> |
| [redacted] | [redacted] | <Insert persons name> | <Insert persons name> |
| [redacted] | [redacted] | <Insert persons name> | <Insert persons name> |
| [redacted] | [redacted] | <Insert persons name> | <Insert persons name> |
| [redacted] | [redacted] | <Insert persons name> | <Insert persons name> |
| 5.29 | Information security during disruption | <Insert persons name> | <Insert persons name> |
| [redacted] | [redacted] | <Insert persons name> | <Insert persons name> |
| 5.31 | Legal, statutory, regulatory and contractual requirements | <Insert persons name> | <Insert persons name> |
| [redacted] | [redacted] | <Insert persons name> | <Insert persons name> |
| 5.33 | Protection of records | <Insert persons name> | <Insert persons name> |
| [redacted] | [redacted] | <Insert persons name> | <Insert persons name> |
| 5.35 | Independent review of information security | <Insert persons name> | <Insert persons name> |
| [redacted] | [redacted] | <Insert persons name> | <Insert persons name> |
| [redacted] | [redacted] | <Insert persons name> | <Insert persons name> |
| **6** | **People Controls** | | |
| 6.1 | Screening | <Insert persons name> | <Insert persons name> |
| 6.2 | Terms and conditions of employment | <Insert persons name> | <Insert persons name> |

|  |  |  |  |
|---|---|---|---|
| 6.3 | Information security awareness, education and training | <Insert persons name> | <Insert persons name> |
| [redacted] | [redacted] | <Insert persons name> | <Insert persons name> |
| [redacted] | [redacted] | <Insert persons name> | <Insert persons name> |
| [redacted] | [redacted] | <Insert persons name> | <Insert persons name> |
| [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | <Insert persons name> | <Insert persons name> |
| **7** | **Physical Controls** |  |  |
| [redacted] | [redacted] | <Insert persons name> | <Insert persons name> |
| 7.2 | Physical entry | <Insert persons name> | <Insert persons name> |
| [redacted] | [redacted] | <Insert persons name> | <Insert persons name> |
| 7.4 | Physical security monitoring | <Insert persons name> | <Insert persons name> |
| 7.5 | Protecting against physical and environmental threats | <Insert persons name> | <Insert persons name> |
| [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] |
| 7.8 | Equipment siting and protection | <Insert persons name> | <Insert persons name> |
| 7.9 | Security of assets off-premises | <Insert persons name> | <Insert persons name> |
| [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] |
| **8** | **Technological Controls** |  |  |
| 8.1 | User endpoint devices | <Insert persons name> | <Insert persons name> |
| 8.2 | Privileged access rights | <Insert persons name> | <Insert persons name> |
| 8.3 | Information access restriction | <Insert persons name> | <Insert persons name> |

| | | | |
|---|---|---|---|
| 8.4 | Access to source code | <Insert persons name> | <Insert persons name> |
| 8.5 | Secure authentication | <Insert persons name> | <Insert persons name> |
| 8.6 | Capacity management | <Insert persons name> | <Insert persons name> |
| 8.7 | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] |
| 8.16 | Monitoring activities | <Insert persons name> | <Insert persons name> |
| 8.17 | Clock synchronization | <Insert persons name> | <Insert persons name> |
| 8.18 | Use of privileged utility programs | <Insert persons name> | <Insert persons name> |
| [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] |

| | | | |
|---|---|---|---|
| 8.29 | Security testing in development and acceptance | <Insert persons name> | <Insert persons name> |
| 8.30 | Outsourced development | <Insert persons name> | <Insert persons name> |
| [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] |

# [Company] : ISO 27001:2013 ISMS RASCI Matrix

**Classification: Confidential**

| ISO27002:2013 - ISMS Accountability | | Responsible Named Person<br>(The person who is ultimately responsible for the completion of a task) | Accountable Named Person<br>(The person who is ultimately accountable for the success or failure of a task) |
|---|---|---|---|
| **4** | **Context of the organisation** | <Insert persons name> | <Insert persons name> |
| 4.1 | Understanding the organisation and its context | <Insert persons name> | <Insert persons name> |
| 4.2 | Understanding the needs and expectations of interested parties | <Insert persons name> | <Insert persons name> |
| [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] |
| **5** | **Leadership** | <Insert persons name> | <Insert persons name> |
| 5.1 | Leadership and commitment | <Insert persons name> | <Insert persons name> |
| 5.2 | Policy | <Insert persons name> | <Insert persons name> |
| 5.3 | Organisational roles, responsibilities and authorities | <Insert persons name> | <Insert persons name> |
| **6** | **Planning** | <Insert persons name> | <Insert persons name> |
| 6.1 | **Actions to address risks and opportunities** | <Insert persons name> | <Insert persons name> |
| 6.1.1 | General | <Insert persons name> | <Insert persons name> |
| [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] |
| 6.2 | **Information security objectives and planning to achieve them** | <Insert persons name> | <Insert persons name> |
| 6.2 | General | <Insert persons name> | <Insert persons name> |

|  |  |  |  |
|---|---|---|---|
| **7** | **Support** | <Insert persons name> | <Insert persons name> |
| 7.1 | Resources | <Insert persons name> | <Insert persons name> |
| 7.2 | Competence | <Insert persons name> | <Insert persons name> |
| [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] |
| 7.5.1 | Documented information General | <Insert persons name> | <Insert persons name> |
| 7.5.2 | Creating and updating | <Insert persons name> | <Insert persons name> |
| 7.5.3 | Control of documented information | <Insert persons name> | <Insert persons name> |
| **8** | **Operation** | <Insert persons name> | <Insert persons name> |
| 8.1 | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] |
| 8.3 | Information security risk treatment | <Insert persons name> | <Insert persons name> |
| **9** | **Performance evaluation** | <Insert persons name> | <Insert persons name> |
| 9.1 | Monitoring, measurement, analysis and evaluation | <Insert persons name> | <Insert persons name> |
| [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] |
| **10** | **Improvement** | <Insert persons name> | <Insert persons name> |
| 10.1 | Nonconformity and corrective action | <Insert persons name> | <Insert persons name> |
| 10.2 | Continual improvement | <Insert persons name> | <Insert persons name> |

# [Company] : ISO 27001:2013 ANNEX A RASCI Matrix

**Classification: Confidential**

| ISO27002:2013 - Annex A Controls | | Responsible Named Person<br>(The person who is ultimately responsible for the completion of a task) | Accountable Named Person<br>(The person who is ultimately accountable for the success or failure of a task) |
|---|---|---|---|
| **5** | **Information Security Policies** | | |
| 5.1.1 | Policies for Information Security | <Insert persons name> | <Insert persons name> |
| 5.1.2 | Review of the policies for Information Security | <Insert persons name> | <Insert persons name> |
| **6** | **Organization of Information Security** | | |
| 6.1.1 | Information security roles and responsibilities | <Insert persons name> | <Insert persons name> |
| 6.1.2 | Segregation of duties | <Insert persons name> | <Insert persons name> |
| [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] |
| **7** | **Human resource security** | | |
| 7.1.1 | Screening | <Insert persons name> | <Insert persons name> |
| 7.1.2 | Terms and conditions of employment | <Insert persons name> | <Insert persons name> |
| 7.2.1 | Management responsibilities | <Insert persons name> | <Insert persons name> |
| 7.2.2 | Information Security awareness, education and training | <Insert persons name> | <Insert persons name> |

| | | | |
|---|---|---|---|
| 7.2.3 | Disciplinary process | <Insert persons name> | <Insert persons name> |
| 7.3.1 | Termination or change of employment responsibilities | <Insert persons name> | <Insert persons name> |
| **8 Asset management** | | | |
| 8.1.1 | Inventory of assets | <Insert persons name> | <Insert persons name> |
| 8.1.2 | Ownership of assets | <Insert persons name> | <Insert persons name> |
| 8.1.3 | Acceptable use of assets | <Insert persons name> | <Insert persons name> |
| 8.1.4 | Return of assets | <Insert persons name> | <Insert persons name> |
| [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] |
| **9 Access control** | | | |
| 9.1.1 | Access Control Policy | <Insert persons name> | <Insert persons name> |
| 9.1.2 | Access to networks and network services | <Insert persons name> | <Insert persons name> |
| 9.2.1 | User registration and de-registration | <Insert persons name> | <Insert persons name> |
| 9.2.2 | User access provisioning | <Insert persons name> | <Insert persons name> |
| 9.2.3 | Management of privileged access rights | <Insert persons name> | <Insert persons name> |
| 9.2.4 | Management of secret authentication information of users | <Insert persons name> | <Insert persons name> |
| 9.2.5 | Review of user access rights | <Insert persons name> | <Insert persons name> |
| [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] |

| | | | |
|---|---|---|---|
| 9.4.4 | Use of privileged utility programs | <Insert persons name> | <Insert persons name> |
| 9.4.5 | Access Control to program source code | <Insert persons name> | <Insert persons name> |
| [redacted] | | | |
| 10.1.1 | Policy on the use of cryptographic controls | <Insert persons name> | <Insert persons name> |
| 10.1.2 | Key management | <Insert persons name> | <Insert persons name> |
| [redacted] | | | |
| 11.1.1 | Physical Security perimeter | <Insert persons name> | <Insert persons name> |
| 11.1.2 | Physical entry controls | <Insert persons name> | <Insert persons name> |
| [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | | | |
| 12.1.1 | Documented operating procedures | <Insert persons name> | <Insert persons name> |
| 12.1.2 | Change management | <Insert persons name> | <Insert persons name> |
| 12.1.3 | Capacity management | <Insert persons name> | <Insert persons name> |
| [redacted] | [redacted] | [redacted] | [redacted] |

|  |  |  |  |
|---|---|---|---|
| 12.2.1 | Controls against malware | <Insert persons name> | <Insert persons name> |
| 12.3.1 | Information backup | <Insert persons name> | <Insert persons name> |
| [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] |
| 12.7.1 | Information systems audit controls | <Insert persons name> | <Insert persons name> |
| [redacted] |  |  |  |
| 13.1.1 | Network controls | <Insert persons name> | <Insert persons name> |
| 13.1.2 | Security of network services | <Insert persons name> | <Insert persons name> |
| [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] |
| 13.2.4 | Confidentiality or non-disclosure agreements | <Insert persons name> | <Insert persons name> |
| [redacted] |  |  |  |
| 14.1.1 | Information Security requirements analysis and specification | <Insert persons name> | <Insert persons name> |
| 14.1.2 | Securing application services on public networks | <Insert persons name> | <Insert persons name> |
| 14.1.3 | Protecting application services transactions | <Insert persons name> | <Insert persons name> |
| 14.2.1 | Secure development policy | <Insert persons name> | <Insert persons name> |
| [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] |

|  |  |  |  |
|---|---|---|---|
| 14.2.5 | Secure system engineering principles | <Insert persons name> | <Insert persons name> |
| 14.2.6 | Secure development environment | <Insert persons name> | <Insert persons name> |
| 14.2.7 | Outsourced development | <Insert persons name> | <Insert persons name> |
| 14.2.8 | System security testing | <Insert persons name> | <Insert persons name> |
| 14.2.9 | System acceptance testing | <Insert persons name> | <Insert persons name> |
| 14.3.1 | Protection of test data | <Insert persons name> | <Insert persons name> |
| **15 Supplier relationships** |  |  |  |
| 15.1.1 | Information Security policy for supplier relationships | <Insert persons name> | <Insert persons name> |
| 15.1.2 | Addressing security within supplier agreements | <Insert persons name> | <Insert persons name> |
| [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] |
| **16 Information security incident management** |  |  |  |
| 16.1.1 | Responsibilities and procedures | <Insert persons name> | <Insert persons name> |
| 16.1.2 | Reporting Information Security events | <Insert persons name> | <Insert persons name> |
| 16.1.3 | Reporting Information Security weaknesses | <Insert persons name> | <Insert persons name> |
| [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] |
| **17 Information security aspects of business continuity management** |  |  |  |
| 17.1.1 | Planning Information Security continuity | <Insert persons name> | <Insert persons name> |
| 17.1.2 | Implementing Information Security continuity | <Insert persons name> | <Insert persons name> |
| [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] |
| **18 Compliance** |  |  |  |

| | | | |
|---|---|---|---|
| 18.1.1 | Identification of applicable legislation and contractual requirements | <Insert persons name> | <Insert persons name> |
| 18.1.2 | Intellectual property rights | <Insert persons name> | <Insert persons name> |
| 18.1.3 | Protection of records | <Insert persons name> | <Insert persons name> |
| 18.1.4 | Privacy and protection of personally identifiable information | <Insert persons name> | <Insert persons name> |
| [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] |