|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Audit Area | Compliant (Yes/No) | | Observations/Comments | | Action Required | |
| GENERAL AUDIT POINTS | | | | | | |
| Policy Compliance | | | | | | |
| 1.1 Are the correct encryption methods being used for data in storage and transmission? |  | |  | |  | |
| 1.2. Are the related DLP Policies being adhered to? |  | |  | |  | |
| 1.3. Are the related Data Classification Policies being adhered to? |  | |  | |  | |
| 1.4. Have forms of physical security for data protection been implemented? |  | |  | |  | |
| 1.5. Have forms of digital security for data protection been implemented? |  | |  | |  | |
| 1.6. Have EASM risks been identified? |  | |  | |  | |
| 1.7. Have appropriate EASM risk management strategies been implemented? |  | |  | |  | |
| 1.7. Have all employees undergone the appropriate User Awareness Training? |  | |  | |  | |
| Audit Area | | | Compliant (Yes/No) | | Observations/Comments | | Action Required | |

|  |  |  |  |
| --- | --- | --- | --- |
| GENERAL AUDIT POINTS | | | |
| Ethical Considerations and Requirements | | | |
| 2.1. Are all forms of data collection briefed with customers, and consent is gathered? |  |  |  |
| 2.2. Has all collected information and data been classified with data classification requirements? |  |  |  |
| 2.3. Is data anonymity used to protect the privacy of customers? |  |  |  |
| 2.4. Is the cryptography policy being adhered to? |  |  |  |
| 2.5. Is data minimalization being put in place when collecting data? |  |  |  |
| 2.6. Looping back to the ISMS policies, are they being adhered to when required? |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| GENERAL AUDIT POINTS | | | |
| Governance | | | |
| 3.1. Is the team adhering to the company’s governance framework? |  |  |  |
| 3.2. Are team roles and responsibilities clearly defined and documented? |  |  |  |
| 3.3. Is there a risk management plan in place? |  |  |  |
| 3.4. Is there an incident response plan in place? |  |  |  |
| 3.5. Are incidents logged and reviewed for continuous improvement? |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Audit Area | Compliant (Yes/No) | Observations/Comments | Action Required |

**Project-Specific Audit Points**[**​**](http://localhost:3000/redback-documentation/docs/cybersecurity/GRC-Team-Audits/audit-template#project-specific-audit-points)

Auditors need to develop their own range of audit points for their respective project of audit, these may only apply to the project that they are auditing. The structure for the General Audit Points section should be used.

**Summary**

After the audit has been completed, a report needs to be formed. The structure of this report can be sourced from existing reports, though the video link below includes a tutorial on how to conduct the audit and formulate an audit report.

**Link:** <https://www.youtube.com/watch?v=FvGHO3ixBo8>

**Key Findings & Recommendations**