|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  | |
|  | **ISO/IEC 27002 Standard** | | |  |  | |
|  |  |  |  |  |  | |
|  | **SECURITY GAP ANALYSIS** | | | |  | |
|  |  |  |  |  |  | |
|  |  |  |  |  |  | |
| **01** | |  |  |  |  | |
|  | **Access Control | Limit access to data** | |  | |
|  | Current Practice: | Role-based access |  | |
|  |  |  | Best Practice: | Mandatory access control |  | |
|  |  |  |  |  |  | |
| **02** | |  |  |  |  | |
|  | **Encryption | Encrypt sensitive data** | |  | |
|  | Current Practice: | Some data encrypted |  | |
|  |  |  | Best Practice: | All sensitive data encrypted |  | |
|  |  |  |  |  |  | |
| **03** | |  |  |  |  | |
|  | **Patch Management | Apply timely patches** | |  | |
|  | Current Practice: | Monthly patch cycle |  | |
|  |  |  | Best Practice: | Weekly patch cycle |  | |
|  |  |  |  |  |  | |
| **04** | |  |  |  |  | |
|  | **Incident Response | Detect and respond to incidents** | |  | |
|  | Current Practice: | Manual incident handling |  | |
|  |  |  | Best Practice: | Automated incident response |  | |
|  |  |  |  |  |  | |
| **05** | |  |  |  |  | |
|  | **Network Security | Segment network zones** | |  | |
|  | Current Practice: | Flat network architecture |  | |
|  |  |  | Best Practice: | VLANs and firewalls for segmentation |  | |
|  |  |  |  |  |  | |
| **06** | |  |  |  |  | |
|  | **Data Backup | Regular backups** | |  | |
|  | Current Practice: | Weekly backups |  | |
|  |  |  | Best Practice: | Daily backups with off-site storage |  | |
|  |  |  |  |  |  | |
|  | **Review your current practices against industry best practices. Note where your organization falls short (the gaps). For each gap, propose corrective actions.** | | | |  | |
|  |  |  |  |  |  | |
|  | **SECURITY CONTROL AREA** | | | **CORRECTIVE ACTION** |  | |
|  |  |  |  |  |  | |
|  | **Access Control Gap** | | | Implement mandatory access controls for critical systems. |  | |
|  | **Encryption Gap** | | | Encrypt all sensitive data at rest and in transit. |  | |
|  | **Patch Management Gap** | | | Increase patch frequency to weekly. |  | |
|  | **Incident Response Gap** | | | Invest in automated incident detection and response tools. |  | |
|  | **Network Security Gap** | | | Implement VLANs (Virtual LANs) and firewalls to segment your network zones. | |  |
|  | **Data Backup Gap** | | | Increase the frequency of data backups to daily and ensure off-site storage. |  | |
|  |  |  |  |  |  | |
|  |  |  |  | [**© TemplateLab.com**](https://templatelab.com/) | | |