# **IT Process Checklist**

The following is a partial list of IT processes that your organization may wish to consider implementing to improve the maturity and stability of your technology platforms. Consider the data you gathered in the *BCF - System Risk Analysis Spreadsheet, ’*System Data’ tab and put a check next to each process that is missing, or not being followed consistently:

|  |  |  |  |
| --- | --- | --- | --- |
| **Followed?** | **Process Name** | **Description** | **Business Risks Addressed** |
| ☐ | **Backup Management** | Regularly creating copies of data to ensure data can be restored in case of loss or corruption. This process should include systematic validation of these backups. | Data loss, data corruption, ransomware attacks, compliance issues. |
| ☐ | **System Protections** (Encryption) | Implementing encryption methods to protect data at rest and in transit. | Data breaches, unauthorized access, data theft, compliance issues. |
| ☐ | **System Protections** (Anti-malware) | Utilizing software to detect, prevent, and remove malicious software. | Malware infections, data breaches, operational disruptions, financial loss. |
| ☐ | **Change Management** | Establishing procedures for managing changes to IT systems and services. | Unplanned downtime, configuration errors, security vulnerabilities, compliance issues. |
| ☐ | **Configuration Management** | Maintaining and managing the configuration of IT systems to ensure consistency and compliance. | Configuration drift, compliance issues, security vulnerabilities, operational inefficiencies. |
| ☐ | **Access Management** | Controlling and monitoring access to systems and data to ensure only authorized users have access. | Unauthorized access, data breaches, insider threats, compliance issues. |
| ☐ | **Incident Management** | Identifying, managing, and resolving incidents to minimize impact on business operations. Includes cyber incident management and response. | Prolonged downtime, data loss, operational disruptions, reputational damage. |
| ☐ | **Vulnerability Management** | Identifying, evaluating, and mitigating security vulnerabilities in IT systems and software. | Security breaches, data theft, compliance issues, operational disruptions. |

(continued…)

|  |  |  |  |
| --- | --- | --- | --- |
| **Followed?** | **Process Name** | **Description** | **Business Risks Addressed** |
| ☐ | **Patch Management** | Regularly updating software and systems with patches to fix vulnerabilities. | Security vulnerabilities, malware infections, compliance issues, operational disruptions. |
| ☐ | **Network Security Management** | Implementing measures to protect the network infrastructure from unauthorized access and threats. | Network breaches, data theft, operational disruptions, financial loss. |
| ☐ | **Disaster Recovery Planning** | Developing and implementing plans to restore IT systems and data after a disaster. | Prolonged downtime, data loss, operational disruptions, financial loss. |
| ☐ | **Vendor Management** | Managing third-party vendors to ensure they meet security and compliance requirements. | Third-party risks, data breaches, compliance issues, operational disruptions. |
| ☐ | **Compliance Management** | Ensuring IT processes and systems comply with relevant regulations and standards. | Regulatory penalties, legal issues, reputational damage, financial loss. |
| ☐ | **Physical Security** | Implementing measures to protect physical access to IT infrastructure and data centers. | Unauthorized physical access, theft, vandalism, data breaches, operational disruptions. |
| ☐ | **Security Monitoring and Management** | Continuously monitoring IT systems for signs of security threats or incidents. | Early detection of security threats, data breaches, unauthorized access, compliance issues. |