ESEVEL

SOC 2 COMPLIANCE CHECKLIST: A DETAILED GUIDE FOR 2025

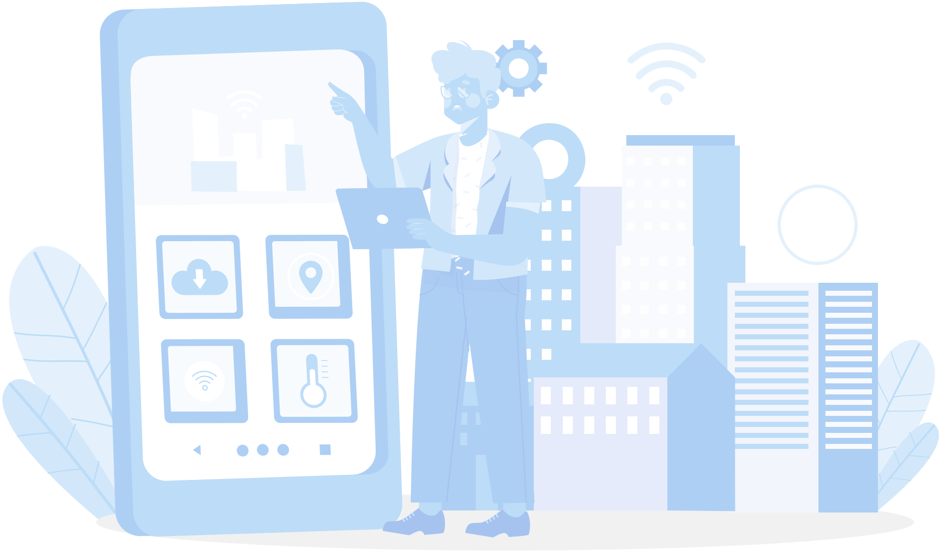
ESEVEL.COM

SECURITY

Access Controls

- Ensure systems are protected against unauthorized access with multi-factor authentication (MFA).
- Implement role-based access control (RBAC) to limit access based on job roles.

- Set up automated workflows with HR and IT software to revoke access as soon as an employee's status changes.
- Regularly review and update user access rights, revoking access promptly for employees who leave the company.
- Ensure physical access to data centers and sensitive areas is restricted to authorized personnel only.



Network and System Security

- Implement firewalls, intrusion detection/prevention systems, and antivirus software.
- Encrypt data in transit and at rest using secure encryption protocols.

📌 **Example:** Use Secure/Multipurpose Internet Mail Extensions (S/MIME) or Pretty Good Privacy (PGP) for email encryption to protect messages containing sensitive data.

- Regularly conduct vulnerability scans and penetration tests on all systems.
- Patch and update software and systems promptly, following a documented patch management process.

Monitoring and Alerting

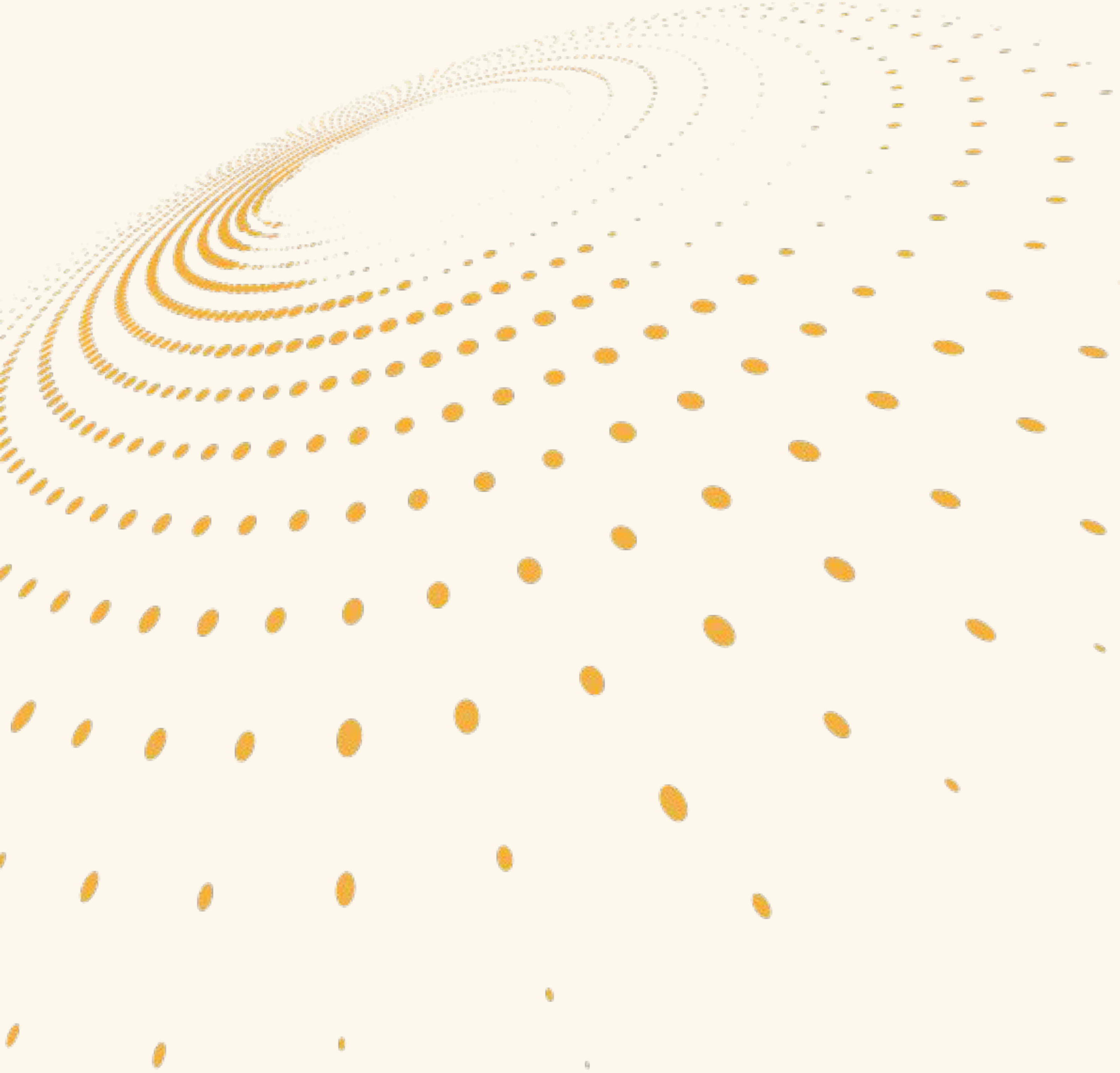
- Monitor systems for unusual activity and log access to sensitive information.
- Set up automated alerts for potential security incidents or breaches.
- Ensure logging mechanisms capture necessary data for security investigations.
- Retain logs for a specified period as per compliance needs (often 1–3 years).

- Develop and maintain an incident investigation and mitigation checklist.
- Conduct regular incident response drills and training for the security team.

📌 **Example:** Simulate a phishing attack as a training exercise.

- Document and analyze all incidents to prevent future occurrences

AVAILABILITY



System and Service Monitoring

- Monitor the uptime of critical systems and set SLAs for service availability.

💡 **Tip:** Use a performance dashboard to visualize and track system uptime metrics in real-time, making it easier to detect and resolve issues proactively.

- Implement redundancy for critical infrastructure components, such as servers and databases.
- Ensure there are automated alerts for service outages or degradations.

Disaster Recovery and Business Continuity

- Develop and maintain a Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP).

🔎 Definition

- **Business Continuity Plan (BCP):** A BCP outlines strategies to keep critical business functions operational during and after an unplanned disruption.
- **Disaster Recovery Plan (DRP):** A DRP details the processes for restoring IT systems and data after a disaster.

- Conduct regular backup procedures and test restore capabilities.

Disaster Recovery and Business Continuity

- Define Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) for all critical systems.

🔎 **Definition**

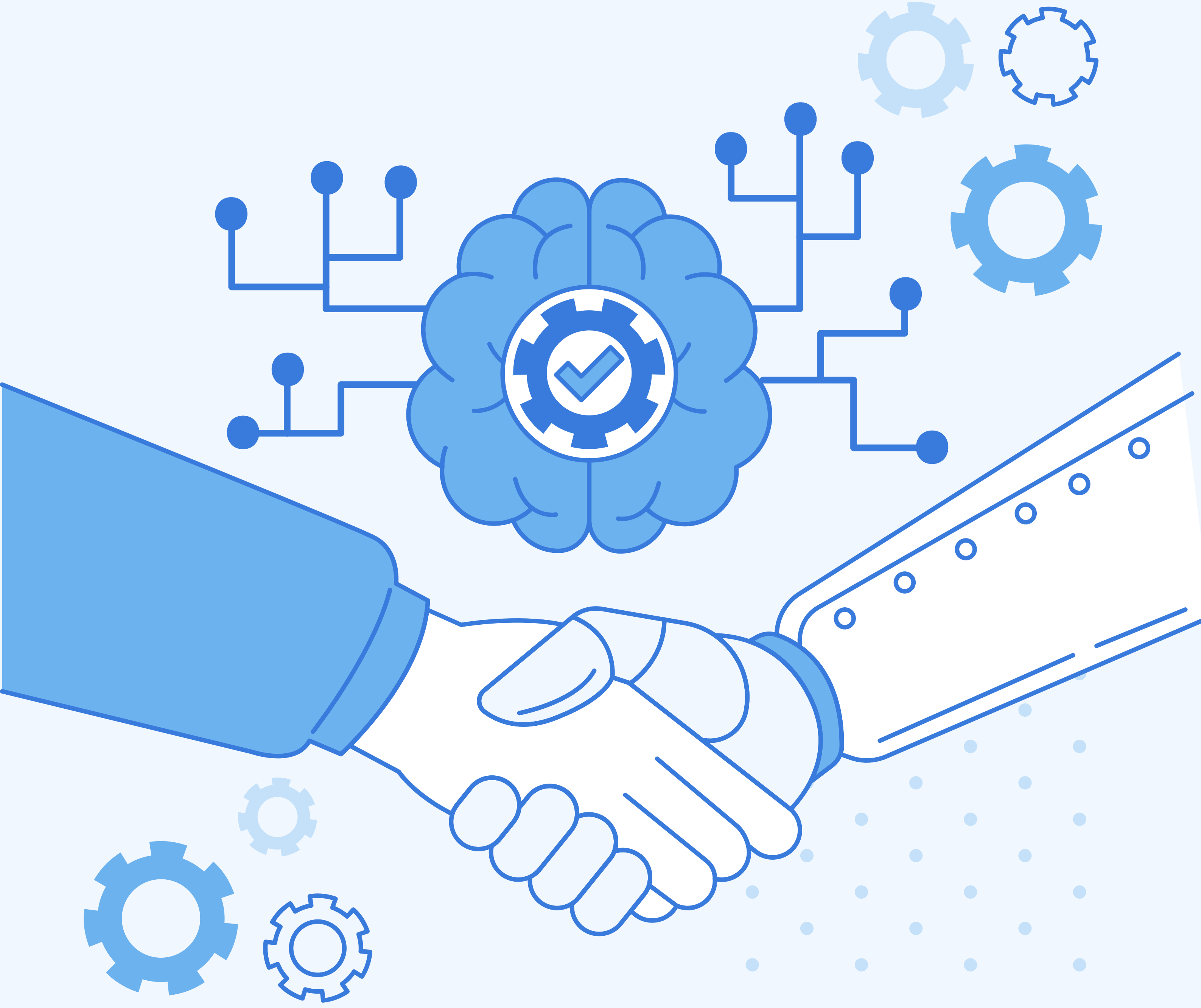
- **Recovery Time Objective (RTO):** RTO is the maximum allowable time to restore systems after a disruption to minimize business impact.
- **Recovery Point Objective (RPO):** RPO is the maximum acceptable data loss measured in time, defining how often data should be backed up.

- Ensure alternate sites and systems are prepared to handle critical business operations.

Capacity Management

- Monitor resource usage (CPU, memory, storage) to prevent resource exhaustion.
- Incorporate auto-scaling policies to ensure your systems can handle increased traffic or demand without compromising performance.
- Regularly assess infrastructure capacity and adjust as necessary to maintain availability.

PROCESSING INTEGRITY



Data Quality and Accuracy

- Implement input validation to ensure data is accurate, complete, and valid.

> 💡 **Tip:** Apply validation to prevent incorrect formats for critical fields, such as requiring email addresses to contain “@” and “.com” for proper structure.
>
> - Use data validation techniques such as checksums or parity bits for data integrity verification.
> - • Ensure data reconciliation processes are in place to detect and correct discrepancies.

System Monitoring and Testing

- Regularly test applications and systems to ensure they are processing data correctly.
- Perform change management and quality assurance testing for all system updates or changes.
- Document and resolve any processing errors or anomalies promptly.

Error Handling and Corrections

- Define error-handling procedures for data processing issues.
- Automate error logging and notification systems for quick detection and resolution.
- Maintain an audit trail of errors and corrective actions.

CONFIDENTIALITY

Data Encryption and Protection

Encrypt sensitive data using industry-standard protocols (e.g., AES-256).

💡 **Tip:** Regularly rotate encryption keys and store them securely to protect encrypted data effectively.

- Use strong access controls to limit access to confidential information.
- • Ensure data is securely disposed of when no longer needed.

📌 **Example:** Use trusted data-wiping software, like Esevel, to securely delete data on retired hardware before disposal.

Data Masking and Anonymization

- Use data masking techniques for non-production environments to protect sensitive data.
- Implement data anonymization or pseudonymization for data used in analysis to protect privacy.

💡 **Tip:** Anonymize data used in analytics to reduce the risk of exposing individual identities

Data Retention and Disposal

Define and enforce a data retention policy based on business and compliance requirements.

💡 **Tip:** Get Esevel free IT asset disposal template to set up a complete and secure device disposal process. 💻

- Securely delete data when it is no longer needed, using methods like shredding or wiping.
- Document the disposal process to maintain an audit trail.

Third-Party Confidentiality Agreements

- Ensure confidentiality clauses are included in contracts with third-party vendors.
- Conduct regular security assessments of third-party vendors to verify their adherence to confidentiality requirements.

PRIVACY

Data Collection and Processing

PRIVACY

- Ensure data collection practices comply with applicable privacy regulations (e.g., GDPR, CCPA).
- Only collect personal data necessary for business operations.

📌 **Example:** For user accounts, collect only essential details like name, email, and contact number, omitting sensitive data unless absolutely require

• Implement consent management systems to track and manage user consent.

Privacy Notice and Transparency

- Update privacy policies to reflect current data practices and regulatory requirements.
- Make privacy notices easily accessible and understandable for users.
- Document data flows and ensure users are informed about how their data is used.

Data Subject Rights

- Implement mechanisms for users to request data access, correction, or deletion.

💡 **Tip:** Establish an easy-to-navigate self-service portal for users to submit requests related to their personal data.

- Respond to data subject requests within regulatory timelines.
- • Keep records of all data subject requests and the actions taken to address them.

Training and Awareness

- Conduct regular privacy training for employees on handling personal data.
- Ensure employees are aware of privacy policies and their responsibilities to protect personal data.
- Test employees’ knowledge of privacy practices to reinforce training effectiveness.

General Best Practices

Documentation and Policies

- Maintain and regularly update all security and compliance policies, including:
- Access Control Policy
- Incident Response Plan
- Data Retention Policy
- Business Continuity Plan
- Keep audit trails and records of compliance activities for SOC 2 audits.

Regular Audits and Assessments

- Conduct internal audits regularly to identify compliance gaps.
- Schedule external audits as required for SOC 2 certification.
- Regularly review and update compliance documentation to align with the latest standards and regulations.