TOPCERTIFIER

Governance, Risk & Compliance Consultants

SOC 2 GAP ANALYSIS TEMPLATE

INTRODUCTION:

Certainly, here's a checklist to help pinpoint areas where your organization might require enhancements to conform with SOC 2 (System and Organization Controls 2) standards. This checklist serves as an initial step in assessing your compliance with SOC 2 Trust Services Criteria

SECTION 1: PROCESS MANAGEMENT

- ☐ Is there clear leadership commitment to information security and SOC 2 compliance?
- ☐ Are information security policies and procedures established and communicated to relevant personnel?
- ☐ Is there a defined risk management program that addresses information security risks?

SECTION 2: PLANNING

- ☐ Are information security policies documented and aligned with SOC 2 Trust Services Criteria?
- ☐ Are there policies and procedures related to access control, data protection, and incident response?

SECTION 3: ASSET MANAGEMENT

- ☐ Are information assets identified, documented, and classified based on sensitivity?
- ☐ Is there a process for managing the lifecycle of information assets, including secure disposal?

SECTION 4: ACCESS CONTROL

- ☐ Are access controls in place to ensure only authorized individuals have access to information systems and data?
- ☐ Is there a process for user access provisioning and de-provisioning, including role-based access controls?

SECTION 5: RISK ASSESSMENT AND MANAGEMENT

- ☐ Are risks to information security assessed, and are appropriate measures in place to mitigate these risks?
- ☐ Is there a documented incident response plan for handling security incidents?

SECTION 6: SECURITY AWARENESS AND TRAINING

- ☐ Is there an awareness program for employees regarding information security and SOC 2 requirements?
- ☐ Are employees trained to recognize and respond to security threats and incidents?

SECTION 7: MONITORING AND RESPONSE

- ☐ Is there continuous monitoring of information systems and networks for security events?
- ☐ Is there a documented process for incident detection, response, and reporting?

SECTION 8: COMPLIANCE AND REPORTING

- ☐ Are regular internal audits conducted to assess compliance with SOC 2 Trust Services Criteria?
- ☐ Is there a process for the timely reporting of security incidents to appropriate parties?

SECTION 9: VENDOR MANAGEMENT

- ☐ Is there a vendor risk management program in place for assessing and monitoring third-party service providers?
- ☐ Are contracts with third-party vendors and service providers reviewed to ensure they meet information security requirements?

SECTION 10: PHYSICAL AND ENVIRONMENTAL SECURITY

- ☐ Are physical security measures in place to protect information systems and data centers?
- ☐ Is environmental protection and monitoring conducted for critical infrastructure?

SECTION 11: SYSTEM DEVELOPMENT AND MAINTENANCE

- ☐ Are secure development practices followed for in-house software development?
- ☐ Is there a process for assessing and managing security during system changes and maintenance?

Please note that this checklist provides a high-level overview, and it's essential to perform a thorough analysis specific to your organization's information systems and context. Additionally, it's recommended to engage with SOC 2 experts or consultants to conduct a comprehensive gap analysis for your organization's unique needs and risks.