Service Organization Control (SOC 2) Compliance

Using RidgeBot Security Validation

RIDGE SECURITY

Protect Organizations from Risk when Engaging 3rd-Party Vendors/Partners

Abstract

This white paper discusses how RidgeBot capabilities—including asset discovery, attack surface identification, iterative security validation, automated and on-demand penetration testing, and vulnerability exploitation and remediation—can help organizations comply with the Service Organization Control (SOC 2) specifications. A SOC 2 certification substantially increases confidence and peace of mind when organizations engage 3rd-party vendors or partners in their business processes, for example, many security-focused organizations require SOC 2 compliance before considering a SaaS provider.

Introduction

Organizations rarely operate in isolation. Increasingly organizations of all sizes outsource aspects of their operations to leverage the economic benefits of business relationships with other organizations—service providers, cloud providers, partners, vendors—to achieve their objectives more efficiently and competitively. While these relationships may increase revenues, expand market opportunities or reduce costs for an organization, they also introduce risks arising from the interactions between the systems of the organization and those of the service organization.

The SOC 2 specifications was developed by The American Institute of Certified Public Accountants (AICPA) circa 2010, and revised in 2013 and 2017. AICPA is the national professional organization of Certified Public Accountants (CPAs) in the United States, with more than 400,000 members in over 100 countries in business and industry, public practice, government, education, student affiliates and international associates. The Institute was founded in 1887 with the objective to set ethical standards for the U.S. accounting profession, as well as auditing standards for private companies, non-profit organizations, federal, state and local governments.

SOC Overview

System and Organization Controls (SOC) is a suite of service offerings CPAs may provide in connection with system-level controls of a service organization, or entity-level controls of other organizations. The SOC suite of offerings include:

- **SOC for Service Organizations:** Internal-control reports on the services provided by a service organization. These reports document valuable information to enable organizations to assess and address the risks associated with an outsourced service:
  - SOC 1: SOC for Service Organizations—Internal Control over Financial Reporting (ICFR)
  - SOC 2: SOC for Service Organizations—Trust Services Criteria
  - SOC 3: SOC for Service Organizations—Trust Services Criteria for General Use Report
- **SOC for Cybersecurity:** A reporting framework through which organizations can communicate relevant useful information about the effectiveness of their cybersecurity risk management program, and CPAs can report on such information to meet the cybersecurity information needs of a broad range of stakeholders.
- **SOC for Supply Chain:** An internal-control report on an entity's system and controls for producing, manufacturing or distributing goods to better understand the cybersecurity risks in their supply chains.

The remainder of this white paper focuses on compliance with the requirements of the *SOC 2: Trust Services Criteria*, as documented here.

SOC 2 Auditing and Certification

The purpose of the *SOC 2 Trust Criteria* is to provide confidence and peace of mind when organizations engage 3rd-party vendors in their business processes. To achieve SOC 2 certification, an organization is audited by an independent licensed CPA who provides an attestation after determining if the organization has the appropriate safeguards and procedures in place.

Auditors provide a SOC 2 report for an organization that details the systems and controls you have in place for security compliance. Auditors check for proof and verify whether you meet the relevant trust principles. The report documents valuable information to enable organizations to assess and address the risks associated with an outsourced service

SOC 2 Trust Criteria

SOC 2 compliance enumerates specific criteria for managing customer data correctly. As is the case with other legal and industry standard requirements such as ISO 27001, PCI DSS and HIPAA, SOC 2 compliance specifications contain a mix of organizational management, process and procedural requirements, as well as technology-focused stipulations.

The *SOC 2 Trust Criteria* consist of 5 Trust Services Categories:

- Security
- Availability
- Processing Integrity
- Confidentiality
- Privacy

The Security Category covers access controls to prevent malicious attacks, unauthorized alteration or destruction of data, misuse of the organizations systems, or unauthorized access or disclosure of company or client information. A checklist of controls to be implemented include:

- **Logical and Physical Access Controls:** Restricting and managing logical and physical access to prevent unintended and unauthorized access.
- **System Operations:** Detecting and mitigating deviations from set procedures.
- **Change Management:** Implementing a process to prevent unauthorized system changes.
- **Risk Mitigation:** Risk mitigation activities to prevent business continuity disruptions.

The *SOC 2 Trust Services Criteria* are aligned with the 17 principles laid out in the COSO framework: the *Internal Control Integrated Framework* developed by the Committee of Sponsoring Organizations of the Treadway Commission (COSO). In addition to the 17 principles of the COSO framework, certain common criteria are shared amongst all the Trust Services Categories (Security, Availability, Processing Integrity, Confidentiality, and Privacy), as well as certain added supplemental criteria applicable to each category, as given in the table below.

Trust Services Category	Common Criteria	Additional Category-Specific Supplemental Criteria
Security	CC Series	N/A
Availability	CC Series	A Series
Processing Integrity	CC Series	PI Series
Confidentiality	CC Series	C Series
Privacy	CC Series	P Series

SOC 2 Content Outline

To provide perspective on where RidgeBot can help with compliance, the structural outline of the SOC 2 Trust Services Criteria (*TSP Section 100 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*) is given below, highlighting the specific sections that concern the protection of technology resources. The full text of the specification can be viewed here.

Common COSO Criteria

- CC1 Series: The Control Environment
  - **CC1.1: COSO principle 1**
  - CC1.2: COSO principle 2
  - CC1.3: COSO principle 3
  - CC1.4: COSO principle 4
  - CC1.5: COSO principle 5
- CC2 Series: Communication and Information
  - **CC2.1: COSO principle 13**
  - CC2.2: COSO principle 14
  - CC2.3: COSO principle 15
- CC3 Series: Risk Assessment
  - **CC3.1: COSO principle 6**
  - **CC3.2: COSO principle 7**
  - **CC3.3: COSO principle 8**
  - **CC3.4: COSO principle 9**
- CC4 Series: Monitoring of Controls
  - **CC4.1: COSO principle 16**
  - **CC4.2: COSO principle 17**
- CC5 Series: Control Activities (Related to The Design and Implementation of Controls)
  - **CC5.1: COSO principle 10**
  - **CC5.2: COSO principle 11**
  - **CC5.3: COSO principle 12**

Supplemental Criteria to COSO Principle 12

- CC6 Series: Logical and Physical Access Controls
  - **CC6.1: COSO principle 12 supplement 6.1**
  - **CC6.2: COSO principle 12 supplement 6.2**
  - CC6.3: COSO principle 12 supplement 6.3
  - **CC6.4: COSO principle 12 supplement 6.4**
  - CC6.5: COSO principle 12 supplement 6.5
  - **CC6.6: COSO principle 12 supplement 6.6**
  - CC6.7: COSO principle 12 supplement 6.7
  - **CC6.8: COSO principle 12 supplement 6.8**

- CC7 Series: System Operations
  - **CC7.1: COSO principle 12 supplement 7.1**
  - **CC7.2: COSO principle 12 supplement 7.2**
  - **CC7.3: COSO principle 12 supplement 7.3**
  - **CC7.4: COSO principle 12 supplement 7.4**
  - **CC7.5: COSO principle 12 supplement 7.5**
- CC8 Series: Change Management
  - **CC8.1: COSO principle 12 supplement 8.1**
- CC9 Series: Risk Mitigation
  - **CC9.1: COSO principle 12 supplement 9.1**
  - **CC9.2: COSO principle 12 supplement 9.2**

Supplemental Criteria Applicable to Specific Trust Categories

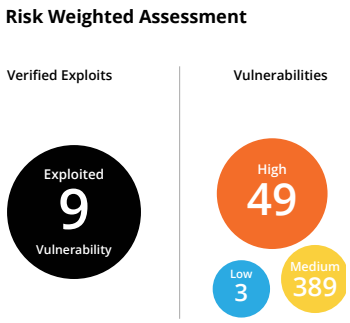
- A Series: Additional Criteria for **Availability**
  - A1.1: Capacity
  - A1.2: Environmental Protections and Backups
  - **A1.3: System Recovery Procedures**
- C Series: Additional Criteria for **Confidentiality**
  - C1.1: Identifies Confidential Information
  - C1.2: Disposal of Confidential Information
- PI Series: Additional Criteria for **Processing Integrity** (Over the Provision of Services or the Production, Manufacturing, or Distribution of Goods)
  - PI1.1: Quality Objectives
  - PI1.2: System Input Completeness and Accuracy
  - PI1.3: System Output Results
  - PI1.4: Output Delivery
  - PI1.5: Stored Items
- P Series: Additional Criteria for **Privacy**
  - P1.0 – P1.1: Privacy Criteria Related to Notice and Communication of Objectives Related to Privacy
  - P2.0 – P2.1: Privacy Criteria Related to Choice and Consent
  - P3.0 – P3.2: Privacy Criteria Related to Collection
  - P4.0 – P4.3: Privacy Criteria Related to Use, Retention, and Disposal
  - P5.0 – P5.2: Privacy Criteria Related to Access
  - P6.0 – P6.7: Privacy Criteria Related to Disclosure and Notification
  - P7.0 – P7.1: Privacy Criteria Related to Quality
  - P8.0 – P8.1: Privacy Criteria Related to Monitoring and Enforcement

Overview of How RidgeBot can Help

RidgeBot helps you find security deficits in your assets, and provides guidance and priority ranking on how to immediately remediate any exposures. Moreover, RidgeBot helps you maintain, on a continuing and cost-effective basis, a security posture that is always in compliance with the latest attack methods and threat intelligence.

Some of RidgeBot's key benefits to your organization's security posture include:

- **Improve and Simplify Security Activities and Process**
  - Discover, inventory and document system components, assets and attack surfaces. Because RidgeBot is fully automated, you can do this continuously, or at much more frequent intervals, than previous periodic manual processes.
  - Reports help document vulnerabilities found, exploited, remediated and validated.
  - Reports provide clear risk ranking to focus manual remediation activity on the highest risk vulnerabilities.
  - RidgeBot's flexibility allows you to run attack testing from inside and outside your environment.
  - RidgeSecurity's Threat Intelligence Platform knowledge base ensures that you are always up to date with industry-leading security vulnerability information.



  - Run RidgeBot attacks, scans and exploitations as a standard part of your ongoing security policy.
- **Continuous Security Validation**
  - RidgeBot provides no-cost iterative, continuous hardening and asset inventory. You can run different scans and exploitations periodically or continuously—because it is fully automated, no manual intervention is required until a vulnerability is reported.
  - Continuous monitoring and asset discovery protect against hacker intrusion caused by an employee (or any other person) accidentally or maliciously connecting untrusted or unplanned IoT, wireless or other unauthorized devices to the environment.
  - Scan reports provide a short list of must-fix exploitable vulnerabilities to document and resolve. Report output ensures all software patches and updates needed to resolve dangerous vulnerabilities are installed on all affected assets.
- **DevOps/SecOps Software Development and Patch/Release Testing**
  - Use RidgeBot during the software development process to help ensure that dangerous coding practices that introduce vulnerabilities never ship in new releases of software.
  - Use RidgeBot to harden software patches, software upgrades, new devices, and any configuration changes before pushing them into the production environment.

- **Security Posture Validation**
  - Continuously, iteratively attack the production environment to maintain security posture and discover misconfigurations in wireless or defensive security appliances or services such as firewall rules or UTM appliances.
  - Continuously monitor and harden login credentials on sensitive assets.
- **Compliance Audit**
  - Continuous asset discovery scanning, and attack and exploitation attempts (and the reports issued) mean your environment is always audit-ready.
  - Use RidgeBot reports to submit evidence of vulnerabilities probed, remediated and resolved.
- **Security Incident Response**
  - Scan reports, containing recommended solutions for each vulnerability found, provide critical information to your security incident response/escalation team.
  - Risk ranking of vulnerabilities feed into the priorities and procedures for incident response.
  - RidgeBot AI/ML exploitation attacks provide forensic capabilities to investigate the origin and path taken by a breach, as well as step-by-step guidance on how to resolve the entry point vulnerability.

RidgeBot includes several template scans that you can easily use, as well as the flexibility to completely customize your own scans. The system templates include:

- **Full scan:** This test launches numerous attack techniques used by real-world hackers. Based on threat intelligence and an exploit knowledge base, RidgeBot profiles assets, mines vulnerabilities and launches attacks against target assets, which may be internal or external to your environment, in a private or public environment.
- **Ransomware scan:** This test is specifically focused on combating ransomware attacks. It launches scans for 27 high-profile ransomware entry point vulnerabilities, includes the ability to attack and exploit these vulnerabilities, and reports in detail exactly how successful exploitations were achieved. Definitions of more ransomware attacks will be added over time, and you can add these to your security arsenal by downloading periodic RidgeBot updates.
- **Weak password scan:** This test launches direct or iterative attacks based on sensitive information collected via weak credential or unauthorized access vulnerabilities. Attack targets include redis, elasticsearch, ActiveMQ, database, web login and other applications.
- **Struts2 scan:** This test launches direct or iterative attacks based on known 1-day or n-day vulnerabilities detected on targets using the Struts 2 framework.
- **Weblogic scan:** This test launches direct or iterative attacks based on known 1-day or n-day vulnerabilities detected on targets using Weblogic middleware.
- **Web scan:** This test launches cyberattacks against target websites, web applications and all related attack surfaces to gain control of the target website for both self-developed and contact management system-based websites.
- **Host scan:** This test launches direct or iterative attacks from inside a corporate network to validate the security system's response to an internal threat. Target systems include all network-accessible internal hosts and servers.

How RidgeBot can Help with Specific SOC 2 Requirements

Only the relevant extracts of the requirements are listed in this section. The full text of the specification can be viewed here.

CC1: The Control Environment

Requirement CC1.1: COSO Principle 1—The entity demonstrates a commitment to integrity and ethical values.

- **Addresses Deviations in a Timely Manner—**Deviations from the entity's expected standards of conduct are identified and remedied in a timely and consistent manner.

  Using RidgeBot to Comply:

  - Scan-and-exploitation reports can assist you in quickly compiling consistent and comparable documentation of vulnerabilities found, vulnerability ranking, successful exploits, and the mitigation and remedial steps taken. This information can be used to take mitigation actions, document past mitigation actions, and/or to prepare management reports.
  - Scan-and-exploitation reports include recommended mitigation solutions for each vulnerability. Following these recommended remediations can address deviations quickly and easily.

CC2: Communication and Information

Requirement CC2.1: COSO Principle 13—The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.

- **Captures Internal and External Sources of Data—**Information systems capture internal and external sources of data.
- **Processes Relevant Data into Information—**Information systems process and transform relevant data into information.

  Using RidgeBot to Comply:

  - Automated asset discovery can help you compile and maintain an inventory of all data processing assets (sources of data) and attack surfaces (the vulnerabilities of your sources of data).
  - Additionally, an asset discovery scan iteratively discovers and documents changes in the presence of assets that may perhaps pose a risk to your sources of data.
  - Scan-and-exploitation reports can assist you in quickly compiling consistent and comparable summary and actionable documentation of vulnerabilities found, vulnerability ranking, successful exploits, and the mitigation and remedial steps taken. This information summarizes a vast quantity of vulnerability scan results into actionable information.

CC3: Risk Assessment

Requirement CC3.1: COSO Principle 6—The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.

- **Considers Tolerances for Risk—**Management considers the acceptable levels of variation relative to the achievement of operations objectives.

  Using RidgeBot to Comply:

  - Scan-and-exploitation reports can assist you in quickly compiling consistent and comparable summary and actionable documentation of vulnerabilities found, vulnerability ranking, successful exploits, and the mitigation and remedial steps taken. The ranking information can be used to judge acceptable levels of risk.

Requirement CC3.2: COSO Principle 7—The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.

- **Includes Entity, Subsidiary, Division, Operating Unit, and Functional Levels—**The entity identifies and assesses risk at the entity, subsidiary, division, operating unit, and functional levels relevant to the achievement of objectives.
- **Analyzes Internal and External Factors—**Risk identification considers both internal and external factors and their impact on the achievement of objectives.
- **Involves Appropriate Levels of Management—**The entity puts into place effective risk assessment mechanisms that involve appropriate levels of management.
- **Estimates Significance of Risks Identified—**Identified risks are analyzed through a process that includes estimating the potential significance of the risk.
- **Determines How to Respond to Risks—**Risk assessment includes considering how the risk should be managed and whether to accept, avoid, reduce, or share the risk.
- **Identifies and Assesses Criticality of Information Assets and Identifies Threats and Vulnerabilities—**The entity's risk identification and assessment process includes (1) identifying information assets, including physical devices and systems, virtual devices, software, data and data flows, external information systems, and organizational roles; (2) assessing the criticality of those information assets; (3) identifying the threats to the assets from intentional (including malicious) and unintentional acts and environmental events; and (4) identifying the vulnerabilities of the identified assets.
- **Analyzes Threats and Vulnerabilities from Vendors, Business Partners, and Other Parties—**The entity's risk assessment process includes the analysis of potential threats and vulnerabilities arising from vendors providing goods and services, as well as threats and vulnerabilities arising from business partners, customers, and others with access to the entity's information systems.
- **Considers the Significance of the Risk—**The entity's consideration of the potential significance of the identified risks includes (1) determining the criticality of identified assets in meeting objectives; (2) assessing the impact of identified threats and vulnerabilities in meeting objectives; (3) assessing the likelihood of identified threats; and (4) determining the risk associated with assets based on asset criticality, threat impact, and likelihood.

Using RidgeBot to Comply:

- A pen-test-and-exploit scan helps verify the security posture of all internal systems, as well as any provider- or cloud-hosted external assets and services. Internal and external systems of subsidiaries, vendors, service providers, business partners or other parties can be assessed for risk by using a pen-test-and-exploit scan in the appropriate environment.
- Scan-and-exploitation reports can assist you in quickly compiling consistent and comparable summary and actionable documentation of vulnerabilities found, vulnerability ranking, successful exploits, and the mitigation and remedial steps taken. The ranking information can be used to determine the significance and likelihood of identified risks. The remedial/mitigation information can be used to help determine how best to respond to the identified risks, or to prepare management reports on risks and mitigation actions.
- Automated asset discovery can help you compile and maintain an inventory of all data processing assets and attack surfaces.
- An asset discovery scan iteratively discovers and documents changes in the presence of assets that should be included in a risk assessment or asset inventory.

Requirement CC3.3: COSO Principle 8—The entity considers the potential for fraud in assessing risks to the achievement of objectives.

- **Considers Various Types of Fraud—**The assessment of fraud considers fraudulent reporting, possible loss of assets, and corruption resulting from the various ways that fraud and misconduct can occur.
- **Assesses Opportunities—**The assessment of fraud risk considers opportunities for unauthorized acquisition, use, or disposal of assets, altering the entity's reporting records, or committing other inappropriate acts.
- **Considers the Risks Related to the Use of IT and Access to Information—**The assessment of fraud risks includes consideration of threats and vulnerabilities that arise specifically from the use of IT and access to information.

Using RidgeBot to Comply:

- Scan-and-exploitation reports can assist you in compiling consistent and comparable documentation of vulnerabilities found, vulnerability ranking, successful exploits, and the mitigation and remedial steps taken. This information can be used in an assessment of fraud opportunities and help take the appropriate mitigation actions.
- An automated asset discovery scan verifies on an ongoing basis that no new, unplanned devices are connected to the infrastructure that can introduce new vulnerabilities. For example, an attacker might set up a rogue wireless access point, or install an IoT device that allows remote access to the internal network.
- A pen-test-and-exploit scan can reveal weak points in physical security processes and systems (cameras, surveillance systems, logging systems, digitally-controlled door locks, audit trails) that could grant an attacker physical or electronic access to secure systems or areas, or allow tampering with surveillance cameras or stored logs or footage.

Requirement CC3.4: COSO Principle 9—The entity identifies and assesses changes that could significantly impact the system of internal control.

- **Assesses Changes in the External Environment—**The risk identification process considers changes to the regulatory, economic, and physical environment in which the entity operates.
- **Assesses Changes in the Business Model—**The entity considers the potential impacts of new business lines, dramatically altered compositions of existing business lines, acquired or divested business operations on the system of internal control, rapid growth, changing reliance on foreign geographies, and new technologies.
- **Assesses Changes in Systems and Technology—**The risk identification process considers changes arising from changes in the entity's systems and changes in the technology environment.
- **Assesses Changes in Vendor and Business Partner Relationships—**The risk identification process considers changes in vendor and business partner relationships.

Using RidgeBot to Comply:

- An automated asset discovery scan verifies on an ongoing basis that no new, unplanned devices are connected to the infrastructure that can introduce new vulnerabilities. For example, an attacker might set up a rogue wireless access point, or install an IoT device that allows remote access to the internal network.
- A pen-test-and-exploit scan helps verify the security posture of all internal systems, as well as any provider- or cloud-hosted external assets and services. Internal and external systems of subsidiaries, vendors, service providers, business partners or other parties can be assessed for risk by using a pen-test-and-exploit scan in the appropriate environment. This risk assessment can be done before a new provider/partner is engaged, or can be run on an ongoing basis to ensure that changed business processes or environments don't introduce new vulnerabilities.
- Automated pen-test-and-exploit capabilities can be run cost-effectively as frequently as necessary, rather than doing occasional one-time tests. This ensures peace of mind that your assets are continually locked-down and that new vulnerabilities are detected immediately after—or often before—they're introduced into your production environment. This can help protect against risks and fraud opportunities inadvertently introduced by changes in the operating environment or business model.

CC4: Monitoring of Controls

Requirement CC4.1: COSO Principle 16—The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.

- **Considers a Mix of Ongoing and Separate Evaluations—**Management includes a balance of ongoing and separate evaluations.
- **Considers Rate of Change—**Management considers the rate of change in business and business processes when selecting and developing ongoing and separate evaluations.

- **Establishes Baseline Understanding—**The design and current state of an internal control system
- **Considers Different Types of Ongoing and Separate Evaluations—**Management uses a variety of different types of ongoing and separate evaluations, including penetration testing, independent certification made against established specifications (for example, ISO certifications), and internal audit assessments.

Using RidgeBot to Comply:

- Automated asset discovery can help you compile and maintain on an ongoing basis (as frequently as necessary) an inventory of all data processing assets and attack surfaces. The scan documentation can provide a baseline of assets.
- An automated asset discovery scan verifies on an ongoing basis that no new, unplanned devices are connected to the infrastructure that can introduce vulnerabilities. For example, an attacker might set up a rogue wireless access point, or install an IoT device that allows remote access to the internal network.
- Automated pen-test-and-exploit capabilities can be run cost-effectively as frequently as necessary, instead of, or in addition to, doing occasional one-time tests. This ensures peace of mind that your assets are continually locked-down and that new vulnerabilities are detected immediately after—or often before—they're introduced into your production environment. This can help protect assets at all times in a fast-rate-of-change environment.

Requirement CC4.2: COSO Principle 17—The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.

- **Assesses Results—**Management and the board of directors, as appropriate, assess results of ongoing and separate evaluations.
- **Communicates Deficiencies—**Deficiencies are communicated to parties responsible for taking corrective action and to senior management and the board of directors, as appropriate.
- **Monitors Corrective Action—**Management tracks whether deficiencies are remedied on a timely basis.

Using RidgeBot to Comply:

- Scan-and-exploitation reports can assist you in quickly compiling consistent and comparable summary and actionable documentation of vulnerabilities found, vulnerability ranking, successful exploits, and the mitigation and remedial steps taken. This information can be used to take (or communicate) corrective action, and track what actions should, or have been, completed, and/or to prepare management reports of corrective action needed or already implemented.

CC5: Control Activities (Related to The Design and Implementation of Controls)

Requirement CC5.1: COSO Principle 10—The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.

- **Evaluates a Mix of Control Activity Types—**Control activities include a range and variety of controls and may include a balance of approaches to mitigate risks, considering both manual and automated controls, and preventive and detective controls.

  Using RidgeBot to Comply:

  - Asset discovery, scan-and-exploitation, pen-test, ransomware, as well as weak password scans can all be automated and cost-effectively run as frequently as necessary to compile documentation, assess risks, find and exploit vulnerabilities, as well as report on required mitigation actions.
  - RidgeBot's built-in AI/ML exploitation engine uses RidgeSecurity's industry leading knowledge base of attack techniques and intelligence, and ensures that your assets are always hardened with the most up to date vulnerability information. It is the best way to stay abreast of emerging technical vulnerabilities in a structured and systematic way.

Requirement CC5.2: COSO Principle 11—The entity also selects and develops general control activities over technology to support the achievement of objectives.

- **Establishes Relevant Technology Infrastructure Control Activities—**Management selects and develops control activities over the technology infrastructure, which are designed and implemented to help ensure the completeness, accuracy, and availability of technology processing.
- **Establishes Relevant Security Management Process Controls Activities—**Management selects and develops control activities that are designed and implemented to restrict technology access rights to authorized users commensurate with their job responsibilities and to protect the entity's assets from external threats.
- **Establishes Relevant Technology Acquisition, Development, and Maintenance Process Control Activities—**Management selects and develops control activities over the acquisition, development, and maintenance of technology and its infrastructure to achieve management's objectives.

  Using RidgeBot to Comply:

  - The asset discovery, scan-and-exploitation, pen-test, ransomware, and weak password scan capabilities can be a key part of a technology control activity and strategy to meet this objective.
  - Automated pen-test-and-exploit capabilities can be run cost-effectively as frequently as necessary, rather than doing occasional one-time tests. This ensures peace of mind that your assets are continually locked-down and that new vulnerabilities are detected immediately after—or often before—they're introduced into your production environment.

- RidgeBot's built-in AI/ML exploitation engine uses RidgeSecurity's industry leading knowledge base of attack techniques and intelligence, and ensures that your assets are always hardened with the most up to date vulnerability information. It is the best way to stay abreast of emerging technical vulnerabilities in a structured and systematic way.
- A pen-test-and-exploit scan can be run as a regular part of your policy/process to harden software patches, software upgrades, new devices, and any configuration or environment changes before pushing them live into the production environment.

Requirement CC5.3: COSO Principle 12—The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.

- **Establishes Policies and Procedures to Support Deployment of Management's Directives—** Management establishes control activities that are built into business processes and employees' day-to-day activities through policies establishing what is expected and relevant procedures specifying actions.
- **Takes Corrective Action—**Responsible personnel investigate and act on matters identified as a result of executing control activities.

Using RidgeBot to Comply:

- Same as for CC5.2.

Supplemental Criteria to COSO Principle 12

CC6: Logical and Physical Access Controls

Requirement CC6.1: The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.

- **Identifies and Manages the Inventory of Information Assets—**The entity identifies, inventories, classifies, and manages information assets.
- **Restricts Logical Access—**Logical access to information assets, including hardware, data (at-rest, during processing, or in transmission), software, administrative authorities, mobile devices, output, and offline system components is restricted through the use of access control software and rule sets.
- **Considers Network Segmentation—**Network segmentation permits unrelated portions of the entity's information system to be isolated from each other.
- **Restricts Access to Information Assets—**Combinations of data classification, separate data structures, port restrictions, access protocol restrictions, user identification, and digital certificates are used to establish access-control rules for information assets.
- **Manages Credentials for Infrastructure and Software—**New internal and external infrastructure and software are registered, authorized, and documented prior to being granted access credentials and implemented on the network or access point.

Using RidgeBot to Comply:

- Automated asset discovery can help you compile and maintain an inventory of all data processing assets and attack surfaces.
- An automated asset discovery scan verifies on an ongoing basis that no new, unplanned devices are connected to the infrastructure that can introduce vulnerabilities. For example, an attacker might set up a rogue wireless access point, or install an IoT device that allows remote access to the internal network.
- A weak password scan run against all assets documents and resolves login credential vulnerabilities.
- A pen-test-and-exploit scan can ensure that all systems or devices used to document events and activities are secure from weak credential vulnerabilities to prevent a hacker from access to erase or alter logs, video surveillance footage, or forensic audit trail information.
- RidgeBot's built-in AI/ML exploitation engine uses RidgeSecurity's industry leading knowledge base of attack techniques and intelligence, and ensures that your assets are always hardened with the most up to date vulnerability information. It is the best way to stay abreast of emerging technical vulnerabilities in a structured and systematic way.
- Automated pen-test-and-exploit capabilities can be run cost-effectively as frequently as necessary to ensure peace of mind that your assets are continually locked-down and that new vulnerabilities are detected immediately. This can help ensure that firewall rules and other network border controls across different network segments are correctly configured and function as intended.

Requirement CC6.2: Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity.

- **Controls Access Credentials to Protected Assets—**Information asset access credentials are created based on an authorization from the system's asset owner or authorized custodian.

Using RidgeBot to Comply:

- A weak password scan run against all assets documents and resolves login credential vulnerabilities.

Requirement CC6.4: The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.

Using RidgeBot to Comply:

- An automated asset discovery scan verifies on an ongoing basis that no new, unplanned devices are connected to the infrastructure that can introduce vulnerabilities. For example, an attacker might set up a rogue wireless access point, or install an IoT device that allows remote access to the internal network or a protected network segment.

- A pen-test-and-exploit scan can reveal weak points in physical security processes and systems (cameras, surveillance systems, logging systems, digitally-controlled door locks) that could grant an attacker physical or electronic access to secure systems or areas, or allow tampering with surveillance cameras or stored logs or footage.
- A pen-test-and-exploit scan can ensure that all systems or devices used to document events and activities are secure from weak credential vulnerabilities to prevent a hacker from access to erase or alter logs, video surveillance footage, or forensic audit trail information.

Requirement CC6.6: The entity implements logical access security measures to protect against threats from sources outside its system boundaries.

- **Restricts Access—**The types of activities that can occur through a communication channel (for example, FTP site, router port) are restricted.
- **Implements Boundary Protection Systems—**Boundary protection systems (for example, firewalls, demilitarized zones, and intrusion detection systems) are implemented to protect external access points from attempts and unauthorized access and are monitored to detect such attempts.

Using RidgeBot to Comply:

- Scan-and-exploitation reports can assist you in quickly compiling consistent and comparable summary and actionable documentation of vulnerabilities found, vulnerability ranking, successful exploits, and the mitigation and remedial steps taken. The vulnerabilities detected in this scan includes open ports and other back doors where hackers can access a system.
- Automated pen-test-and-exploit capabilities can be run cost-effectively as frequently as necessary to ensure peace of mind that your assets are continually locked-down and that new vulnerabilities are detected immediately. This can help ensure that firewall rules and other network border controls (such as IPS/IDS) across different network segments are correctly configured and function as intended.

Requirement CC6.8: The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.

- **Uses a Defined Change Control Process—**A management-defined change control process is used for the implementation of software.
- **Uses Antivirus and Anti-Malware Software—**Antivirus and anti-malware software is implemented and maintained to provide for the interception or detection and remediation of malware.
- **Scans Information Assets from Outside the Entity for Malware and Other Unauthorized Software—**Procedures are in place to scan information assets that have been transferred or returned to the entity's custody for malware and other unauthorized software and to remove any items detected prior to its implementation on the network.

Using RidgeBot to Comply:

- A pen-test-and-exploit scan can be run as a regular part of your policy/process to harden software patches, software upgrades, new devices, and any configuration changes before pushing them live into the production environment.

- A pen-test-and-exploit scan discovers, exploits and documents all vulnerabilities found. Run this scan as a regular part of your software development and software validation processes.
- A pen-test-and-exploit scan can ensure that all systems or devices used to document events and activities are secure from software/malware vulnerabilities where a hacker can get access to erase or alter logs, video surveillance footage, or forensic audit trail information.
- RidgeBot's built-in AI/ML exploitation engine uses RidgeSecurity's industry leading knowledge base of attack techniques and intelligence, and ensures that your assets are always hardened with the most up to date vulnerability information. It is the best way to stay abreast of emerging technical vulnerabilities in a structured and systematic way.

CC7: System Operations

Requirement CC7.1: To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.

- **Monitors Infrastructure and Software—**The entity monitors infrastructure and software for noncompliance with the standards, which could threaten the achievement of the entity's objectives.
- **Implements Change-Detection Mechanisms—**The IT system includes a change detection mechanism (for example, file integrity monitoring tools) to alert personnel to unauthorized modifications of critical system files, configuration files, or content files.
- **Detects Unknown or Unauthorized Components—**Procedures are in place to detect the introduction of unknown or unauthorized components.
- **Conducts Vulnerability Scans—**The entity conducts vulnerability scans designed to identify potential vulnerabilities or misconfigurations on a periodic basis and after any significant change in the environment and takes action to remediate identified deficiencies on a timely basis.

Using RidgeBot to Comply:

- An asset discovery scan iteratively discovers and documents changes in the presence of assets that should be included in a risk assessment or asset inventory.
- An automated asset discovery scan verifies on an ongoing basis that no new, unplanned devices are connected to the infrastructure that can introduce vulnerabilities. For example, an attacker might set up a rogue wireless access point, or install an IoT device that allows remote access to the internal network.
- Automated pen-test-and-exploit capabilities can be run cost-effectively as frequently as necessary, rather than doing occasional one-time tests. This ensures peace of mind that your assets are continually locked-down and that new vulnerabilities are detected immediately after—or often before—they're introduced into your production environment.

- RidgeBot's built-in AI/ML exploitation engine uses RidgeSecurity's industry leading knowledge base of attack techniques and intelligence, and ensures that your assets are always hardened with the most up to date vulnerability information. It is the best way to stay abreast of emerging technical vulnerabilities in a structured and systematic way.

Requirement CC7.2: The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.

- I**mplements Detection Policies, Procedures, and Tools—**Detection policies and procedures are defined and implemented and detection tools are implemented on infrastructure and software to identify anomalies in the operation or unusual activity on systems. Procedures may include (1) a defined governance process for security event detection and management that includes provision of resources; (2) use of intelligence sources to identify newly discovered threats and vulnerabilities; and (3) logging of unusual system activities.
- **Designs Detection Measures—**Detection measures are designed to identify anomalies that could result from actual or attempted (1) compromise of physical barriers; (2) unauthorized actions of authorized personnel; (3) use of compromised identification and authentication credentials; (4) unauthorized access from outside the system boundaries; (5) compromise of authorized external parties; and (6) implementation or connection of unauthorized hardware and software.
- **Implements Filters to Analyze Anomalies—**Management has implemented procedures to filter, summarize, and analyze anomalies to identify security events.

  Using RidgeBot to Comply:

  - RidgeBot's built-in AI/ML exploitation engine uses RidgeSecurity's industry leading knowledge base of attack techniques and intelligence, and ensures that your assets are always hardened with the most up to date vulnerability information. It is the best way to stay abreast of emerging technical vulnerabilities in a structured and systematic way.
  - Asset discovery, scan-and-exploitation, pen-test, ransomware, as well as weak password scans can all be automated and cost-effectively run as frequently as necessary to compile documentation, assess risks, find and exploit vulnerabilities, as well as report on required mitigation actions.
  - A pen-test-and-exploit scan can reveal weak points in physical security processes and systems (cameras, surveillance systems, logging systems, digitally-controlled door locks) that could grant an attacker physical or electronic access to secure systems or areas, or allow tampering with surveillance cameras or stored logs or footage.

Requirement CC7.3: The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.

- **Communicates and Reviews Detected Security Events—**Detected security events are communicated to and reviewed by the individuals responsible for the management of the security program and actions are taken, if necessary.
- **Develops and Implements Procedures to Analyze Security Incidents—**Procedures are in place to analyze security incidents and determine system impact.
- **Assesses the Impact on Personal Information—**Detected security events are evaluated to determine whether they could or did result in the unauthorized disclosure or use of personal information and whether there has been a failure to comply with applicable laws or regulations.
- **Determines Personal Information Used or Disclosed—**When an unauthorized use or disclosure of personal information has occurred, the affected information is identified.

Using RidgeBot to Comply:

- A forensic scan—perhaps after a security incident has occurred—can help determine where and how the breach was perpetrated. From there it can be extrapolated as to which systems and what data might have been exposed.
- Scan-and-exploitation reports—which include recommended solutions for each vulnerability—provide critical information for your security incident response/escalation or forensics team to ensure timely and effective handling of all situations.

Requirement CC7.4: The entity responds to identified security incidents by executing a defined incident-response program to understand, contain, remediate, and communicate security incidents, as appropriate.

- **Mitigates Ongoing Security Incidents—**Procedures are in place to mitigate the effects of ongoing security incidents.
- **Ends Threats Posed by Security Incidents—**Procedures are in place to end the threats posed by security incidents through closure of the vulnerability, removal of unauthorized access, and other remediation actions.
- **Obtains Understanding of Nature of Incident and Determines Containment Strategy—**An understanding of the nature (for example, the method by which the incident occurred and the affected system resources) and severity of the security incident is obtained to determine the appropriate containment strategy, including (1) a determination of the appropriate response time frame, and (2) the determination and execution of the containment approach.
- **Remediates Identified Vulnerabilities—**Identified vulnerabilities are remediated through the development and execution of remediation activities.

Using RidgeBot to Comply:

- Same as CC7.3.

Requirement CC7.5: CC7.5 The entity identifies, develops, and implements activities to recover from identified security incidents.

- **Determines Root Cause of the Event—**The root cause of the event is determined.
- **Implements Changes to Prevent and Detect Recurrences—**Additional architecture or changes to preventive and detective controls, or both, are implemented to prevent and detect recurrences on a timely basis.

Using RidgeBot to Comply:

- Same as CC7.3.

CC8: Change Management

Requirement CC8.1: The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.

- **Manages Changes Throughout the System Life Cycle—**A process for managing system changes throughout the life cycle of the system and its components (infrastructure, data, software, and procedures) is used to support system availability and processing integrity.
- **Designs and Develops Changes—**A process is in place to design and develop system changes.
- **Documents Changes—**A process is in place to document system changes to support ongoing maintenance of the system and to support system users in performing their responsibilities.
- **Tracks System Changes—**A process is in place to track system changes prior to implementation.
- **Configures Software—**A process is in place to select and implement the configuration parameters used to control the functionality of software.
- **Tests System Changes—**A process is in place to test system changes prior to implementation.
- **Deploys System Changes—**A process is in place to implement system changes.
- **Identifies and Evaluates System Changes—**Objectives affected by system changes are identified and the ability of the modified system to meet the objectives is evaluated throughout the system development life cycle.
- **Identifies Changes in Infrastructure, Data, Software, and Procedures Required to Remediate Incidents—**Changes in infrastructure, data, software, and procedures required to remediate incidents to continue to meet objectives are identified and the change process is initiated upon identification.

Using RidgeBot to Comply:

- A pen-test-and-exploit scan can be run as a regular part of your policy/process to harden software patches, software upgrades, new devices, and any configuration changes before pushing them live into the production environment.

- A pen-test-and-exploit scan discovers, exploits and documents all vulnerabilities found. Run this scan as a regular part of your software development and software validation processes.
- An asset discovery scan iteratively discovers and documents changes in the presence of assets that should be included in a risk assessment or asset inventory.
- An automated asset discovery scan verifies on an ongoing basis that no new, unplanned devices are connected to the infrastructure that can introduce vulnerabilities. For example, an attacker might set up a rogue wireless access point, or install an IoT device that allows remote access to the internal network.
- Automated pen-test-and-exploit capabilities can be run cost-effectively as frequently as necessary, rather than doing occasional one-time tests. This ensures peace of mind that your assets are continually locked-down and that new vulnerabilities are detected immediately after—or often before—they're introduced into your production environment. This can help ensure that firewall rules and other network border controls (such as IPS/IDS) across different network segments are correctly configured and function as intended.

CC9: Risk Mitigation

Requirement CC9.1: The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.

- **Considers Mitigation of Risks of Business Disruption—**Risk mitigation activities include the development of planned policies, procedures, communications, and alternative processing solutions to respond to, mitigate, and recover from security events that disrupt business operations. Those policies and procedures include monitoring processes, information, and communications to meet the entity's objectives during response, mitigation, and recovery efforts.

  Using RidgeBot to Comply:

  - Automated pen-test-and-exploit capabilities can be run cost-effectively as frequently as necessary, rather than doing occasional one-time tests. This ensures peace of mind that your assets are continually locked-down and that new vulnerabilities are detected immediately after—or often before—they're introduced into your production environment.
  - The recommended remedial steps in RidgeBot reports provide evidence that risks are being adequately found, measured, reviewed and treated.
  - RidgeBot's built-in AI/ML exploitation engine uses RidgeSecurity's industry leading knowledge base of attack techniques and intelligence, and ensures that your assets are always hardened with the most up to date vulnerability information. It is the best way to stay abreast of emerging technical vulnerabilities in a structured and systematic way.

Requirement CC9.2: The entity assesses and manages risks associated with vendors and business partners.

- **Assesses Vendor and Business Partner Risks—**The entity assesses, on a periodic basis, the risks that vendors and business partners (and those entities' vendors and business partners) represent to the achievement of the entity's objectives.
- **Assesses Vendor and Business Partner Performance—**The entity periodically assesses the performance of vendors and business partners.
- **Implements Procedures for Addressing Issues Identified During Vendor and Business Partner Assessments—**The entity implements procedures for addressing issues identified with vendor and business partner relationships.

Using RidgeBot to Comply:

- A pen-test-and-exploit scan helps verify the security posture of all internal systems, as well as any provider- or cloud-hosted assets and services. Internal and external systems of subsidiaries, vendors, service providers, business partners or other parties can be assessed for risk.

Supplemental Criteria Applicable to Specific Trust Categories

A Series: Additional Criteria for Availability

Requirement A1.3: The entity tests recovery plan procedures supporting system recovery to meet its objectives.

- **Implements Business Continuity Plan Testing—**Business continuity plan testing is performed on a periodic basis. The testing includes (1) development of testing scenarios based on threat likelihood and magnitude; (2) consideration of system components from across the entity that can impair the availability; (3) scenarios that consider the potential for the lack of availability of key personnel; and (4) revision of continuity plans and systems based on test results.

Using RidgeBot to Comply:

- A pen-test-and-exploit scan identifies, analyzes and evaluates all risks found. The scan reports provide a ranked list of vulnerabilities found based on each vulnerability's likelihood to be exploited, including those that were successfully exploited during the test. The reports also provide an evaluation with granular steps to remediate each vulnerability.
- Automated pen-test-and-exploit capabilities can be run cost-effectively as frequently as necessary. This ensures peace of mind that your assets are continually locked-down and that new vulnerabilities are detected immediately after—or often before—they're introduced into your production environment.

Ridge Security Technology Inc.

www.ridgesecurity.ai