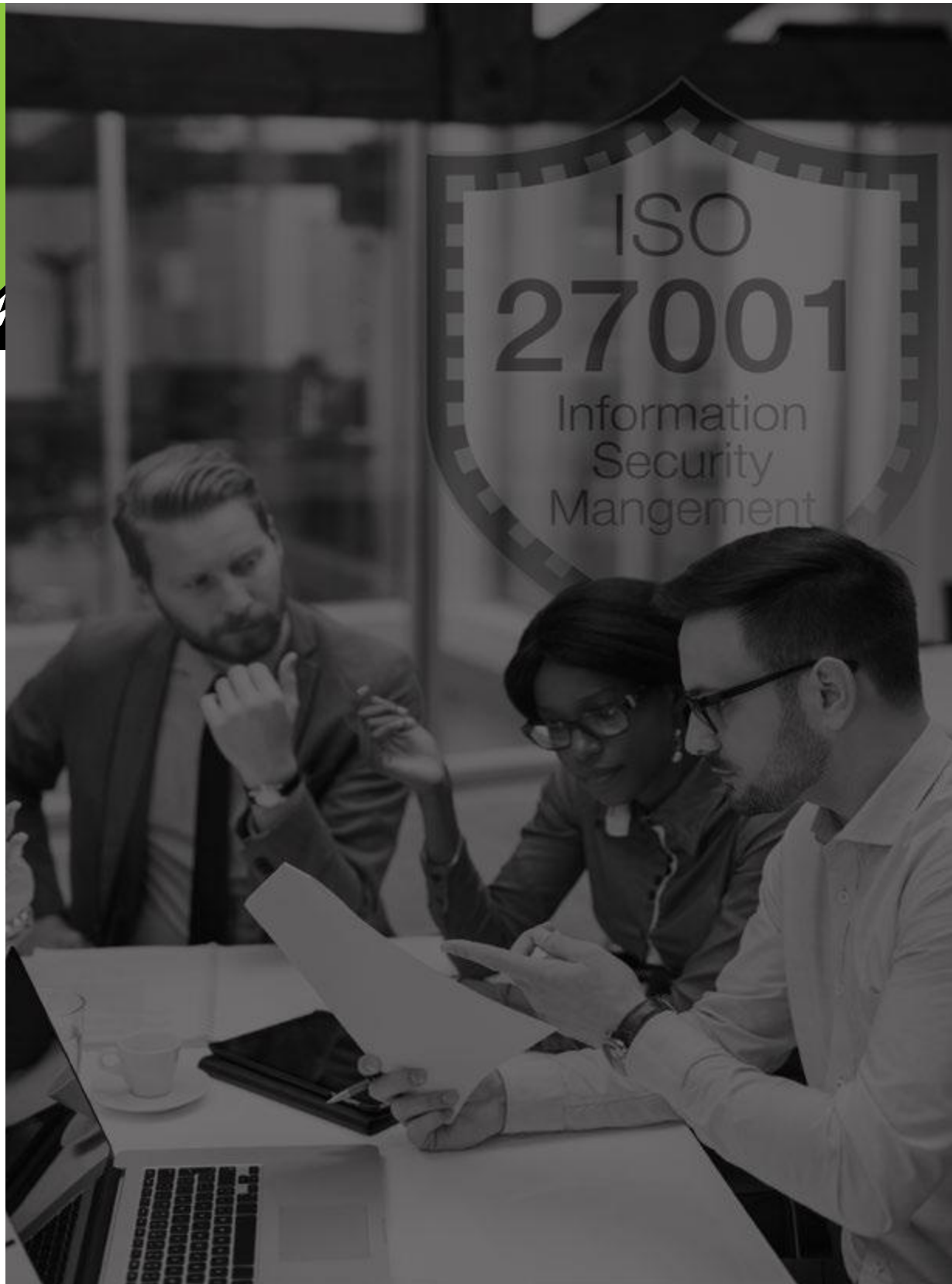
ISO27001 Compliance

Using RidgeBot Security Validation



Overview

Continuous Validation with Automated Attacks; Detailed Steps to Resolve and Lock Down Vulnerabilities

The digital transformation of worldwide economic, business and government operations has seen rapid growth in security defense technologies such as encryption, Next-gen firewalls, filtering methods, malware screening, multi-factor authentication, and surveillance.

Despite advances in these defensive technologies, networks, hosts and applications are continuously under attack by increasingly creative and sophisticated methods. Breaches are continually growing in number, size, and the damage inflicted by the attackers.

Industry Trends

Traditional defensive security mechanisms have failed to adequately protect networks, data centers, hosts, and applications from infiltration, attacks, and breaches. The effectiveness of traditional defensive security mechanisms pivots mainly on the concept of border security—while increasingly, industry trends in SaaS, IaaS, cloud computing, IoT, virtualization, and mobility have blurred or erased borders in networks and computer processing and storage systems.

Security posture is also distressed because, while attacks have escalated in number, subtlety, and precision, IT resources for security measures, audits, and protective activities, have tightened.

Penetration Testing

Rapidly increasing threat incidence and sophistication have made it imperative to harden security posture with active, offensive methods. Not supplanting, but in addition to traditional defensive measures—such as penetration testing that probe for vulnerabilities, addressing them before they are exploited.

Breach Prevention Traditional Defense 2002	Post Breach Detection 2012	Pre-Breach Offensive Defense 2020

Penetration testing is an expensive, resource-intensive, disruptive, and often manual process. Testing is often executed periodically (for example, annually) when there is an upcoming audit or other collateral need to gain or reaffirm compliance with one of the many worldwide standards and regulations regarding financial, personal, health, or sensitive information. Your environment is vulnerable during the often-lengthy periods in between audits doing scheduled pen-testing validation.

Automated Continuous Validation with RidgeBot

RidgeBot is an intelligent robot that provides low-cost continuous, automated security validation services to harden your security posture ongoing and deliver always-on compliance monitoring. It has built-in collective real-time knowledge of the latest threats, vulnerabilities, exploits, and state-of-the-art AI/ML-assisted hacking methods and techniques. It scales as needed and runs as a VM, on an appliance, or as SaaS.

RidgeBot automates penetration testing, making it an ongoing high-use tool integral to your security policy and procedures instead of an expensive one-time test exercise. RidgeBot is your personal robot assistant that details how and where hackers can successfully compromise your assets. It recommends step-by-step how-to-build and maintain your assets in a secure, protected manner.

RidgeBot does much more than a pen-test: it auto-discovers assets and then proceeds to probe them continuously, iteratively, fully automated, at scale, and exploits the vulnerabilities found. In its report, it alerts you to the ranked short-list of dangerous, successfully exploited vulnerabilities as well as a list of lower-priority non-exploited vulnerabilities. Your network is always locked down, always patch-up to date, always ready for audit, and always ready to submit proof of security posture—all at minimal cost and human intervention.

RidgeBot provides the following key capabilities:

- **Discovery:** Automatically crawls through your environment to identify and document types of assets (including networks, hosts, applications, plug-ins, images, IoT devices, and mobile devices) and the attack surfaces of those assets.
- **Scanning:** Assets and attack surfaces are mined for vulnerabilities by leveraging RidgeSecurity's leading-edge Threat Intelligence Platform—a collective vulnerability knowledge database—that includes more than 2-billion pieces of security intelligence data, 100 million attack libraries, and 150K exploit libraries.
- **Exploit:** AI/ML-assisted attack techniques/modes automatically exploit vulnerabilities found. Findings are documented along with remediation recommendations in accurate, reliable, and usable reports. AI/ML algorithms draw on an expert knowledge base guides RidgeBot in attack-path-finding and path-selection. They launch iterative attacks based on learning along the path and achieve much broader test coverage and more in-depth inspection than traditional pen-test methods.
- **Post-exploit Risk Prioritization:** RidgeBot visualizes the kill-chain and quantifies risks based on multiple factors, giving organizations detailed and specific rankings of the most dangerous vulnerabilities. Focusing on specific exploitable vulnerabilities (a single-digit percentage), RidgeBot's analytics drastically reduce the manual work required to rank and remediate vulnerabilities.

ISO 27001 Overview

The ISO 27000 family of standards offers a set of specifications, codes of conduct, and best-practice guidelines for organizations to ensure strong information security management. ISO/IEC 27001:2013, superseding ISO/IEC 27001:2005, specifies the best practices to implement and maintain an Information Security Management system (ISMS): a systematic approach to securely managing data and includes people, processes, and technology.

ISO 27001 is a technology-neutral security management standard that prescribes the attributes of an effective ISMS. ISO 27002—an essential supplementary piece to the standard—details the best practices to implement an effective ISMS.

Type of Requirement: ISO 27001 is an information security industry standard. It is not a legal requirement, but certification is often a prerequisite for contracts or conducting business with government entities, government-funded entities, or large corporate clients.

Geographic Applicability: Worldwide.

Ownership: Published by the International Organization for Standardization (ISO) (an international management and business continuity standards organization with representatives from 165 national standards organizations) and the International Electrotechnical Commission (IEC) (an international standards organization for electrical, electronic and related technologies).

Compliance Verification and Enforcement: Companies achieve certification with ISO 27001 by preparing for compliance. Then companies must schedule an audit with a national accreditation body that is a member of the International Accreditation Forum (IAF). The ANSI National Accreditation Board (ANAB) is in the US, or the United Kingdom Accreditation Service (UKAS) is in the UK. Certified companies participate annually in an external review process and must recertify every three years to maintain compliance.

More information:

- ISO 27001: https://www.iso27001security.com/html/27001.html
- ISO 27002: https://www.iso27001security.com/html/27002.html
- United Kingdom: https://www.itgovernance.co.uk/iso27001
- United States: https://www.itgovernanceusa.com/iso27001

ISO 27001 Certification and Compliance

ISO 27001:2013 focuses on setting objectives, assessing performance, and defining metrics for measuring effectiveness. Objectives or controls are organized by 14 categories or domains, with specific details given in Annex A of the standard. Organizations are not required to implement all ISO 27001's controls—they represent a list of possibilities to consider based on a company's particular business and environment.

1. Annex A.5: Information security policies
2. Annex A.6: Organization of information security
3. Annex A.7: Human resource security
4. Annex A.8: Asset management
5. Annex A.9: Access control
6. Annex A.10: Cryptography
7. Annex A.11: Physical and environmental security
8. Annex A.12: Operations security
9. Annex A.13: Communications security
10. Annex A.14: System acquisition, development, and maintenance
11. Annex A.15: Supplier relationships
12. Annex A.16: Information security incident management
13. Annex A.17: Information security aspects of business continuity management
14. Annex A.18: Compliance

Implementation of an ISO 27001-compliant ISMS is a multi-step process, broadly following this outline:

- **Governance**: This requires a demonstrated top management commitment to an ISMS.
- **Risk Assessment**: Requires exact understanding of the risks to information security faced by the organization.
- **Documentation**: Sets out how the ISMS works.
- **Continual improvement**: Once the ISMS is implemented, performance and effectiveness must be measured, deviations must be identified, and corrective action must be taken.

Several supplementary standards contribute to the interpretation and implementation of ISO 27001.

- **ISO 27002** recommends best practices for effective implementation of the ISO 27001 specifications.
- **ISO 27005** guides information security risk management.
- **ISO 27017** focuses on how the ISO 27001 controls apply to information stored in the cloud.
- **ISO 27018** offers guidance on protecting sensitive information in the cloud.
- **ISO 27701** defines additional ISMS requirements to cover data privacy, recognizing that information security is essential to effective privacy management. It was created in response to the General Data Protection Regulation (GDPR) to detail how ISO 27001 controls intersect with data privacy.

OVERVIEW

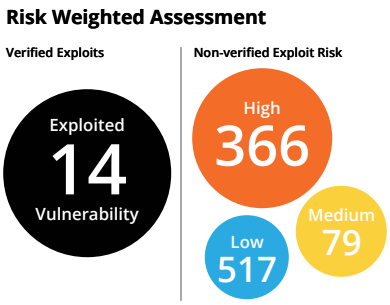
How RidgeBot Can Help

In a general sense, RidgeBot helps find non-compliant issues in your assets and guides how and immediately resolves any exposures. Moreover, RidgeBot continually maintains a security posture that is always in compliance with ISO 27001 and other standards and regulations.

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 and scans 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 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 shortlist 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 Release Testing

- Use RidgeBot during software development to ensure that dangerous coding practices introducing vulnerabilities never ship in new software releases.
- 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. 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.
- RidgeBot reports submit evidence of vulnerabilities probed, remediated, and resolved.

Security Incident Response

- Scan reports containing recommended solutions for each vulnerability found and provide critical information to your security incident response/escalation team.
- Risk ranking of vulnerabilities feeds 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 and step-by-step guidance on how to resolve the entry point vulnerability.

RidgeBot includes several template scans and the flexibility to completely customize your 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.
- **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.
- Struts 2 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

ISO 27001 Implementation and Certification

RidgeBot can help in many ways with specific implementation stages, implementation challenges, and ongoing maintenance of ISO 27001 Certification, Audit, and Review.

- **Asset Identification**: ISO 27001 requires that several classes of assets be inventoried, including digital records, IT assets, business applications, and mobile devices.

  RidgeBot's automated asset discovery can help inventory all assets while preparing for an ISO 27001 [re]certification. It can additionally verify that no new, unplanned devices are connected to the infrastructure that introduces vulnerabilities on an ongoing basis. 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.

- **Risk Assessment**: ISO 27001 requires you to conduct regular risk assessments. The standard stipulates that your risk assessment process must produce "consistent, valid, and comparable results"—the stages of risk assessment involve Identifying, Analyzing, and Evaluating risks. Furthermore, ISO 27001 states that once all risks are identified, each risk must be individually assessed as to the likelihood of exploitation, the harm that could occur. A rank or score must be assigned to each vulnerability by the risk criteria.

  RidgeBot's pen-test capabilities identify, analyze, and evaluate all risks found. Additionally, it exploits risks found and provides remedial steps. 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. The RidgeBot scan reports provide a vehicle to comply with the "consistent, valid, and comparable results" requirement of ISO 27001.

- **Risk Treatment Plan**: ISO 27001 states that your Risk Treatment Plan must determine the "methods for monitoring, measurement, analysis, and evaluation […] to ensure valid results". The effectiveness of about half of the controls listed in ISO 27001 Annex A can only be sufficiently evaluated using penetration testing.

  RidgeBot's fully automated pen-test capabilities can be run cost-effectively as frequently as necessary, rather than hiring a consulting firm to do a one-time test. Peace of mind is ensured that your assets are continually locked-down. New vulnerabilities are detected immediately after—or often before—introduced into your production environment. Your business environment is always compliant with ISO 27001, not just when you prepare for an audit, a review, or recertification.

- **Documentation**: An arduous aspect of an ISO 27001 ISMS implementation is developing the Standard's documentation explicitly required.

  RidgeBot's scan reports (results from the same scan repeat on a fixed schedule) can assist in compiling "consistent, valid and comparable" documentation of vulnerabilities found, vulnerability ranking, successful exploits, and mitigation and remedial steps are taken.

- **Continual Improvement through Measurement, Monitoring, and Review**: This aspect of ISO 27001 requires that your ISMS is continually analyzed and reviewed for performance, effectiveness, compliance, and identifying process improvements.

  RidgeBot's scan reports—run continually or periodically—can assist in providing reports and recommended remedial steps providing the evidence the Standard requires to show that risks are being adequately found, measured, reviewed, and treated.

  A penetration testing service that regularly tests the ISO 27001 controls and, when necessary, test changes to IT and security infrastructure is a fundamental part of any continuous improvement process.

  RidgeBot provides this service at a very cost-effective price-point. It is fully automated. Scans can be scheduled as often as needed (fulfilling the "internal audit" ISO 27001 requirement). RidgeBot scan output provides consistent and comparable reports, including quantitative measurements (vulnerability categories and rankings) that demonstrate your ISMS's effectiveness.

ISO 27001 Annex A Controls

ISO 27001 Annex A provides a brief overview of controls and domains. ISO 27002 provides more detailed information to help with implementation.

Each of the 14 ISO 27001:2013 domains (and the controls within them) is summarized below. Many controls pertain to human management practices and procedures. Several others concern IT assets and infrastructure. These annotate RidgeBot's penetration testing, vulnerability ranking, AI/ML-assisted vulnerability exploitation, and reported remediation steps to help implement and meet ISO 27001 control.

Annex A.5 Information security policies

Ensure that policies are written and reviewed in line with the organization's information security practices.

- 5.1 Management direction for information security: Define a set of policies to clarify management's direction of, and support for, information security.

Annex A.6 Organization of information security

Assignment of responsibilities for specific tasks.

- 6.1 Internal organization: Layout roles and responsibilities for information security and allocate them to individuals.
- 6.2 Mobile devices and teleworking: Establish security policies and controls for mobile devices and teleworking. Ensure that anyone who works from home or on-the-go follows appropriate practices.

Annex A.7 Human resource security

Ensure that prospective, current, and past employees and contractors understand their information security responsibilities.

- 7.1 Before employment: Information security responsibilities should be taken into account when recruiting permanent employees, contractors, and temporary staff and included in contracts.
- 7.2 During employment: Ensure that employees and contractors are aware of, and motivated to comply with, information security obligations, including a disciplinary process.
- 7.3 Termination and change of employment: Security aspects of a person's departure or role-change must be managed, such as returning corporate information and equipment and updating access rights.

Annex A.8 Asset management

Identify information assets and define appropriate protection responsibilities.

- 8.1 Responsibility for assets: Inventory all information assets and identify owners accountable for their security.
- 8.2 Information classification: Classify and label information according to the security protection needed and handle it appropriately.
- 8.3 Media handling: Information storage media should be managed, controlled, moved, and disposed of without compromising information content.

USING RIDGEBOT TO COMPLY

- Run an asset discovery scan to identify and document all assets and attack surfaces. Iteratively running this scan discovers and documents any changes in the presence of assets that should be included in the inventory.

Annex A.9 Access control

Ensure that employees can only view information relevant to their job.

- 9.1 Business requirements of access control: Control access to information assets documented in control policy and procedures. Restrict network access and connections.
- 9.2 User access management: Control user access rights from initial user registration to removing rights when no longer required. Conduct regular reviews and updates of access rights.
- 9.3 User responsibilities: Users must be aware of their responsibilities towards maintaining effective access controls, such as strong passwords and confidentiality.
- 9.4 System and application access control: Restrict information access in line with the access control policy, such as secure login and password management.

USING RIDGEBOT TO COMPLY

- Run a weak password scan against all assets to document and resolve login credential vulnerabilities.

Annex A.10 Cryptography

Data encryption and the management of sensitive information.

- 10.1 Cryptographic controls: Establish and maintain a policy on the use of encryption, cryptographic authentication, and integrity controls such as digital signatures, message authentication codes, and cryptographic key management.

USING RIDGEBOT TO COMPLY

- Ensure that a scan specifically targeting encryption-related vulnerabilities is part of the policy for cryptographic controls.

Annex A.11 Physical and environmental security

Prevent unauthorized physical access, damage, or interference to the organization's premises, equipment, or sensitive information.

- 11.1 Secure areas: Define physical perimeters and barriers with physical entry controls, protect the premises, offices, rooms, delivery/loading areas, etc. against unauthorized access.
- 11.2 Equipment: Secure and maintain information and computer equipment plus supporting utilities (such as power and air conditioning) and cabling.

USING RIDGEBOT TO COMPLY

- Run an access scan to ensure that all systems or devices used to control, log or surveil physical entry to premises are secure from weak credentials or other software/malware vulnerabilities. Hackers can allow physical access (instead of denying it) or erase or alter logs, video surveillance, or audit trail information.
- Penetration testing can reveal weak points in physical security processes that could grant an attacker access to secure systems or areas.

Annex A.12 Operations security

Ensure that information processing facilities are secure.

- 12.1 Operational procedures and responsibilities: Document IT operating responsibilities and procedures; control changes to IT facilities and systems; manage capacity and performance; separate development, test, and operational systems.
- 12.2 Protection from malware: Malware controls are required, including user awareness.
- 12.3 Backup: Make and retain appropriate backups in accordance with backup policy.
- 12.4 Logging and monitoring: Protect and log system user and administrator/operator activities, exceptions, faults, and information security events. Synchronize clocks.
- 12.5 Control of operational software: Control software installation on operational systems.
- 12.6 Technical vulnerability management: Patch vulnerabilities, and ensure rules are in place to govern user software installation.
- 12.7 Information systems audit considerations: Plan and control IT audits to minimize adverse effects on production systems or inappropriate data access.

USING RIDGEBOT TO COMPLY

- Run a pen-test scan to ensure that all assets are secure from weak credentials or other software/malware vulnerabilities where hackers can gain unauthorized access.
- Run a scan to ensure that all systems or devices used to log events and activities are secure from weak credentials or other software/malware vulnerabilities. Areas where hackers can get access to erase or alter logs, video surveillance, or audit trail information.
- Run full scans, with exploitation turned on for the vulnerabilities found, as a regular part of your policy/process for hardening software patches, software upgrades, new devices, and any configuration changes before pushing them live into the production environment.
- The scan reports (containing listed vulnerabilities detected, successful exploits, and remedial steps) address the Standard's requirement to detect emerging technical vulnerabilities in a structured and systematic way.

Annex A.13 Communications security

Protect the information in networks.

- 13.1 Network security management: Ensure security of networks and network services, for example, by segregation.
- 13.2 Information transfer: Ensure policies, procedures, and agreements (such as non-disclosure agreements) concerning information transfer to/from third parties, including electronic messaging, are in place.

USING RIDGEBOT TO COMPLY

- Run a pen-test scan to ensure that all assets that participate in information transfer and electronic messaging systems are secure from weak credentials or other software/malware vulnerabilities where hackers can gain unauthorized access.

Annex A.14 System acquisition, development, and maintenance

Ensure information security remains a central part of processes across the entire lifecycle for internal systems as well as services provided over public networks.

- 14.1 Security requirements of information systems: Security control requirements should be analyzed and specified, including web applications and transactions.
- 14.2 Security in development and support processes: Define as policy the rules governing secure software/systems development. You can control changes to both applications and operating systems. Secure the development environment, as well as outsourced development—test system security against security-defined acceptance criteria.
- 14.3 Test data: Test data should be carefully selected/generated and controlled.

Using RidgeBot to Comply

- Run a pen-test scan against internal systems as well as any provider- or cloud-hosted assets and services.
- Run a full scan with exploitation turned on for the vulnerabilities found as a regular part of the software development, software validation and change control processes and procedures.
- Run an access scan to ensure appropriate access controls exist to separate your software development/test environments from production environments.
- Run full scans, with exploitation turned on for the vulnerabilities found, as a regular part of your policy and process for hardening new software during the software development process.
- Run continuous scans, with exploitation turned on for the vulnerabilities found. Continually scan parts of your software or website development process, as well as the testing process to harden software patches, software upgrades, new devices, and any configuration changes before pushing them into your production environment.

Annex A.15 Supplier relationships

Contractual agreements between organizations and third parties.

- 15.1 Information security in supplier relationships: Define policies, procedures, awareness, etc. to protect information accessible to outsourcers and external suppliers throughout the supply chain, agreed within the contracts or agreements.
- 5.2 Supplier service delivery management: Monitor service delivery by external suppliers and review/audit against contracts/agreements. Control service changes.

Annex A.16 Information security incident management

Manage and report security incidents.

- 16.1 Management of information security incidents and improvements: Define responsibilities and procedures to manage (report, assess, respond to and learn from) information security events, incidents, and weaknesses consistently and effectively, and collect forensic evidence.

USING RIDGEBOT TO COMPLY

- The pen-test scan 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.
- A forensic scan (after a security incident has occurred) can also help determine where and how a breach is perpetrated.

Annex A.17 Information security aspects of business continuity management

Create an effective system to manage business disruptions.

- 17.1 Information security continuity: Plan, implement, and review information security continuity as an integral part of the business continuity management system.
- 17.2 Redundancies: Ensure IT facilities have sufficient redundancy to satisfy availability requirements.

Annex A.18 Compliance

Identify relevant laws and regulations. Understand legal and contractual requirements to mitigate the risk of non-compliance and penalties.

- 18.1 Compliance with legal and contractual requirements: Identify and document obligations to external authorities and other third parties relevant to information security, including intellectual property, [business] records, privacy/personally identifiable information, and cryptography.
- 18.2 Information security reviews: Independently review (audit) information security arrangements and report to management. Managers must review employees' and systems' compliance with security policies, procedures and initiate corrective action.

USING RIDGEBOT TO COMPLY

- Run full scans, with exploitation turned on for the vulnerabilities found, as a regular part of your policy and process to review that your security controls are effective against the latest threats.
- RidgeBot's built-in AI/ML exploitation engine uses RidgeSecurity's industry-leading knowledge base of attack techniques and ensures that your assets are always hardened with the most up to date vulnerability intelligence.
- The scan reports—containing listed vulnerabilities detected, successful exploits, and remedial steps—provide documentation for an independent or management review of your security controls and their effectiveness. They also outline steps for corrective action.

Company Profile

Ridge Security delivers ethical, efficient and affordable pen testing solutions to enterprises, small and large. We ensure our customers stay compliant, alerted and secure at all times in the cyber world. The management team has many years of networking and security experience. Ridge Security is located in the heart of Silicon Valley and is expanding into other areas including Latin America, Asia and Europe.

RidgeBot, a robotic penetration testing system, fully automates the testing process by coupling ethical hacking techniques to decision-making algorithms. RidgeBots locate, exploit and document business risks and vulnerabilities discovered during the testing process, highlighting the potential impact or damage.

Ridge Security Technology Inc.
www.ridgesecurity.ai