How Wazuh Helps You Meet ISO 27001 Requirements: A Practical Guide for SMBs.

Organizations racing to meet the ISO 27001:2022 transition deadline face a common challenge: finding security tools that demonstrate compliance without breaking the budget. WAZUH, the open-source XDR and SIEM platform trusted by thousands of enterprises worldwide, offers a compelling solution by directly supporting the technical controls that auditors want to see. While WAZUH doesn't ship with a dedicated ISO 27001 dashboard like it does for PCI DSS or HIPAA, its comprehensive security capabilities map remarkably well to the standard's Annex A requirements—particularly the **34 technological controls** that demand evidence of logging, monitoring, and threat detection.

The 2022 revision of ISO 27001 reorganized controls from 14 domains into just four streamlined themes and introduced **11 new controls** specifically addressing modern threats like cloud security and threat intelligence. This restructuring places greater emphasis on continuous monitoring and evidence-based security—precisely where WAZUH excels. For security teams building an Information Security Management System (ISMS), WAZUH provides the technical foundation to satisfy dozens of control requirements through a single, unified platform.

Understanding WAZUH's architecture for compliance

WAZUH operates as a complete security monitoring ecosystem built on four interconnected components that work together to collect, analyze, store, and visualize security data across your entire infrastructure.

The **WAZUH agent** deploys directly on endpoints—Windows, Linux, macOS, and even legacy systems like Solaris and AIX—where it runs specialized modules for log collection, file integrity monitoring, vulnerability scanning, and configuration assessment. These lightweight agents communicate with the central **WAZUH server** through AES-256 encrypted channels, sending security telemetry for analysis against thousands of detection rules mapped to the MITRE ATT&CK framework.

The server's analysis engine processes incoming data through decoders and rules, generating alerts that flow to the **WAZUH indexer** (built on OpenSearch) for storage and fast retrieval. Security teams interact with everything through the **WAZUH dashboard**, which provides out-of-the-box visualizations for threat hunting, vulnerability management, and compliance reporting. This architecture enables organizations to monitor hundreds or thousands of endpoints while maintaining the centralized audit trail that ISO 27001 auditors require.

What makes WAZUH particularly valuable for compliance is its extensibility. Every detection rule can be tagged with compliance identifiers, and custom rules inherit this capability. Organizations can tag their rules with iso_27001_A.8.15 or similar identifiers to create filtered views showing exactly which security events relate to specific controls.

Meeting logging and monitoring requirements with WAZUH

Control **A.8.15 (Logging)** and **A.8.16 (Monitoring activities)** form the backbone of ISO 27001:2022's technical requirements. The standard mandates that organizations produce, store, protect, and analyze logs recording activities, exceptions, faults, and security events. WAZUH's log data collection module addresses these requirements comprehensively.

The agent's log collector reads flat log files, Windows Event logs with XPath filtering support, and system journals. It captures exactly what A.8.15 specifies: successful and rejected access attempts, configuration changes, privileged operations, file access patterns, and the activation or deactivation of security systems. Each log entry includes the user ID, timestamp, device identity, network address, and event details that auditors need to verify compliance.

For monitoring activities, WAZUH's real-time analysis engine continuously evaluates incoming data against detection rules designed to identify anomalous behavior. The platform monitors inbound and outbound network traffic, tracks access to protected resources, and watches for behavioral indicators like processes abruptly terminating, connections to known malicious IP addresses, or patterns matching DDoS attacks and intrusion attempts. When the analysis engine detects a potential security incident, it generates alerts that trigger the incident management workflows required by controls **A.5.24 through A.5.28**.

Vulnerability management that satisfies A.8.8

Control **A.8.8 (Management of technical vulnerabilities)** requires organizations to obtain information about technical vulnerabilities, evaluate their exposure, and take appropriate measures. This control links directly to asset inventory requirements and demands a systematic approach to identifying and remediating security weaknesses.

WAZUH's vulnerability detection module implements this control through a two-stage process. First, the **Syscollector module** on each agent inventories installed software, capturing package names, versions, and deployment details across the entire endpoint fleet. This data feeds directly into compliance with control **A.5.9 (Inventory of information and other associated assets)**.

The server's vulnerability detector then correlates this inventory against multiple authoritative sources: the National Vulnerability Database (NVD), CISA advisories, and vendor-specific feeds from Canonical, Debian, Red Hat, Amazon Linux, Arch Linux, and Microsoft. When matches occur, WAZUH generates alerts containing CVE identifiers, severity ratings, CVSS scores, and remediation guidance. Security teams can prioritize patching based on actual risk exposure rather than theoretical vulnerability counts.

The platform performs three scan types to maintain current vulnerability awareness: baseline scans when agents first register, full scans when the CVE database updates, and partial scans whenever new software appears on endpoints. This continuous assessment model aligns with ISO 27001's emphasis on ongoing security evaluation rather than point-in-time audits. Organizations can export vulnerability reports as audit evidence demonstrating their systematic approach to technical vulnerability management.

Tracking configuration changes through file integrity monitoring

ISO 27001:2022 introduced **A.8.9 (Configuration management)** as a new control, recognizing that unauthorized configuration changes represent a significant attack vector. The control requires organizations to establish, document, implement, monitor, and review configurations for hardware, software, services, and networks.

WAZUH's File Integrity Monitoring module directly addresses this requirement by tracking changes to critical system files, configurations, and Windows Registry entries. The module stores cryptographic checksums (MD5, SHA-1, and SHA-256) along with file attributes including permissions, ownership, size, and modification timestamps. When changes occur, WAZUH compares current values against the stored baseline and generates alerts for any discrepancies.

The "who-data" audit capability adds crucial context by capturing which user, program, and process made each change—essential information for incident investigation and demonstrating accountability. Organizations can configure FIM to monitor specific paths using wildcards, run scheduled scans at defined intervals, or enable real-time monitoring for the most sensitive files.

This same capability supports control **A.8.10 (Information deletion)** by alerting when files are removed, and control **A.8.32 (Change management)** by integrating with ticketing systems like Jira and

ServiceNow. When WAZUH detects an unauthorized change, automated workflows can create tickets for review, establishing the documented change management process auditors expect to see.

Security Configuration Assessment closes compliance gaps

Beyond detecting changes, organizations must prove their systems are configured securely in the first place. WAZUH's Security Configuration Assessment module addresses this by continuously scanning endpoints against established security benchmarks.

The platform ships with policies based on **CIS Benchmarks** covering Windows, Ubuntu, RHEL, and other common operating systems. These policies check for security misconfigurations like overly permissive file permissions, disabled security features, exposed services, and weak authentication settings. Each check includes the rationale for the requirement, steps to remediate failures, and mappings to relevant compliance frameworks.

Organizations can create custom SCA policies in YAML format to check for organization-specific requirements. The resulting reports show passed and failed checks with trend data over time, providing evidence that configuration management controls are not just implemented but continuously enforced.

Incident response capabilities for controls A.5.24 through A.5.28

ISO 27001:2022 dedicates five controls to incident management, covering planning, assessment, response, learning, and evidence collection. WAZUH's Active Response module and Cases feature work together to support this entire incident lifecycle.

When detection rules trigger alerts meeting specified criteria—rule IDs, severity levels, or threat categories—Active Response can automatically execute defensive actions. Default scripts block IP addresses at the firewall, add entries to hosts.deny files, disable compromised user accounts, or restart services. Organizations can write custom scripts in Python, Bash, or PowerShell for incident types specific to their environment.

The **Cases feature** bundles related alerts, investigation notes, and tickets into unified incident records. Security analysts can document their assessment decisions, track containment actions, and preserve the investigation timeline that control A.5.28 requires for evidence collection. Integration with external platforms extends these capabilities into established ITSM workflows.

For forensic investigation, WAZUH enables remote command execution and device queries for live data collection—capturing running processes, network connections, or registry contents without physical access to compromised systems. This capability proves invaluable when responding to incidents across distributed environments while maintaining the evidence chain auditors need to see.

Building your ISO 27001 compliance dashboard

While WAZUH provides pre-built compliance dashboards for PCI DSS, HIPAA, NIST 800-53, and GDPR, ISO 27001 requires custom configuration. However, the platform's flexibility makes building an ISO 27001 view straightforward.

Security teams can tag detection rules with ISO 27001 control identifiers using the standard group syntax: <group>iso_27001_A.8.15, iso_27001_A.8.16</group>. Dashboard queries can then filter alerts by these tags, creating focused views showing security events relevant to specific controls. Organizations commonly create visualizations grouping alerts by:

- **A.8.15 and A.8.16**: All logging and monitoring events

- **A.8.8**: Vulnerability detection alerts
- **A.8.9**: Configuration drift and FIM alerts
- **A.8.7**: Malware detection events
- **A.5.24-A.5.28**: Incident-related alerts requiring response

The platform's export capabilities let teams generate reports for audit evidence, saved searches for recurring analysis, and incident packages documenting specific security events. Combined with the Cases feature for incident documentation, these tools provide the audit trail demonstrating that controls are not just implemented but actively operating.

A practical approach leverages WAZUH's existing NIST 800-53 mappings, which share significant overlap with ISO 27001. Organizations can use established crosswalk documents to translate NIST control evidence into ISO 27001 compliance documentation, accelerating the certification process.

Practical implementation roadmap

Organizations beginning their ISO 27001:2022 compliance journey with WAZUH should focus on establishing foundational capabilities before expanding coverage.

Start by deploying agents across critical systems identified in your asset inventory. Configure log collection to capture authentication events, privilege escalation, and system changes—the core evidence for A.8.15 compliance. Enable file integrity monitoring on configuration files, system binaries, and sensitive data locations to address A.8.9 requirements.

Activate vulnerability detection to satisfy A.8.8, scheduling regular scans and establishing remediation workflows for discovered vulnerabilities. Run Security Configuration Assessment against CIS benchmarks to identify misconfigurations, then work through findings systematically to establish your secure baseline.

Configure alerting integration with your existing communication channels—Slack, PagerDuty, or email—to ensure security events reach appropriate personnel for A.5.25 assessment and decision-making. Set up Active Response scripts for common attack patterns like SSH brute force attempts or detected malware.

Finally, build custom dashboards and reports mapping WAZUH capabilities to your Statement of Applicability. Document which WAZUH features address each applicable control and configure alerting to demonstrate continuous monitoring. This documentation becomes your evidence package showing auditors exactly how your technical controls satisfy ISO 27001 requirements.

Conclusion

WAZUH delivers enterprise-grade security monitoring capabilities that map directly to ISO 27001:2022's technological control requirements. Its unified approach to log collection, file integrity monitoring, vulnerability detection, configuration assessment, and incident response addresses dozens of Annex A controls through a single platform—without licensing fees that inflate as data volumes grow.

The **transition deadline** makes selecting compliant security tooling urgent. Organizations that implement WAZUH now gain immediate security visibility while building the evidence base their ISO 27001 certification requires. The platform's flexibility means security teams can start with core capabilities and expand coverage incrementally, demonstrating continuous improvement that auditors value highly.

For security professionals and compliance officers evaluating SIEM solutions, WAZUH's open-source model eliminates vendor lock-in while its active development community ensures the platform evolves alongside emerging threats and regulatory requirements. Whether deployed on-premises, in the cloud, or through WAZUH's managed service, the platform provides the technical foundation organizations need to demonstrate ISO 27001:2022 compliance—and the operational security that compliance alone cannot guarantee.