Security Lab GRC Documentation

ISO 27001:2022, Annex A



Created By: Paul Leone

April 4, 2026

Table of Contents

ISO 27001:2022, Annex A 2
Version 2.0 ; Change Log (from v1.2, March 2026) 2
5. Organizational Controls 6
6. People Controls 13
7. Physical Controls 15
8. Technological Controls 16
Control Deployment Summary 25
Version History 26

ISO 27001:2022, Annex A

Document Control:

Version:	**2.0**
Last Updated:	April 2026
Owner:	Paul Leone
Prior Version:	1.2 - March 2026

International Organization for Standardization

Version 2.0 ; Change Log (from v1.2, March 2026)

Cloud workload content has been integrated directly into the Evidence/Implementation Detail column of each affected control. Cloud node inventory: AWS (2 nodes: Amazon Linux 2, Windows Server 2025), Azure (2 nodes: Ubuntu 24.04 LTS, Windows Server 2025), GCP (2 nodes: Debian 13.4, Ubuntu) ; 6 nodes total across 3 providers. All nodes connected via Tailscale WireGuard mesh VPN with no public management ports exposed.

Control	Control Name	Change	Status Impact
A 5.7	**Threat Intelligence**	AWS GuardDuty ML-based behavioral detection (VPC flow logs, CloudTrail, DNS query logs), GCP Security Command Center (asset inventory, vulnerability findings, threat detection), and Azure Defender for Cloud + Sentinel (KQL detection rules, automated incident creation) added as cloud-native threat intelligence sources supplementing MISP, CrowdSec, and AlienVault OTX.	Implemented
A 5.9	**Asset Inventory**	Asset inventory expanded to include 6 cloud nodes across 3 providers tracked in Checkmk, Wazuh, and PatchMon via Tailscale. Cloud VPC/VNet topology, Tailscale mesh routing tables, and per-provider instance IDs documented.	Implemented
A 5.14	**Information Transfer**	Tailscale WireGuard (ChaCha20-Poly1305) added as primary encryption layer for all cloud-to-on-premises management traffic. SSH AES-256-GCM enforced for Linux cloud node terminal access. No plaintext management paths exist across any cloud node.	Implemented
A 5.15	**Access Control**	Cloud access controls added: AWS Security Groups (tailscale-access + lab-services) restrict all inbound to homelab subnets and Tailnet CGNAT; GCP VPC firewall policy (17 rules, Google Threat Intelligence blocking); Azure NSG homelab-nsg2 with DenyAllInBound at priority 65500. AWS IAM instance profiles scoped to minimum required actions.	Implemented
A 5.16	**Identity Management**	Cloud node identity management added: Linux cloud nodes use SSH Ed25519 keys distributed via	Implemented

		Ansible. AWS Windows Server 2025 and Azure Windows Server 2025 domain-joined to home.com via Tailscale for Kerberos authentication, Group Policy, and WSUS patch management.	
A 5.19	**Supplier Relationships**	Cloud provider supply chain controls documented: AWS IAM instance profiles (no long-lived access keys on EC2), GCP service accounts with minimal role assignments (no owner/editor on Compute instances), Azure ARM template with securestring parameters. Provider-native image signing and verification acknowledged.	Partial
A 5.22	**Monitoring of Supplier Services**	Cloud provider audit trails added as continuous monitoring sources: AWS CloudTrail (all API events), GCP Admin Activity and Data Access logs (always-on), Azure Activity Log and Monitor. Cloud-native security posture tools (GuardDuty, SCC, Defender for Cloud) provide continuous monitoring independent of on-premises toolchain.	Partial
A 5.23	**Information Security for Use of Cloud Services**	Expanded from SaaS-only scope to include full IaaS deployment across AWS, Azure, and GCP. IAM least-privilege, network segmentation (VPC/VNet with provider-native firewall policies), encryption in transit (TLS 1.3/WireGuard), no public management ports, cloud-native audit logging, and Wazuh EDR extended to all 6 cloud nodes.	Implemented
A 5.26	**Response to Incidents**	Cloud containment actions added: Wazuh Active Response (firewall-drop, host-deny, disable-account) executes on cloud nodes via Tailscale. AWS Security Group modification, GCP VPC firewall rule updates via Terraform, and Azure NSG rule modification via ARM template available for rapid cloud node isolation.	Implemented
A 5.29	**Information Security During Disruption**	Cloud HA added: Tailscale subnet router redundancy via dual on-premises pfSense nodes. Azure Spot instance Deallocate policy with documented restart procedure. Cloud node RTO target validated at less than 2 hours via Ansible rebuild playbooks.	Implemented
A 5.30	**ICT Readiness for Business Continuity**	Cloud rebuild capability added: ARM template (Azure), Ansible new_install_baseline_roles.yml, and Tailscale pre-authorized key re-enrollment enable cloud node rebuild from code. Cloud node RTO target less than 2 hours tested. Uptime Kuma monitors Tailscale tunnel health for all 6 cloud nodes.	Implemented
A 8.1	**User Endpoint Devices**	Cloud node endpoint coverage added: Wazuh agents deployed on all 6 cloud nodes applying CIS SCA policies (CIS Amazon Linux, Debian 12/13, Ubuntu 22.04/24.04, Windows Server 2025). Microsoft Defender active on Windows Server 2025 nodes	Implemented

		(AWS, Azure). ClamAV deployed on all 4 Linux cloud nodes.	
A 8.6	**Capacity Management**	Cloud capacity monitoring added: AWS CloudWatch Agent (CPU, memory, disk, network per EC2 instance), GCP Cloud Monitoring Ops Agent for Compute nodes, Azure Monitor VM metric alert rules (7 active rules). All cloud metrics feed Checkmk on-premises dashboard and Discord alerting.	Implemented
A 8.8	**Management of Technical Vulnerabilities**	Cloud vulnerability management added: Wazuh CIS SCA on all 6 cloud nodes daily, PatchMon daily CVE correlation for 4 Linux cloud nodes, WSUS for 2 Windows cloud nodes. AWS Inspector, GCP SCC vulnerability assessment, and Azure Defender for Cloud recommendations provide supplemental cloud-native scanning. Critical less than 72h MTTR SLA maintained across cloud scope.	Implemented
A 8.9	**Configuration Management**	Cloud configuration management added: Ansible linux_hardening.yml and new_install_baseline_roles.yml applied to all 4 Linux cloud nodes via SSH over Tailscale. Azure ARM template version-controlled in Git. Windows cloud nodes managed via GPO (domain-joined). All cloud configurations stored in Git alongside on-premises IaC.	Implemented
A 8.12	**Data Leakage Prevention**	Cloud egress filtering added as partial compensating control: AWS Security Group outbound rules restrict to required management destinations, GCP VPC firewall policy limits egress to documented management services, Azure NSG outbound rules enforce explicit allow-list. Formal DLP solution planned Q2 2026.	Partial
A 8.13	**Information Backup**	Cloud backup procedures added: AWS EBS snapshots, GCP disk snapshots, Azure VM snapshots with provider-native encryption. Cloud node rebuild from Git + Ansible provides infrastructure-as-code recovery path independent of backup images. RTO target less than 2 hours validated.	Implemented
A 8.15	**Logging**	Cloud audit logging integrated: AWS CloudTrail (all management events to S3 with SSE), GCP Admin Activity logs (always-on, cannot be disabled) and Data Access audit logs, Azure Activity Log and Monitor. Wazuh agent on all 6 cloud nodes forwards endpoint security events to on-premises Splunk. 90-day retention maintained across all cloud log sources.	Implemented
A 8.16	**Monitoring Activities**	Cloud monitoring added: AWS CloudWatch Agent metrics and GuardDuty behavioral detection, GCP Cloud Monitoring Ops Agent with SCC threat detection and VPC network IDS endpoint, Azure	Implemented

		Monitor VM metric alerts and Sentinel KQL detection rules (NSG deny spikes, sign-in anomalies, domain join events, AMA data gaps). All 6 cloud nodes visible in Checkmk on-premises dashboard.	
A 8.17	**Clock Synchronization**	Cloud time synchronization confirmed: all 4 Linux cloud nodes configured with NTP (time.google.com, time.cloudflare.com) via Ansible. Windows cloud nodes sync via domain NTP policy over Tailscale. Cloud provider hypervisors provide host-level time sync baseline.	Implemented
A 8.19	**Installation of Software**	Cloud software installation controls added: Ansible-controlled deployments for Linux cloud nodes via Tailscale; WSUS approval workflows for Windows cloud nodes (AWS, Azure); Wazuh SCA validates running services against CIS benchmarks on all 6 cloud nodes.	Implemented
A 8.20	**Network Security**	Cloud network security added: AWS VPC with Security Groups (default-deny), GCP VPC firewall policy with Google Threat Intelligence blocking (TOR exit nodes, malicious IPs, sanctioned countries), Azure NSG homelab-nsg2 (explicit allow-list, default-deny). GCP Cloud Armor three-tier WAF/DDoS policies (edge, backend, application-level) protect GCP workloads.	Implemented
A 8.21	**Security of Network Services**	Cloud network service security added: all cloud management traffic encrypted via Tailscale WireGuard (ChaCha20-Poly1305); SSH v2 AES-256-GCM enforced on Linux cloud nodes via Ansible; TLS 1.3 for all cloud-hosted HTTPS services; cloud DNS resolved via on-premises Unbound (192.168.1.153/154) over Tailscale with DNSSEC validation and malware domain blocking.	Implemented
A 8.22	**Segregation of Networks**	Cloud network segmentation added: per-provider network isolation ; AWS VPC (172.31.0.0/16), GCP VPC (10.128.0.0/16), Azure VNet homelab-vnet2 (10.130.0.0/16) each isolated from other providers. Inter-cloud communication only via Tailscale overlay. Cloud nodes not directly routable to on-premises without Tailscale ACL authorization.	Implemented
A 8.24	**Use of Cryptography**	Cloud cryptographic controls added: Tailscale WireGuard (ChaCha20-Poly1305) for all management paths; AWS S3 SSE for CloudTrail logs; GCP default encryption for persistent disks and GCS buckets; Azure Managed Disk and Log Analytics workspace encrypted at rest. Provider-native key management used for cloud storage encryption.	Implemented

5. Organizational Controls

Control	2013 Ref	Control Name	Evidence / Implementation Detail	Status
A 5.1	A 5.1.1, A 5.1.2	**Policies for Information Security**	Lab mission statement defines security-first architecture; compliance requirements documented; comprehensive logging policy (100% security event coverage); SSH hardening policy (CIS Benchmark); TLS 1.3 minimum policy; vulnerability remediation SLAs by severity (Critical less than 72h, High less than 7 days); risk-based CVSS scoring methodology.	Implemented
A 5.2	A 6.1.1	**Information Security Roles and Responsibilities**	Not applicable - personal lab environment.	N/A
A 5.3	A 6.1.2	**Segregation of Duties**	Not applicable - personal lab environment.	N/A
A 5.4	A 7.2.1	**Management Responsibilities**	Not applicable - personal lab environment.	N/A
A 5.5	A 6.1.3	**Contact with Authorities**	Not applicable - personal lab environment.	N/A
A 5.6	A 6.1.4	**Contact with Special Interest Groups**	Not applicable - personal lab environment.	N/A
A 5.7	NEW	**Threat Intelligence**	CrowdSec community signals; MISP threat feeds (bi-directional); NVD vulnerability database; Shuffle CVE aggregation (NIST NVD, Exploit-DB); Cortex multi-source enrichment (VirusTotal, AbuseIPDB, Shodan, MISP, URLhaus, PhishTank); SIEM correlation with threat feeds. Cloud: AWS GuardDuty ML-based behavioral detection (VPC flow logs, CloudTrail, DNS query logs) provides cloud-native threat intelligence with no manual rule maintenance. GCP Security Command Center delivers asset inventory, vulnerability findings, and threat detection across the GCP project. Azure Defender for Cloud and Sentinel (KQL detection rules: NSG deny-inbound spikes, Entra ID sign-in from new geographic location, unexpected domain join events, AMA data gaps) provide cloud-layer behavioral intelligence. All cloud-native findings forwarded to on-premises SIEM via Wazuh agent telemetry.	Implemented
A 5.8	A 6.1.5, A 14.1.1	**Information Security in Project Management**	Infrastructure as Code (Terraform, Ansible); Git version control; security requirements in deployment automation; threat modeling for new services; CI/CD security linting (planned).	Partial

			Cloud: ARM templates (Azure), Terraform cloud modules, and Ansible playbooks follow security-by-default patterns; cloud node provisioning IaC reviewed before apply; all cloud configurations version-controlled in Git.	
A 5.9	A 8.1.1, A 8.1.2	**Inventory of Information and Other Associated Assets**	PatchMon tracks 5,000+ packages across 30+ on-premises hosts; WUD tracks 50+ containers; OpenVAS asset database (75+ assets); Nessus software inventory; Wazuh agent inventory (31+ endpoints); DNS records; SSH host keys (Ansible); Checkmk infrastructure inventory; Prometheus node exporters; NetAlert network inventory. Cloud: 6 cloud nodes across 3 providers ; AWS (Amazon Linux 2 EC2 t3.micro, Windows Server 2025 EC2 c7i-flex.large), Azure (Ubuntu 24.04 LTS Standard_B2ats_v2, Windows Server 2025 Standard_E2s_v3), GCP (Debian 13.4 e2.micro, Ubuntu e2.micro) ; all enrolled in Checkmk, Wazuh, and PatchMon via Tailscale. Cloud VPC/VNet CIDR allocations (AWS 172.31.0.0/16, GCP 10.128.0.0/16, Azure 10.130.0.0/16) and Tailscale mesh routing tables documented.	Implemented
A 5.10	A 8.1.3, A 8.2.3	**Acceptable Use of Information and Other Associated Assets**	Not applicable - personal lab environment.	N/A
A 5.11	A 8.1.4	**Return of Assets**	Not applicable - personal lab environment.	N/A
A 5.12	A 8.2.1	**Classification of Information**	Data classification scheme: Public, Internal, Confidential; lab data classified as Internal Use; no sensitive/classified data processed. Cloud data classified under same scheme: CloudTrail logs (Confidential), GCP audit logs (Confidential), Wazuh agent telemetry (Internal), Azure Log Analytics homelab-log (Internal).	Partial
A 5.13	A 8.2.2	**Labelling of Information**	Not formalized ; lab environment informal labeling.	Not Implemented
A 5.14	A 13.2.1, A 13.2.2, A 13.2.3	**Information Transfer**	TLS 1.3 encryption (Traefik); SSH encrypted file transfers; syslog-ng TLS transmission to SIEM; encrypted backups; Cloudflare Tunnels for secure remote access; Tailscale mesh VPN; no unencrypted data transmission. Cloud: all management traffic between cloud nodes and on-premises encrypted via Tailscale WireGuard (ChaCha20-Poly1305). SSH AES-256-GCM for Linux cloud node terminal access. Cloud-to-	Implemented

			cloud communication routes through Tailscale overlay, not public internet. Cloud provider VPC/VNet internal traffic uses provider-encrypted private networking. No plaintext management paths exist across any cloud node.	
A 5.15	A 9.1.1, A 9.1.2	**Access Control**	Authentik SSO integration; centralized SSH key management via Ansible; individual user accounts (no shared credentials); MFA enforcement (Authentik TOTP); Traefik ForwardAuth SSO; IP allowlisting; firewall rules restrict backend access. Cloud: AWS Security Groups (tailscale-access + lab-services) restrict all inbound management to homelab subnets and Tailnet CGNAT (100.64.0.0/10). GCP VPC firewall policy restricts SSH to 192.168.0.0/16. Azure NSG homelab-nsg2 enforces explicit allow-list with DenyAllInBound at priority 65500. AWS IAM instance profiles scoped to minimum required actions; no wildcard permissions.	Implemented
A 5.16	A 9.2.1	**Identity Management**	Centralized via Authentik; SSH keys tracked in Ansible inventory; Active Directory user management; unique user accounts; SIEM correlation identifies orphaned accounts; Wazuh tracks active user sessions. Cloud: Linux cloud nodes (4 nodes: Amazon Linux 2, Debian 13.4, Ubuntu x2) use SSH Ed25519 keys distributed via Ansible. AWS Windows Server 2025 and Azure Windows Server 2025 domain-joined to home.com via Tailscale, providing Kerberos authentication, Group Policy enforcement, and WSUS patch management. Cloud IAM service accounts (AWS instance profiles, GCP service accounts, Azure Managed Identity) inventoried with minimal role assignments.	Implemented
A 5.17	A 9.2.4, A 9.3.1, A 9.4.3	**Authentication Information**	SSH private keys encrypted; Authentik credentials in Vaultwarden (zero-knowledge encryption); MFA enforcement (100% admin accounts); password complexity requirements; no hardcoded credentials (Ansible Vault); biometric unlock (Vaultwarden). Cloud: no shared credentials on cloud nodes; SSH key-only access for Linux cloud nodes (passwords disabled globally); Windows cloud nodes authenticate via domain Kerberos; cloud console access (AWS, GCP, Azure) enforces provider MFA.	Implemented

A 5.18	A 9.2.2, A 9.2.5, A 9.2.6	**Access Rights**	Authentik RBAC groups; SSH sudo policies; least-privilege access; privilege escalation logged to SIEM; access review via authentication logs; Wazuh monitors unauthorized access attempts; centralized SSH key revocation via Ansible. Cloud: AWS IAM access key quarterly review (no long-lived keys on EC2 ; instance profiles used); GCP service account IAM recommender audits; Azure Entra ID accounts subject to 45-day dormancy policy; cloud node access revocation via SSH key removal (Ansible), Tailscale node key expiry, and IAM role disassociation.	Implemented
A 5.19	A 15.1.1	**Information Security in Supplier Relationships**	Vetted open-source projects; official Docker registries; trusted package repositories; MISP vendor compromise tracking. Cloud: cloud provider supply chain controls documented ; AWS IAM instance profiles with least-privilege roles (no long-lived access keys on EC2), GCP service accounts with minimal IAM role assignments (no owner/editor on Compute instances), Azure VMs provisioned via ARM template with securestring parameters. Provider-native image signing verified for AMIs, GCP Compute images, and Azure Marketplace images.	Partial
A 5.20	A 15.1.2	**Addressing Information Security Within Supplier Agreements**	Not applicable - personal lab environment.	N/A
A 5.21	A 15.1.3	**Managing Information Security in the ICT Supply Chain**	Package signature verification; Docker image SHA-256 validation; software provenance tracking (limited); SBOM implementation planned (Trivy/Grype). Cloud: cloud node base images (AMIs, GCP Compute images, Azure Marketplace images) tracked by version; provider-maintained base images (Amazon Linux 2, Ubuntu, Debian) used with same-day security patch availability; no formal SBOM for cloud node packages pending Trivy/Grype deployment.	Partial
A 5.22	A 15.2.1, A 15.2.2	**Monitoring, Review and Change Management of Supplier Services**	Dependabot/Renovate dependency updates (planned); WUD container update monitoring; PatchMon package tracking; automated vulnerability scanning of third-party components. Cloud: AWS CloudTrail captures all provider API calls including IAM role assumptions and service configuration changes. GCP Admin Activity audit logs	Partial

			(always-on) capture all resource changes. Azure Activity Log records all ARM deployments and resource modifications. Cloud-native security posture tools (GuardDuty, SCC, Defender for Cloud) reviewed continuously for provider-specific findings.	
A 5.23	NEW	**Information Security for Use of Cloud Services**	Cloud IaaS security controls defined and implemented across AWS, GCP, and Azure: IAM least-privilege (per-provider service accounts/instance profiles with minimal role assignments), network segmentation (VPC/VNet with provider-native firewall policies enforcing default-deny), encryption in transit (TLS 1.3/WireGuard across all management paths), no public management port exposure (all access via Tailscale WireGuard with device-bound authentication), cloud-native audit logging enabled by default, and on-premises Wazuh EDR extended to all 6 cloud nodes. Cloud provider security services enabled: AWS GuardDuty + Security Hub, GCP Security Command Center + Cloud Armor three-tier WAF/DDoS, Azure Defender for Cloud + Sentinel + DDoS Protection plan. Cloud node patch management via PatchMon (Linux) and WSUS (Windows) maintains Critical less than 72h MTTR SLA. Cloud DNS resolved via on-premises Unbound resolvers over Tailscale for consistent malware domain blocking.	Implemented
A 5.24	A 16.1.1	**Information Security Incident Management Planning and Preparation**	TheHive IR workflows (15+ documented playbooks: phishing, malware, ransomware, lateral movement, vulnerability response); Cortex responders (automated containment); Shuffle automated orchestration; SOC team structure; escalation procedures; multi-channel communication (Discord, SMTP, Cloudflare); on-call rotation. Cloud: AWS GuardDuty findings and Azure Sentinel incidents automatically create TheHive cases via Shuffle SOAR webhook; GCP SCC findings trigger alerting policy notifications; cloud node IR runbooks (Tailscale containment, Security Group/NSG modification, Wazuh Active Response) documented.	Implemented
A 5.25	A 16.1.4	**Assessment and Decision on Information Security Events**	Cortex multi-engine analysis (VirusTotal, AbuseIPDB, Shodan, MISP, Yara, File_Info, URLhaus, PhishTank); MISP threat intelligence correlation; threat scoring (confidence-based); severity assessment (CVSS, asset criticality); Shuffle automated enrichment workflows;	Implemented

			TheHive observable correlation; SIEM-based event triage. Cloud: AWS GuardDuty finding types mapped to MITRE ATT&CK (Recon:EC2/Portscan, CredentialAccess:IAMUser/AnomalousBehavior, etc.); GCP SCC finding categories aligned to cloud attack taxonomy; Azure Sentinel analytics rules tagged with MITRE ATT&CK techniques.	
A 5.26	A 16.1.5	**Response to Information Security Incidents**	TheHive case management (structured workflows); automated containment (Wazuh Active Response: firewall-drop, host-deny, disable-account; Cortex responders; Shuffle orchestration); multi-party coordination (Discord real-time collaboration); escalation to management (PagerDuty); forensic data collection (Wazuh, memory dumps); MISP IOC sharing; sub-30-minute MTTR. Cloud: Wazuh Active Response (firewall-drop, host-deny, disable-account) executes on cloud nodes via Tailscale using same containment playbooks as on-premises. AWS Security Group modification for EC2 isolation, GCP VPC firewall rule update via Terraform, Azure NSG rule modification via ARM template or CLI available for rapid cloud node containment. Cloud node disk snapshots available for offline forensic analysis.	Implemented
A 5.27	A 16.1.6	**Learning from Information Security Incidents**	Metrics tracking (MTTR, MTTD, case volume); process improvement (workflow optimization); lessons learned (playbook updates); Shuffle workflow refinement based on execution data; trend analysis dashboards (Grafana). Cloud: Azure Spot instance eviction experience documented and restart procedure refined; Tailscale tunnel recovery procedure updated; cloud node Wazuh re-enrollment runbook tested and updated following agent version upgrades.	Implemented
A 5.28	A 16.1.7	**Collection of Evidence**	Wazuh forensic data collection; immutable SIEM logs (Splunk read-only indexes, Elastic immutable streams); TheHive evidence management; chain of custody documentation; encrypted log transmission (syslog-ng TLS); 90-day retention; memory dump capability; packet captures (tcpdump/Wireshark). Cloud: Wazuh agents on cloud nodes collect forensic data (process trees, file hashes, network connections) forwarded to on-premises SIEM. AWS VPC flow logs and CloudTrail provide immutable control-	Implemented

			plane forensic trail. GCP Admin Activity logs provide always-on audit trail. Azure Sentinel workspace retains logs for investigation.	
A 5.29	A 17.1.1, A 17.1.2, A 17.1.3	**Information Security During Disruption**	HA DNS failover (dual Unbound/Technitium); snapshot-before-patch; pre-scan snapshots for critical systems; documented restore procedures; rollback capability for failed patches; dual SIEM deployment (Splunk + Elastic); multi-layered detection reduces blind spots. Cloud: Tailscale subnet router redundancy via dual on-premises pfSense nodes ensures alternate management path if single cloud node is unavailable. Azure Spot instance (Standard_E2s_v3) eviction handled by Deallocate policy with documented restart procedure. Cloud node RTO target less than 2 hours via Ansible rebuild playbooks validated.	Implemented
A 5.30	NEW	**ICT Readiness for Business Continuity**	Infrastructure as Code enables rapid rebuild (Terraform, Ansible); documented disaster recovery procedures; IaC rebuild tested (less than 2 hour RTO); automated backups (bi-weekly); quarterly restore testing; Git version control for configurations. Cloud: ARM template (Azure), Ansible new_install_baseline_roles.yml, and Tailscale pre-authorized key re-enrollment enable cloud node rebuild from code. Cloud node rebuild timing validated against less than 2 hour RTO target. Uptime Kuma monitors Tailscale tunnel health for all 6 cloud nodes with Discord webhook alerting on tunnel failure.	Implemented
A 5.31	A 18.1.1, A 18.1.5	**Legal, Statutory, Regulatory and Contractual Requirements**	Compliance framework mappings documented (NIST CSF, CIS, PCI-DSS conceptual); no regulated data processing; open-source licensing compliance. Cloud: AWS, Azure, and GCP provider terms of service acknowledged; no cardholder data processed on cloud nodes; cloud provider SOC 2 and ISO 27001 certifications acknowledged.	Partial
A 5.32	A 18.1.2	**Intellectual Property Rights**	Open-source software licensing tracked; GPL/MIT/Apache compliance; no proprietary software piracy; license documentation in Git. Cloud: cloud provider base images (Amazon Linux 2, Ubuntu, Debian) use open-source licensing; Azure Marketplace image licensing terms acknowledged.	Partial
A 5.33	A 18.1.3	**Protection of Records**	90-day log retention (SIEM); immutable audit trails; encrypted backups; documented retention schedules; compliance with data retention requirements. Cloud: AWS CloudTrail	Implemented

			logs retained in S3 with 90-day lifecycle policy; GCP Admin Activity logs retained per GCP defaults (400 days); Azure Log Analytics homelab-log configured for 90-day retention; cloud endpoint events forwarded to on-premises SIEM subject to 90-day hot / 1-year cold retention.	
A 5.34	A 18.1.4	**Privacy and Protection of PII**	No PII processing in lab environment; data minimization principles; encryption for any personal data (Vaultwarden); GDPR principles applied. Cloud: no PII processed on cloud nodes; cloud audit logs (CloudTrail, GCP Audit Logs, Azure Activity Log) contain operational metadata only; data minimization maintained across cloud scope.	Implemented
A 5.35	A 18.2.1	**Independent Review of Information Security**	Not applicable - personal lab environment.	N/A
A 5.36	A 18.2.2, A 18.2.3	**Compliance with Policies, Rules and Standards**	CIS Benchmark compliance audits (92-98%); Nessus configuration audits; policy violations detected via compliance scans; Wazuh SCA detects deviations; SIEM dashboards track compliance metrics; continuous compliance monitoring. Cloud: Wazuh SCA applies CIS benchmarks (CIS Amazon Linux, Debian 12/13, Ubuntu 22.04/24.04, Windows Server 2025) to all 6 cloud nodes daily. AWS Security Hub CIS AWS Foundations benchmark assessed. Azure Defender for Cloud Secure Score monitored. GCP SCC security health analytics flags misconfigurations.	Implemented
A 5.37	A 12.1.1	**Documented Operating Procedures**	Ansible playbooks as documentation; Terraform modules; runbooks in Git; incident response playbooks (TheHive); change management procedures; backup/restore procedures; IaC serves as living documentation. Cloud: cloud node provisioning runbooks (Tailscale enrollment, Wazuh agent installation, Ansible baseline application), recovery procedures (Azure Spot restart, Tailscale re-enrollment, CIS SCA validation), and decommissioning checklists (SSH key removal, Tailscale revocation, IAM role cleanup) documented in Git.	Implemented

6. People Controls

Control	2013 Ref	Control Name	Evidence / Implementation Detail	Status
A 6.1	A 7.1.1	**Screening**	Not applicable - personal lab, single administrator.	N/A
A 6.2	A 7.1.2	**Terms and Conditions of Employment**	Not applicable - personal lab, no employees.	N/A
A 6.3	A 7.2.2	**Information Security Awareness, Education and Training**	Not applicable - personal lab, no employees.	N/A
A 6.4	A 7.2.3	**Disciplinary Process**	Not applicable - personal lab, no employees.	N/A
A 6.5	A 7.3.1	**Responsibilities After Termination or Change of Employment**	Not applicable - personal lab, no employees.	N/A
A 6.6	A 13.2.4	**Confidentiality or Non-Disclosure Agreements**	Not applicable ; no external parties with access.	N/A
A 6.7	A 6.2.2	**Remote Working**	SSH secure remote access; Tailscale mesh VPN; Cloudflare Tunnels; MFA enforcement for remote access; encrypted connections (TLS 1.3); VPN monitoring and logging; IP allowlisting. Cloud: all cloud node management access routes exclusively through Tailscale WireGuard with device-bound authentication; no public management ports on any cloud instance; cloud console access (AWS, GCP, Azure) enforces provider MFA independently.	Implemented
A 6.8	A 16.1.2, A 16.1.3	**Information Security Event Reporting**	Discord webhooks for real-time alerts; email notifications via SMTP relay; Cloudflare email routing; TheHive case creation from alerts; Splunk scheduled reports; Wazuh Discord/email integration; Prometheus Alertmanager; Grafana threshold alerts; multi-channel redundancy ensures zero missed notifications. Cloud: AWS SNS notifications, GCP alerting policy notifications, and Azure Monitor action group (RecommendedAlertRules-AG-1) integrated into Discord/email notification chain. AWS GuardDuty and Azure Sentinel automatically create TheHive cases via Shuffle SOAR webhook.	Implemented

7. Physical Controls

Control	2013 Ref	Control Name	Evidence / Implementation Detail	Status
A 7.1	A 11.1.1	**Physical Security Perimeters**	Home lab environment ; residential security (locks, alarm system); server equipment in dedicated secure area.	N/A
A 7.2	A 11.1.2, A 11.1.6	**Physical Entry**	Not applicable - personal lab.	N/A
A 7.3	A 11.1.3	**Securing Offices, Rooms and Facilities**	Not applicable - personal lab.	N/A
A 7.4	NEW	**Physical Security Monitoring**	HVAC monitoring via Prometheus; temperature alerts configured; Pulse hypervisor monitoring for hardware health; no video surveillance. Cloud: physical security for cloud nodes delegated to provider (AWS, GCP, Azure maintain SOC 2 / ISO 27001 certified data centers with physical access controls, CCTV, and environmental monitoring).	Partial
A 7.5	A 11.1.4	**Protecting Against Physical and Environmental Threats**	UPS battery backup for critical systems; environmental monitoring (temperature, humidity via Prometheus); fire detection (residential smoke detectors); HVAC for cooling. Cloud: physical and environmental threats for cloud nodes managed by provider; no additional on-premises physical controls required.	Partial
A 7.6	A 11.1.5	**Working in Secure Areas**	Not applicable - personal lab.	N/A
A 7.7	A 11.2.9	**Clear Desk and Clear Screen**	Not applicable - personal lab.	N/A
A 7.8	A 11.2.1	**Equipment Siting and Protection**	Not applicable - personal lab.	N/A
A 7.9	A 11.2.6	**Security of Assets Off-Premises**	Not applicable - personal lab.	N/A
A 7.10	A 8.3.1, A 8.3.2, A 8.3.3, A 11.2.5	**Storage Media**	Encrypted backup media; secure storage of backup drives; removable media disabled via GPO (Windows); USB device restrictions; encrypted portable drives. Cloud: cloud nodes have no removable media; cloud storage encryption covered under A 8.24.	Implemented
A 7.11	A 11.2.2	**Supporting Utilities**	UPS for power backup; dual internet connections (primary + backup); redundant power supplies in servers. Cloud: cloud provider infrastructure redundancy (AWS	Partial

			Availability Zone us-east-2c, GCP us-central1-c, Azure North Central US) provides utility resilience beyond on-premises capability.	
A 7.12	A 11.2.3	**Cabling Security**	Not applicable - personal lab.	N/A
A 7.13	A 11.2.4	**Equipment Maintenance**	Regular hardware maintenance logged; firmware updates tracked; scheduled maintenance windows; Proxmox hardware monitoring; Checkmk infrastructure monitoring. Cloud: cloud node OS maintenance handled via PatchMon (Linux) and WSUS (Windows); Checkmk monitors cloud node health metrics (CPU, memory, disk, services) via Tailscale.	Partial
A 7.14	A 11.2.7	**Secure Disposal or Re-Use of Equipment**	Secure deletion procedures documented; DBAN/shred for drive sanitization; physical destruction of retired drives; encrypted storage wiping before disposal. Cloud: AWS EC2 EBS volume deletion documented in decommissioning runbook; GCP persistent disk deletion policy documented; Azure Managed Disk cleanup included in decommissioning checklist; cloud-native data destruction verified via provider console.	Implemented

8. Technological Controls

Control	2013 Ref	Control Name	Evidence / Implementation Detail	Status
A 8.1	A 6.2.1, A 11.2.8	**User Endpoint Devices**	Wazuh EDR on 31+ endpoints (25+ on-premises + 6 cloud); endpoint encryption (BitLocker, LUKS planned); device certificates via Step-CA; endpoint compliance monitoring; Group Policy hardening (Windows); antivirus (Microsoft Defender, ClamAV); GPO-enforced security settings. Cloud: Wazuh agents deployed on all 6 cloud nodes applying CIS SCA policies (CIS Amazon Linux for Amazon Linux 2, CIS Debian 12/13 for Debian 13.4, CIS Ubuntu 22.04/24.04 for Ubuntu nodes, CIS Windows Server 2025 for Windows Server 2025 on AWS and Azure). Microsoft Defender active on both Windows Server 2025 cloud nodes. ClamAV deployed on all 4 Linux cloud nodes. Non-compliant cloud nodes identified via CIS SCA score in Wazuh dashboard.	Implemented

A 8.2	A 9.2.3	**Privileged Access Rights**	Separate privileged accounts; monitored via SIEM (Splunk admin login dashboard); MFA enforced (100% admin accounts); SSH key-based auth for privileged access; sudo usage logged; Wazuh tracks privileged authentication events; no shared admin credentials. Cloud: AWS IAM instance profiles scoped to minimum required actions (no AdministratorAccess policy); GCP service accounts use minimal roles (no owner/editor); Azure subscription admin access MFA-enforced via Entra Conditional Access; cloud console access governed by provider IAM with MFA.	Implemented
A 8.3	A 9.4.1	**Information Access Restriction**	Traefik ForwardAuth restricts application access; firewall rules (pfSense default-deny); SSH IP allowlisting; file permissions (least privilege); Wazuh FIM monitors unauthorized access; network segmentation (VLANs); backend isolation. Cloud: Tailscale ACL policy enforces per-device/per-subnet explicit allow rules (default deny for all inter-node traffic); cloud firewall policies restrict access to defined homelab subnet ranges; Wazuh FIM monitors sensitive file paths on all cloud nodes.	Implemented
A 8.4	A 9.4.5	**Access to Source Code**	Git access control (SSH keys); branch protection rules; code review requirements (pull requests); Ansible playbooks version controlled; infrastructure code (Terraform) in private repositories; no public exposure of sensitive code. Cloud: Azure ARM templates, cloud Terraform modules, and cloud Ansible inventory stored in same Git repository as on-premises IaC with same branch protection and review requirements.	Implemented
A 8.5	A 9.4.2	**Secure Authentication**	MFA enforcement (Authentik TOTP); SSH key-based authentication (Ed25519); TLS 1.3 client certificates; password complexity requirements; account lockout policies (5 failed attempts); session timeout (30 min idle); replay-resistant authentication (SSH session tokens, Authentik CSRF protection). Cloud: SSH key-only access for Linux cloud nodes (passwords disabled globally via Ansible); Windows cloud nodes authenticate via domain Kerberos over Tailscale; cloud console access enforces provider MFA independently.	Implemented

A 8.6	A 12.1.3	**Capacity Management**	Prometheus capacity monitoring; Grafana dashboards track resource usage (CPU, memory, disk, bandwidth); storage capacity alerts (80% threshold); auto-archival of logs; capacity planning for growth; resource trending analysis. Cloud: AWS CloudWatch Agent collects CPU, memory, disk, and network metrics per EC2 instance. GCP Cloud Monitoring Ops Agent provides Compute node metrics. Azure Monitor VM metric alert rules (7 active: Available Memory Bytes, Data Disk IOPS Consumed %, Network In/Out Total, OS Disk IOPS, Percentage CPU, VM Availability) feed Discord alerting. All cloud node metrics visible in Checkmk on-premises dashboard.	Implemented
A 8.7	A 12.2.1	**Protection Against Malware**	Wazuh FIM with VirusTotal integration; Suricata/Snort IDS signatures; ClamAV (Linux); Microsoft Defender (Windows); rootkit detection (Wazuh); automated signature updates; Yara rules for malware detection; Cortex malware analysis (multi-engine). Cloud: Wazuh FIM and rootkit detection deployed on all 6 cloud nodes with same monitored path configuration as on-premises. ClamAV freshclam runs on 4 Linux cloud nodes. Windows Defender definitions updated via WSUS on 2 Windows cloud nodes. AWS GuardDuty ML-based behavioral detection, GCP SCC threat detection, and Azure Defender for Cloud behavioral analytics provide cloud-native malware detection independent of signature databases.	Implemented
A 8.8	A 12.6.1, A 18.2.3	**Management of Technical Vulnerabilities**	Weekly OpenVAS network scans (52/year); monthly Nessus authenticated scans (12/year); daily PatchMon package checks; CVE correlation with NVD; CVSS-based prioritization; MTTR less than 72h Critical, less than 7 days High; 95% patched within SLA; Wazuh vulnerability assessment; SIEM correlation with exploit databases; automated vulnerability-to-patch correlation. Cloud: Wazuh agents run CIS SCA and vulnerability assessment on all 6 cloud nodes daily. PatchMon daily CVE correlation for 4 Linux cloud nodes (Amazon Linux 2, Debian 13.4, Ubuntu x2). WSUS manages 2 Windows cloud nodes (AWS, Azure) with automated approval workflows.	Implemented

			AWS Inspector provides agent-based vulnerability assessment for EC2. GCP SCC vulnerability assessment for Compute instances. Azure Defender for Cloud recommendations for Azure VMs. Critical less than 72h MTTR SLA maintained across all cloud nodes.	
A 8.9	NEW	**Configuration Management**	Ansible playbooks define baselines; Terraform IaC; Git version control; configuration drift detection; CIS Benchmark compliance audits (92-98%); automated remediation; Nessus configuration audits; Wazuh SCA; baseline deviation alerts. Cloud: Ansible linux_hardening.yml and new_install_baseline_roles.yml applied to all 4 Linux cloud nodes via SSH over Tailscale. Windows cloud nodes managed via GPO (domain-joined to home.com via Tailscale). Azure ARM template (azuredeploy.json) version-controlled in Git. Cloud configuration changes require Git commit and apply workflow; no ad-hoc console changes.	Implemented
A 8.10	NEW	**Information Deletion**	Secure deletion procedures documented; automated log archival/deletion; 90-day retention policy enforcement; secure file deletion (shred/srm); encrypted storage wiping; immutable SIEM indexes prevent premature deletion. Cloud: AWS EC2 EBS volume deletion on instance termination (documented in runbook); GCP persistent disk deletion policy documented; Azure Managed Disk cleanup in decommissioning checklist; cloud-native audit logs subject to 90-day retention policy consistent with on-premises SIEM.	Implemented
A 8.11	NEW	**Data Masking**	Not implemented ; no production PII/sensitive data processing in lab.	Not Implemented
A 8.12	NEW	**Data Leakage Prevention**	Egress filtering via firewall; DNS query logging (Unbound/Pi-hole); Suricata/Snort monitors outbound traffic; unusual outbound traffic alerts (Prometheus); bandwidth monitoring; no formal DLP solution. Cloud: AWS Security Group outbound rules restrict to required management destinations (Wazuh 1514/1515, DNS 53, Checkmk, PatchMon ports). GCP VPC firewall policy limits egress to documented management services (priority 1000-2030 egress rules). Azure NSG outbound rules enforce explicit allow-list. Formal DLP solution planned Q2 2026; cloud	Partial

			egress filtering provides partial compensating control.	
A 8.13	A 12.3.1	**Information Backup**	Proxmox automated backups (bi-weekly); dual backup solutions (Proxmox Backup Server + external); encrypted backups (AES-256); offsite backup storage; quarterly restore testing; snapshot-before-patch; automated backup verification. Cloud: AWS EBS snapshots encrypted (account default KMS key); GCP disk snapshots encrypted at rest; Azure VM snapshots encrypted. Cloud node rebuild from code (Git + Ansible) provides infrastructure-as-code recovery path independent of backup images. Tailscale pre-authorized keys stored offline for re-enrollment. Cloud node RTO target less than 2 hours validated.	Implemented
A 8.14	A 17.2.1	**Redundancy of Information Processing Facilities**	HA firewall cluster (pfSense CARP); dual Unbound/Technitium DNS failover (less than 5s); dual SIEM deployment (Splunk + Elastic); redundant internet connections; multiple VPN paths (Tailscale, PIA, Cloudflare); load balancing (Traefik, MetalLB); failover capability documented. Cloud: Tailscale subnet router redundancy via dual on-premises pfSense nodes provides alternate management path. Cloud node redundancy across 3 independent providers (AWS, GCP, Azure) reduces single-provider dependency risk.	Implemented
A 8.15	A 12.4.1, A 12.4.2, A 12.4.3	**Logging**	100% security event logging; centralized SIEM (Splunk + Elastic); 90-day retention; structured JSON format; comprehensive coverage (DNS, SSH, Traefik, scans, patches, Wazuh, firewall, IDS, application logs); encrypted log transmission (syslog-ng TLS); immutable audit trails; logs include timestamp, user, source IP, action, result. Cloud: AWS CloudTrail collects all management events (IAM role assumptions, Security Group modifications, EC2 lifecycle events) delivered to S3 with SSE. GCP Admin Activity logs (always-on, cannot be disabled) and Data Access audit logs capture all resource changes. Azure Activity Log and Monitor record all ARM deployments. Wazuh agents on all 6 cloud nodes forward endpoint security events to on-premises Splunk via Tailscale. 90-day retention maintained across all cloud log sources.	Implemented

A 8.16	NEW	**Monitoring Activities**	Prometheus metrics collection; Grafana dashboards (25+); Uptime Kuma service availability (50+ monitors); Checkmk infrastructure monitoring; Pulse hypervisor monitoring; Wazuh endpoint monitoring (FIM, rootkit, processes); Splunk/Elastic SIEM correlation; Suricata/Snort IDS; TheHive case activity tracking; Cortex job monitoring; Shuffle workflow execution logs; NetAlert network monitoring; 100% visibility across infrastructure. Cloud: AWS CloudWatch Agent and GuardDuty behavioral detection cover EC2 nodes. GCP Cloud Monitoring Ops Agent with SCC threat detection and VPC network IDS endpoint for gcp-debian-host1. Azure Monitor VM metric alerts (7 active rules) and Sentinel KQL detection rules for Azure nodes. All 6 cloud nodes enrolled in Checkmk on-premises dashboard. Uptime Kuma monitors Tailscale tunnel health for all cloud nodes with sub-5-minute failure detection.	Implemented
A 8.17	A 12.4.4	**Clock Synchronization**	NTP time synchronization (Chrony); centralized time source (pool.ntp.org); sub-second accuracy; time drift monitoring; all systems synchronized; SIEM time correlation; accurate timestamps for forensics. Cloud: all 4 Linux cloud nodes configured with NTP (time.google.com, time.cloudflare.com) via Ansible. Windows cloud nodes sync via domain NTP policy over Tailscale. Cloud provider hypervisors provide host-level time synchronization as a baseline layer.	Implemented
A 8.18	A 9.4.4	**Use of Privileged Utility Programs**	Ansible execution restricted to authorized keys; sudo usage logged to SIEM; privileged command monitoring; Wazuh tracks privileged tool execution; administrative tool access restricted (RBAC); audit trail for privileged operations. Cloud: cloud console access (AWS, GCP, Azure) governed by provider IAM with MFA; cloud API access via instance profiles/service accounts with no interactive privileged utility exposure; all cloud administrative actions logged via CloudTrail, GCP Audit Logs, and Azure Activity Log.	Implemented
A 8.19	A 12.5.1, A 12.6.2	**Installation of Software on Operational Systems**	WSUS approval workflows (Windows); Ansible-controlled deployments (Linux); Watchtower automated container updates (labeled); authenticated vulnerability scans	Implemented

			verify only approved software; unauthorized applications detected (Nessus compliance scans); change control via Git; software inventory tracking (PatchMon, Wazuh). Cloud: Ansible-controlled software installation for 4 Linux cloud nodes via SSH over Tailscale; WSUS approval workflows for 2 Windows cloud nodes (AWS, Azure); Wazuh SCA validates running services against CIS benchmarks on all 6 cloud nodes; cloud provider package repositories used as trusted sources.	
A 8.20	A 13.1.1	**Networks Security**	HA firewall cluster (pfSense); default-deny rules; VLAN/subnet segmentation; ACLs per network segment; IDS/IPS (Suricata inline, Snort passive); network monitoring (NetAlert, Prometheus, pfSense logs); egress filtering; ingress controls (Traefik); DMZ isolation. Cloud: AWS VPC with Security Groups enforcing default-deny between cloud nodes and the internet. GCP VPC network firewall policy (homelab, 17 rules) with Google Threat Intelligence blocking (TOR exit nodes, known malicious IPs, sanctioned countries at priority 100-130). Azure NSG homelab-nsg2 with explicit allow-list and DenyAllInBound default. GCP Cloud Armor three-tier WAF/DDoS policies (edge: Tailscale/homelab allow-list; backend: DDoS rate limiting; application: SQLi/XSS blocking via v33-stable expression sets) protect GCP workloads. Azure DDoS Protection plan (homelab-ddos) protects Azure VNet.	Implemented
A 8.21	A 13.1.2	**Security of Network Services**	TLS 1.3 mandatory for all services; weak ciphers disabled; certificate validation enforced (Step-CA PKI); DNS security (DNSSEC); secure protocols only (SSH, HTTPS); service hardening (CIS Benchmarks); Traefik secure headers (HSTS, CSP, X-Frame-Options). Cloud: all cloud management communication via Tailscale WireGuard (ChaCha20-Poly1305); SSH v2 AES-256-GCM enforced on all 4 Linux cloud nodes via Ansible; TLS 1.3 for all cloud-hosted HTTPS services; all cloud nodes resolve DNS via on-premises Unbound (192.168.1.153/154) over Tailscale providing DNSSEC validation and malware domain blocking.	Implemented
A 8.22	A 13.1.3	**Segregation of Networks**	Firewall rules enforce isolation; subnet ACLs; DMZ for public-facing services; Traefik	Implemented

			backend isolation; NGINX Ingress isolates K3s pods; network topology documented; inter-VLAN traffic controlled. Cloud: per-provider network isolation enforced ; AWS VPC (172.31.0.0/16), GCP VPC (10.128.0.0/16), Azure VNet homelab-vnet2 (10.130.0.0/16) each isolated from other providers. Inter-cloud communication only via Tailscale overlay with ACL enforcement. Cloud nodes not directly routable to on-premises without Tailscale ACL authorization.	
A 8.23	NEW	**Web Filtering**	DNS-based ad-blocking (Unbound/Pi-hole); malware domain blocking (2M+ blocked domains); SafeLine WAF (OWASP CRS rules); Traefik middleware filtering; content filtering (DNS); phishing site blocking; URL reputation filtering (MISP). Cloud: all cloud nodes resolve via on-premises Unbound over Tailscale, inheriting DNS-layer malware and phishing domain blocking. GCP Cloud Armor application-level policy blocks malicious URL patterns (SQLi/XSS via preconfigured expression sets).	Implemented
A 8.24	A 10.1.1, A 10.1.2	**Use of Cryptography**	TLS 1.3 (Traefik); Ed25519 SSH keys; AES-256-GCM encryption; DNSSEC; Step-CA PKI (offline root, online intermediate); automated certificate management (ACME); strong ciphersuites only; certificate expiry monitoring; OCSP validation; encrypted backups; no weak algorithms (vulnerability scans detect). Cloud: Tailscale WireGuard (ChaCha20-Poly1305) encrypts all management traffic. AWS S3 SSE (SSE-S3) for CloudTrail logs; GCP default encryption for persistent disks and GCS buckets (Google-managed keys); Azure Managed Disks and Log Analytics workspace encrypted at rest by default. Provider-native key management used for cloud storage encryption; no customer-managed key gaps identified at current scale.	Implemented
A 8.25	A 14.2.1	**Secure Development Life Cycle**	Infrastructure as Code (Terraform, Ansible); Git version control; CI/CD security linting (planned); code review (pull requests); security requirements in deployment automation; threat modeling for new services; secure defaults; configuration validation (Ansible dry-run, Terraform plan). Cloud: Terraform plan review required before cloud infrastructure changes applied; ARM	Partial

			template parameter validation before Azure deployment; no automated SAST scanning of IaC currently implemented.	
A 8.26	A 14.1.2, A 14.1.3	**Application Security Requirements**	Security requirements defined for deployments; input validation (WAF); authentication/authorization requirements; encryption requirements (TLS 1.3 mandatory); logging requirements (100% coverage); secure configuration baselines; OWASP Top 10 mitigation strategies. Cloud: cloud nodes provisioned with no public management ports (secure default); IAM least-privilege enforced; provider-native security services enabled by default (GuardDuty, SCC, Defender for Cloud).	Implemented
A 8.27	A 14.2.5	**Secure System Architecture and Engineering Principles**	Defense-in-depth architecture; zero-trust principles (verify explicitly, least privilege, assume breach); network segmentation; layered security controls; fail-secure design; security by default; threat modeling; documented architecture diagrams; secure service design (Traefik reverse proxy, backend isolation). Cloud: Tailscale ACL-enforced mesh (default deny, explicit allow policy) extends zero-trust posture to cloud nodes. Per-provider enclave gateway model (AWS Security Groups, GCP VPC firewall policy, Azure NSG) mirrors on-premises zone-based segmentation. No implicit trust between cloud providers or between cloud and on-premises segments.	Implemented
A 8.28	NEW	**Secure Coding**	Not applicable ; minimal custom code development; reliance on vetted open-source projects; code review for any custom scripts (pull requests).	N/A
A 8.29	A 14.2.8, A 14.2.9	**Security Testing in Development and Acceptance**	Ansible dry-run testing; Terraform plan review; vulnerability scanning before production deployment (OpenVAS/Nessus); configuration validation; WSUS test deployments; snapshot-before-patch for rollback capability; staging environment testing. Cloud: Terraform plan review and ARM template validation before cloud infrastructure changes; Wazuh SCA validation run post-rebuild to confirm CIS baseline compliance; cloud node rebuild timing validated against RTO target.	Implemented
A 8.30	A 14.2.7	**Outsourced Development**	Not applicable ; no outsourced development; reliance on open-source community projects; vendor security	N/A

			assessed informally (project maturity, community support, vulnerability history).	
A 8.31	A 12.1.4, A 14.2.6	**Separation of Development, Test and Production Environments**	Separate dev/test VLANs; staging environment for patch testing (WSUS); production isolated from development; snapshot-based testing environments; environment-specific configurations (Ansible); no production data in dev/test. Cloud: cloud nodes operate in dedicated VPCs/VNets isolated from on-premises production VLAN; cloud nodes used for demonstration and learning, not production data processing.	Implemented
A 8.32	A 12.1.2, A 14.2.2, A 14.2.3, A 14.2.4	**Change Management**	Git branching strategy; code review (pull requests); snapshot-before-patch; WSUS approval workflows; Ansible change control; Terraform plan review before apply; change logging (Git commits, SIEM); rollback capability; change impact assessment; documented change procedures. Cloud: cloud infrastructure changes (Security Group rules, VPC firewall policy, NSG rules) managed via Terraform IaC with Git commit history; no ad-hoc console changes; cloud change history available via CloudTrail, GCP Audit Logs, and Azure Activity Log.	Implemented
A 8.33	A 14.3.1	**Test Information**	No production data in test environments; synthetic test data only; staging data anonymized; test data management procedures documented; production database not used for testing. Cloud: no production data processed on cloud nodes; cloud nodes contain only operational monitoring data (Wazuh telemetry, PatchMon inventory, Checkmk metrics).	Implemented
A 8.34	A 12.7.1	**Protection of Information Systems During Audit Testing**	Not applicable - personal lab.	N/A

Control Deployment Summary

Overall Statistics

Metric	Count	Percentage
Total Controls	93	100%
Implemented	55	59%
Partial	14	15%
Not Implemented	2	2%
N/A	22	24%

Applicable Controls	71	100%
Coverage (Applicable)	69	77%

Control Family Breakdown

Control Category	Total	Implemented	Partial	Not Impl.	N/A	Coverage
Organizational (5.x)	37	22	8	1	6	71%
People (6.x)	8	2	0	0	6	100%
Physical (7.x)	14	2	4	0	8	33%
Technological (8.x)	34	29	2	1	2	91%
TOTAL	93	55	14	2	22	77%

Note: Compliance scores unchanged from v1.2. Cloud integration strengthens evidence for existing compliant controls but does not open new gaps or close existing partial items.

Version History

Version	Date	Changes
1.0	January 2026	Initial assessment and summary statistics.
1.1	January 2026	Corrected N/A controls and coverage percentages.
1.2	March 2026	Minor updates and formatting corrections.
2.0	April 2026	Cloud IaaS integration (AWS, Azure, GCP - 6 nodes total). Cloud content integrated