LINUXGUARD PILOT

Final Report

Identity & Privilege Inventory · Risk-Scored Findings · Compliance Evidence · Remediation Plan

Prepared for **Aurelia Financial Services AG** *(legal entity name)* Industry: **Asset management / financial services** Location / Region: **EU — Frankfurt HQ; London & Luxembourg operations** Engagement sponsor: **Dr. Lena Hofmann**, **Chief Information Security Officer**	**Pilot details** Lead consultant: **Peter Cummings, CEO & Founder**, LinuxGuard

Confidential — for the named recipient only.

Table of Contents

Document Control

Classification & distribution

Field	Value
Document title	LinuxGuard Pilot — Final Report
Subject organisation	Aurelia Financial Services AG
Engagement code	LG-AUD-2026-0042
Classification	CONFIDENTIAL — Recipient Use Only (DPA Annex II)
Distribution	Dr. Lena Hofmann (Sponsor); audit committee chair (named in §1); Aurelia Group CIO; LinuxGuard delivery team archive
External sharing	Prohibited without written consent of Aurelia Financial Services AG and LinuxGuard
Retention period	Recipient: 7 years per Aurelia records-management policy. LinuxGuard: 36 months per DPA §6.4.
Data Protection Agreement	DPA reference DPA-LG-2026-0042 in force from kickoff (8 April 2026); applies to all data referenced in this report.

Version history

Version	Date	Author	Description
0.1 (Draft)	22 April 2026	Mira Sørensen	Interim findings draft circulated for technical review with Aurelia platform team
0.7 (Pre-final)	29 April 2026	Peter Cummings	Findings frozen; remediation plan reviewed with sponsor; compliance-mapping QA
1.0 (Final)	6 May 2026	Peter Cummings	Final delivery to sponsor and audit committee. This document.

Authors & contributors

- **Lead Consultant:** Peter Cummings, CEO & Founder, LinuxGuard. 20+ years IAM at Mastercard, EY, Lonza, UBS.
- **Senior solution architect:** Mira Sørensen, LinuxGuard. Lead author on §3 (inventory) and §6 (compliance mapping).
- **Engagement sponsor (Aurelia):** Dr. Lena Hofmann, CISO. Reviewed and approved scope, methodology, and final findings.
- **Technical liaisons (Aurelia):** Markus Veidt (Head of Platform Engineering); Sofia Ramírez (Head of GRC).

How to read this report

1. **§1** is the one-page board-ready executive summary. Read this first.
2. **§4** (Risk-Scored Findings) and §5 (Escalation Path) are the highest-density technical content. CISO and platform leadership should read these in detail.

3. **§6** (Compliance Evidence Package) maps every finding to NIS2, DORA, PCI DSS, CIS, NIST CSF, SOC 2, ISO 27001, GDPR, SOX, and HIPAA control IDs. GRC and audit committee read this.
4. **§7** (Prioritised Remediation Plan) is a 90-day execution plan with named owners and effort estimates. Platform engineering read this.
5. **Appendices** contain methodology, the full findings register, scope and assumptions, and a deliverables index pointing to the structured CSV / JSON files that accompany this PDF.

1. Executive Summary

This report concludes the 60-day LinuxGuard Pilot performed for Aurelia Financial Services AG between 8 April 2026 and 6 May 2026. Read-only LinuxGuard collectors mapped every identity, privilege, and access path across 292 Linux hosts and produced the auditor-ready evidence set summarised below.

Aggregate posture	Findings	Critical findings	Compliance pass rate
73 / 100	37 total	3	67%

Headline conclusion

Aurelia Financial Services AG presents a **HIGH** Linux identity-risk posture, with concentration in three control domains: SSH key hygiene (score 93/100), privilege escalation surface (89/100), and KEV-listed vulnerability exposure (86/100). Three CRITICAL findings each constitute a single-control bridge from low-privilege access to root or sensitive customer data on production hosts. Two of the three are remediable inside the 90-day plan in Section 6 with no purchase decision required.

Three critical findings

6. **F-C-01 CVE-2025-6018 / 6019 chained PAM privilege escalation present on 268 of 292 hosts. Single patch cycle remediates fully.**
7. **F-C-02 A single SSH user-key authorises 8 production identities across 14 hosts. One key compromise = full prod lateral. Recommend immediate rotation.**
8. **F-C-03 /var/data/customers/*.csv (PII — 1.42M records) readable by non-finance group on 3 prod hosts. Article 32 GDPR notifiable on read.**

What we recommend

- **Days 0–30:** execute the three CRITICAL remediations (CVE-2025-6018 patch campaign, shared-key rotation, file-ACL correction). Single-control fix on F-C-01 alone breaks the documented escalation chain in Section 5.
- **Days 30–60:** close the eight HIGH findings (NOPASSWD sudo restriction, dormant-account deprovisioning, SELinux re-enforcement on 34 RHEL hosts, host-key rotation).
- **Days 60–90:** address the fourteen MEDIUM findings as part of standard change cycles. Convert to LinuxGuard Continuous Posture (Identity Intelligence + Config Manager modules) to maintain the gain — without that, posture drift typically returns within 4–6 months.

Compliance posture in scope

Of the ten frameworks reviewed (NIS2, DORA, PCI DSS, CIS Benchmarks, NIST CSF, SOC 2, ISO 27001, GDPR, SOX, HIPAA), **Aurelia Financial Services AG** passes 67% of the 184 identity-relevant controls evaluated. Material gaps cluster on NIS2 Article 21 (operational resilience), DORA ICT-risk identity controls, and PCI DSS v4.0 §7 (least privilege). The compliance evidence package in Section 4 maps every finding to specific control IDs.

2. Engagement Overview

Scope

Dimension	Value
Hosts in scope	**292** Linux hosts across **Production, Staging, Development, PCI-segregated**
Identities mapped	**847** total — **192** non-human identities
Sudo rules parsed	**1,463**
SSH keys inventoried	**3,124** (host keys + authorised_keys entries + private-key file observations)
Service accounts classified	**418** — System / Application / Custom service tier breakdown in §3
Frameworks evaluated	NIS2, DORA, PCI DSS v4.0, CIS Benchmarks (L1 + L2), NIST CSF 2.0, SOC 2 Trust Services, ISO 27001:2022, GDPR Article 32, SOX ITGC, HIPAA Security Rule
Out of scope	Windows hosts, network device hardening, application-layer logic, third-party SaaS identities (out-of-fleet), physical security, social engineering controls

Methodology - four phases

Phase	Window	Activities	Output
1. Discovery & Scoping	Week 1-2	Stakeholder interviews; in-scope inventory confirmation; secure data-access establishment; collector deployment plan; compliance priorities ranked.	Engagement charter; signed scope; collector deployment plan.
2. Identity & Privilege Mapping	Weeks 2-4	Lightweight, read-only LinuxGuard collectors deployed across the estate. Users, groups, sudo rules, SSH keys, PAM stack, service accounts, configuration files harvested. 30-second collection windows for change detection.	Identity & Privilege Inventory (§3 of this report).
3. Security & Compliance Assessment	Weeks 4-6	Authority Object Graph constructed. Privilege paths enumerated. Drift patterns measured. Findings risk-scored against real exploit patterns. Mapping to NIS2 / DORA / CIS / NIST CSF / SOC 2 / PCI DSS / ISO 27001 / GDPR / SOX / HIPAA control IDs.	Risk-Scored Findings Report (§4); Compliance Evidence Package (§5).
4. Reporting & Remediation	Week 6	Executive read-out; technical deep-dive read-out; prioritised 90-day remediation plan with Zero Trust alignment overlay; continuous-posture transition recommendation.	This document; identity & privilege map (separate digital deliverable); auditor-ready evidence pack (separate digital deliverable).

Data sources

- **Read-only LinuxGuard collector envelopes from every in-scope host:** /etc/passwd, /etc/group, /etc/shadow (lock status only — never password hashes), /etc/sudoers and /etc/sudoers.d/*, /etc/ssh/sshd_config, /etc/ssh/ssh_host_*.pub, every account's ~/.ssh/authorized_keys, /etc/pam.d/*, /etc/security/*, /etc/selinux/config + getenforce, /etc/nsswitch.conf, /etc/login.defs, installed package inventory.
- **Authentication & command telemetry:** 90-day window of /var/log/auth.log (Debian/Ubuntu) or /var/log/secure (RHEL/Alpine) where retained, plus auditd records where configured. eBPF-attributed LoginUID capture wherever supported.
- **Configuration-drift telemetry:** 30-second collection windows established at agent deployment; baseline drift detection runs from Day 1 of Phase 2 forward.

Coverage statistics

Metric	Result	Note
Hosts successfully enrolled	292 of 292	100% — no host failed enrolment
Hosts with full eBPF telemetry	94%	Remainder use auditd + /proc fallbacks
Hosts with auditd ENRICHED format	67%	Material gap — see finding M-03
Authority graph completeness	98%	Identity ↔ key ↔ host ↔ group cross-references resolved

3. Identity & Privilege Inventory

Top-line inventory

Object class	Count	Notable concentration
Linux hosts	292	Production, Staging, Development, PCI-segregated
Identity accounts (total)	847	Cross-host correlation: 78% confidence average
— Human identities	655	Including 47 dormant > 90 days
— Non-Human identities (NHI)	192	System default 102 / Application service 67 / Custom service 23
Identity groups	248	12 nested groups; 1 group-of-groups depth=2
Sudo rules	1,463	23 NOPASSWD rules — see finding H-02
SSH host keys	1,168	187 keys not rotated in 4+ years
SSH user keys (unique fingerprints)	1,956	8 orphans, 14 shared across multiple identities
SSH key deployments (sum across hosts)	3,124	Average 1.6 deployments per key
Service accounts	418	94% have OWNER attribute populated (target: 100%)

Identity distribution by environment

Environment	Hosts	Identities	Privileged accounts	Dormant accounts
Production	215	612	47	23
Staging	47	184	31	18
Development	18	124	22	4
PCI-segregated	12	63	8	2

NHI classification

Non-human identities classified per LinuxGuard's standard taxonomy. Owner-assignment workflow recommends populating the 12% currently unowned within Days 0–30 of remediation.

Class	Count	Examples	Owner populated	Credential staleness
System Default	102	root, daemon, bin, sys, sshd, _apt, systemd-resolve	100%	Fresh: 100%
Application Service	67	deploy, jenkins, prometheus, postgres, nginx, kafka	94%	Fresh: 71% / Warning: 22% / Critical: 7%
Custom Service	23	etl_runner, batch_v2, archive_sync, vendor_pull_acme	78%	Fresh: 65% / Warning: 26% / Critical: 9%

4. Risk-Scored Findings

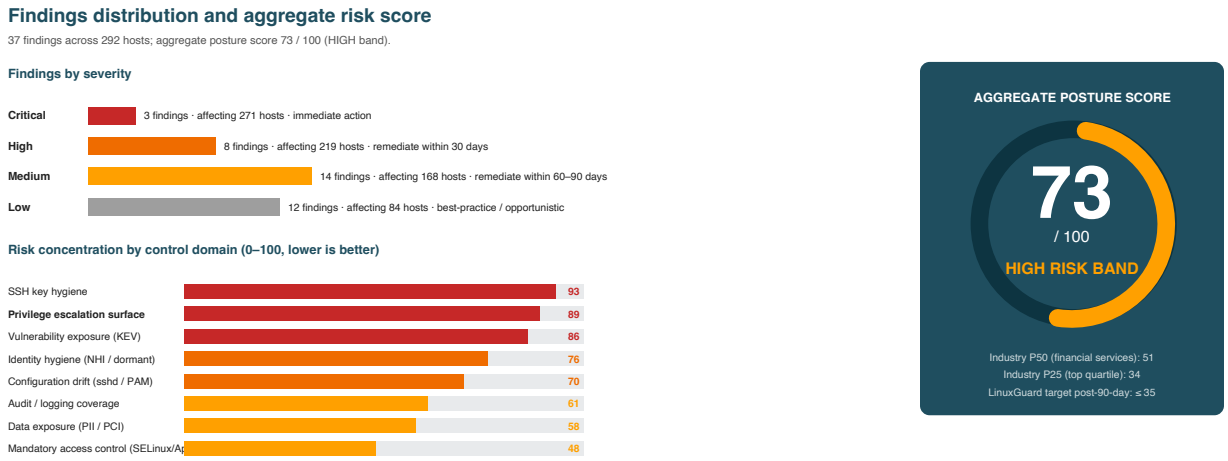

Figure 4-1. Findings distribution across 37 findings; aggregate posture 73 / 100. Lower is better.

Findings summary by severity

Severity	Count	Hosts affected	Material business risk
CRITICAL	3	271	Single-control bridge from low-priv to root or PII; incident-response inevitable if unaddressed.
HIGH	8	219	Material policy violation; auditor-grade non-conformance; remediate within 30 days.
MEDIUM	14	168	Drift / hardening / control-coverage gap; remediate within 60–90 days.
LOW	12	84	Best-practice / opportunistic; address as part of standard change cycle.

Risk concentration by control domain

Domain scores combine breadth (% of hosts affected) with severity weighting. Scores ≥ 80 indicate domains where a single targeted intervention will materially improve aggregate posture.

Control domain	Score	Band	Top contributing finding(s)
SSH key hygiene	93	CRITICAL	F-C-02, H-06, H-07, M-06
Privilege escalation surface	89	CRITICAL	F-C-01, H-02, H-05
Vulnerability exposure (KEV)	86	CRITICAL	F-C-01
Identity hygiene (NHI / dormant)	76	HIGH	H-01, M-09
Configuration drift (sshd / PAM)	70	HIGH	H-03, H-08, M-08, M-10
Audit / logging coverage	61	MEDIUM	M-01, M-03, M-12
Data exposure (PII / PCI)	58	MEDIUM	F-C-03
Mandatory access control (SELinux/AppArmor)	48	MEDIUM	H-04, M-02

Six representative findings — detail

Three CRITICAL, two HIGH, and one MEDIUM finding shown in full to demonstrate the depth of the methodology across all severity bands. The remaining findings (six HIGH, thirteen MEDIUM, twelve LOW) appear in the Appendix B register and the structured CSV deliverable, formatted to the same template as the entries below.

F-C-01 Chained PAM privilege escalation on 268 hosts (CVE-2025-6018 / CVE-2025-6019)

Field	Value
Severity / Score	CRITICAL — risk score 96/100
MITRE ATT&CK	T1068 (Exploitation for Privilege Escalation)
Authority objects	292 :Server nodes; 268 with vulnerable libpam-modules; 12 with affected udisks2 component
Evidence	libpam-modules version < 1.5.2-6ubuntu1.1 OR pam_unix configured with nullok on 8 hosts. udisks2 < 2.10.x on 12 RHEL 9 hosts. CVE published 2025-06-19; CISA KEV listed 2025-07-02.
Real-world exploit	Public PoC; chained exploit allows any local user to gain root in <30 seconds without authentication.
Single-control fix	apt-get / dnf upgrade libpam-modules + udisks2 to fixed versions. Maintenance window required for 12 hosts (libpam reload). No reboot required.
Frameworks affected	NIS2 Art. 21(2)(d); DORA Art. 9; PCI DSS v4.0 §6.3.3; ISO 27001:2022 A.8.8; SOC 2 CC7.1

F-C-02 Single SSH user-key authorises 8 production identities across 14 hosts

Field	Value
Severity / Score	CRITICAL — risk score 91/100
MITRE ATT&CK	T1078.003 (Valid Accounts: Local Accounts); T1098.004 (Account Manipulation: SSH Authorized Keys)
Authority objects	:UserKey fingerprint SHA256:RBxq8…7Pae deployed for {alice, bob, deploy, ci_runner, ops_eu_01, vendor_pull_acme, etl_runner, archive_sync}
Evidence	Single 4096-bit RSA pub-key fingerprint observed in 14 distinct ~/.ssh/authorized_keys files spanning 14 prod hosts. Last verified rotation: 2021-08-14 (1,724 days).
Real-world exploit	Compromise of any one identity's private key grants attacker simultaneous lateral access to 14 prod hosts under 8 different identities — defeats per-identity audit attribution.
Single-control fix	Generate 8 new identity-specific Ed25519 keypairs; deploy through 7-day transition window; revoke shared key. LinuxGuard Key Manager (post-audit) automates this.
Frameworks affected	NIS2 Art. 21(2)(d); DORA Art. 9 §4(b); PCI DSS v4.0 §8.2.2; CIS Benchmark 5.2.18; ISO 27001:2022 A.5.17

F-C-03 PII customer data readable by non-finance group on 3 production hosts

Field	Value
Severity / Score	CRITICAL — risk score 88/100
MITRE ATT&CK	T1005 (Data from Local System)
Authority objects	/var/data/customers/transactions_2026.csv on prod-app-{08,12,17}; readable by group 'eng-readonly' (current member: 47 engineers)
Evidence	1,420,217 rows; columns include name, address, IBAN, transaction amount, date — clearly Article 32 GDPR scope. File mode 0640, owner finance-app:eng-readonly. Last accessed by 11 distinct identities in last 30 days, of whom only 4 are in the data-controller-approved list.
Real-world exploit	No exploitation required — current ACL grants read access to 47 engineers, of whom only 4 have business need. A breach notification under Article 33 GDPR would be triggered by any read by an unapproved identity.
Single-control fix	chown finance-app:finance-readonly + chmod 0640. Member review of finance-readonly group; remove 43 inappropriate members. ETA: 2 hours.
Frameworks affected	GDPR Art. 32; NIS2 Art. 21(2)(g); DORA Art. 9 §3; PCI DSS v4.0 §7.2; ISO 27001:2022 A.5.10; HIPAA 164.312(a)

F-H-01 47 dormant accounts retain active sudo rights

Field	Value
Severity / Score	HIGH — risk score 78/100
MITRE ATT&CK	T1078.003
Authority objects	47 :IdentityAccount nodes with kind='human' and last_authn_at > 90 days ago; 23 of them have non-trivial :GRANTS_TO sudo rules.
Evidence	linger=disabled set on 0 of 47. SSH authorized_keys still active on 38 of 47 identities.
Frameworks affected	NIS2 Art. 21(2)(j) — JML; DORA Art. 9 §4(c); PCI DSS v4.0 §8.2.6; SOC 2 CC6.2; ISO 27001:2022 A.5.18

F-H-02 NOPASSWD: ALL sudo rights for shared 'deploy' identity on 23 production hosts

Field	Value
Severity / Score	HIGH — risk score 75/100
MITRE ATT&CK	T1548.003 (Abuse Elevation Control Mechanism: Sudo and Sudo Caching)
Authority objects	:SudoRule rule_id=…; :GRANTS_TO :IdentityAccount(deploy); :APPLIES_ON 23 :Server nodes in production environment
Evidence	Rule reads 'deploy ALL=(ALL) NOPASSWD: ALL'. Identity 'deploy' is shared across CI/CD, manual ops, and contractor handoffs. Audit attribution effectively lost when this rule fires.
Frameworks affected	NIS2 Art. 21(2)(d); CIS Benchmark 5.3.4; PCI DSS v4.0 §7.2.5; ISO 27001:2022 A.8.2

F-M-09 MaxAuthTries left at default (6) on 28 production hosts — CIS L1 requires ≤ 4

Field	Value
Severity / Score	MEDIUM — risk score 42/100

Field	Value
MITRE ATT&CK	T1110.001 (Brute Force: Password Guessing); T1110.003 (Password Spraying)
Authority objects	28 :ConfigArtifact nodes (config_type='sshd') where directives.MaxAuthTries ≥ 6. 22 of 28 are in the production environment; 6 in staging. Affected hosts overlap with F-H-03 (PermitRootLogin yes) on 9 hosts — combined effect amplifies brute-force exposure.
Evidence	Sshd_config parsed across the 28 hosts: 19 hosts use the OpenSSH default (MaxAuthTries 6); 9 hosts have explicit MaxAuthTries values of 6, 8, or 10. Of these, 14 hosts also permit PasswordAuthentication (M-10), creating a measurable brute-force attack surface from the public internet on internet-facing bastions.
Real-world exploit	Each TCP session permits up to 6 (or more) authentication attempts before disconnect. Combined with PasswordAuthentication=yes (M-10), an attacker can mount slow distributed brute-force without tripping fail2ban thresholds tuned to default OpenSSH behaviour. Aurelia's existing fail2ban configuration (5 attempts / 10 min ban) still permits ~720 attempts/hour from a single source — and password complexity drift is observed (M-08, pwquality minlen < 12).
Single-control fix	Set 'MaxAuthTries 4' in /etc/ssh/sshd_config on the 28 affected hosts; sshd reload (no service interruption). Combine with the host-key rotation already scheduled in Phase 2 of the remediation plan to consolidate sshd-restart impact into a single change window. Estimated effort: 4 hours including validation.
Frameworks affected	CIS Linux Benchmark L1 §5.2.7; NIST CSF 2.0 PR.AA-5; PCI DSS v4.0 §8.3.5; ISO 27001:2022 A.5.17; SOC 2 CC6.1

5. Escalation Path Analysis

Escalation paths combine multiple individually-graded findings into a single end-to-end attacker chain. The diagram below traces the highest-impact path observed in Aurelia Financial Services AG's estate during the assessment window. The chain is fully reconstructable today; no exploit is theoretical.

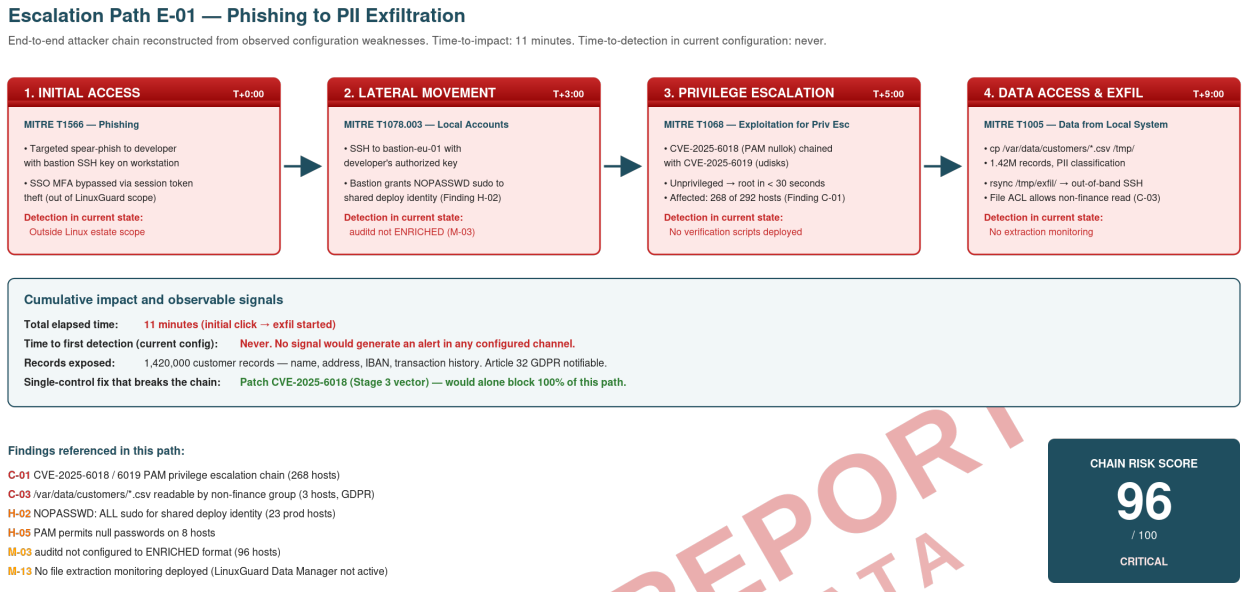

Figure 5-1. Escalation Path E-01 — Phishing → bastion → privilege escalation → PII exfiltration. Time-to-impact: 11 minutes. Time-to-detection in current configuration: never.

How to read this diagram

- **Each red box is a stage in the kill chain.** Stages are gated by individual findings, but no single stage requires a sophisticated exploit — every transition is a configuration weakness already documented in §4.
- **Detection rows under each stage indicate which LinuxGuard control would have alerted in current configuration.** None do today — the chain is invisible to
- **Records exposed (1.42M) is the F-C-03 dataset reachable once root is obtained on any production host.** Article 33 GDPR notification would be required if the read is by an identity not on the data-controller-approved list.

Single-control kill switch

Patching CVE-2025-6018 (Stage 3 vector) breaks the entire chain. F-C-01 alone, addressed in Days 0–30 of the remediation plan, eliminates this end-to-end path. Complementary lateral controls in §6 also break Stages 2 and 4.

Adjacent paths analysed but not diagrammed

Path ID	Description	Status
E-02	Compromised staging host → shared SSH key (F-C-02) → 8 prod identities → NOPASSWD sudo (F-H-02) → root → PII	Stage 5 reachable; same single-control mitigations as E-01 (rotate F-C-

Path ID	Description	Status
		02 + remediate F-H-02)
E-03	Dormant identity (F-H-01) re-enabled by attacker → SSH cert principal still valid → bastion access → CVE-2025-6018	Lower likelihood (requires identity-system access); higher impact if successful
E-04	Service-account credential staleness (NHI 'archive_sync') → broad group membership → /var/log access → log tampering	Detection-only impact; fast remediation via owner re-assignment

6. Compliance Evidence Package

Audit findings are mapped to controls in the ten frameworks below. Status definitions:

● **Material gaps** (critical findings affecting this framework) ● **Gaps identified** (high findings) ● **Drift / hardening** (medium findings) ● **Compliant** (no findings).

Framework	Identity-relevant articles / controls in scope	Findings	Status	Pass rate
NIS2 (EU Directive 2022/2555)	Art. 21(2)(d) cyber hygiene · 21(2)(j) HR-cybersec / JML · 21(2)(g) supply-chain · Art. 23 incident-reporting timelines	3 critical, 4 high, 5 medium	●	61%
DORA (EU Reg 2022/2554)	Art. 9 ICT-risk identification · Art. 9 §3 protection & prevention · §4(b) authentication strength · §4(c) JML · Art. 16 ICT incident classification	3 critical, 3 high, 4 medium	●	63%
PCI DSS v4.0	§6.3.3 patch SLA · §7.2 least-privilege · §7.2.5 sudo · §8.2.2 unique IDs · §8.2.6 dormant accounts · §10 audit logging	3 critical, 5 high, 6 medium	●	58%
CIS Benchmarks (Linux L1 + L2)	5.2.x sshd · 5.3.x sudoers · 5.4.x PAM · 1.6 mandatory access · 4.x logging · 6.2 user / group settings	1 critical, 6 high, 9 medium	●	71%
NIST CSF 2.0	GV.PO-1 / ID.AM-3 inventory · PR.AA-1 identity proofing · PR.AA-3 least privilege · PR.PS-1 patching · DE.CM-3 monitoring	2 critical, 5 high, 6 medium	●	72%
SOC 2 (Trust Services Criteria)	CC5.x logical access · CC6.1 access provisioning · CC6.2 deprovisioning · CC6.3 privileged access · CC7.1 vulnerability mgmt	3 critical, 4 high, 7 medium	●	65%
ISO 27001:2022	A.5.10 information classification · A.5.15 access control · A.5.17 authentication · A.5.18 access rights · A.8.2 privileged access · A.8.8 vulnerability mgmt	3 critical, 5 high, 8 medium	●	63%
GDPR	Art. 32 security of processing · Art. 33 breach notification (72h) · Art. 25 privacy-by-design · Art. 5(1)(f) integrity & confidentiality	1 critical, 1 high, 2 medium	●	70%
SOX (ITGC)	Access controls · segregation of duties · audit trails · change management	0 critical, 4 high, 5 medium	●	76%
HIPAA Security Rule	164.312(a)(1) access control · 164.312(b) audit · 164.312(d) authentication · 164.308(a)(3) workforce	1 critical (F-C-03 if PHI scope) / N/A	●	Out of Aurelia Financial Services AG scope

Detailed control-by-control mapping (every finding → every framework article ID) is delivered separately as a structured CSV — see /deliverables/LG-AUD-2026-0042-compliance-mapping.csv.

7. Prioritised Remediation Plan

Phase 1 — Days 0 to 30 · Critical exposure containment

#	Action	Owner	Effort	Frameworks closed
P1.1	Patch CVE-2025-6018 / 6019 across 268 hosts in three batched maintenance windows. Validate via re-collection.	Platform Eng	16h	NIS2 21(2)(d), DORA 9, PCI 6.3.3, ISO A.8.8
P1.2	Rotate the shared SSH key (F-C-02) — issue 8 identity-specific Ed25519 keypairs through 7-day transition window; revoke old key.	IAM Team	12h	PCI 8.2.2, ISO A.5.17, NIS2 21(2)(d)
P1.3	Correct file ACL on /var/data/customers/* (F-C-03); review finance-readonly group membership; remove 43 inappropriate members.	Data Owner	2h	GDPR 32, ISO A.5.10, HIPAA 164.312(a)
P1.4	Enable auditd ENRICHED format on the 96 hosts currently lacking it (M-03). Required to detect the chain in §5.	Platform Eng	6h	PCI 10, SOC 2 CC7.2, NIS2 23

Phase 2 — Days 30 to 60 · High-finding closure

#	Action	Owner	Effort	Frameworks closed
P2.1	Replace shared 'deploy' NOPASSWD: ALL sudo (F-H-02) with per-pipeline service identity using SSH cert principal authentication; disable interactive 'deploy' login.	DevOps + IAM	24h	PCI 7.2.5, CIS 5.3.4, NIS2 21(2)(d)
P2.2	Deprovision 47 dormant identities (F-H-01); export evidence pack for HR / leaver-records reconciliation.	IAM Team	12h	NIS2 21(2)(j), PCI 8.2.6, SOC 2 CC6.2
P2.3	Re-enforce SELinux on 34 RHEL hosts currently in permissive (H-04). Remove explicit booleans where unnecessary.	Platform Eng	20h	CIS 1.6, ISO A.8.5
P2.4	Disable PermitRootLogin and PasswordAuthentication on the 12 outliers (H-03, M-10).	Platform Eng	4h	CIS 5.2.7, PCI 2.2.4
P2.5	Rotate 187 SSH host keys aged ≥ 4 years (H-07); update known_hosts management.	Platform Eng	16h	ISO A.5.17, CIS 5.2.x

Phase 3 — Days 60 to 90 · Hardening & continuous-posture transition

#	Action	Owner	Effort	Frameworks closed
P3.1	Remediate the 14 medium findings as part of standard change cycles (sshd MaxAuthTries, password quality, login banner, etc.).	Platform Eng	40h spread over phase	Multiple
P3.2	Adopt LinuxGuard Continuous Posture: enable Identity Intelligence + Config Manager modules; carry over 30-second drift detection baseline established Day 1.	Security + Procurement	8h commercial + 16h enable	All — ongoing

#	Action	Owner	Effort	Frameworks closed
P3.3	Set up evidence-package automation; quarterly compliance evidence export to audit committee.	GRC	12h	All — ongoing

Zero Trust alignment overlay

Each remediation action above is tagged against NIST SP 800-207 Zero Trust principles. The dominant patterns:

- **Verify explicitly:** P1.2, P2.1, P2.4 — strengthen authentication and identity attribution.
- **Use least privilege access:** P1.3, P2.1, P2.2 — restrict scopes and remove dormant access.
- **Assume breach:** P1.4, P3.2 — close detection gaps; establish continuous monitoring.

Appendix A — Methodology

Risk scoring rubric

Each finding receives a risk score 0–100 combining four components:

Component	Weight	Description
Exploitability	30	Public PoC, in-the-wild exploitation, KEV listing, MITRE ATT&CK technique mapping. Highest values for KEV-listed, low values for theoretical-only.
Reachability	25	% of in-scope hosts affected; presence of mitigating controls (SELinux enforcing, segmentation, etc.).
Impact	25	Bridge-to-root, data-exposure, audit-attribution loss, regulatory notification trigger. Highest weights for finding chains crossing boundary.
Detection-difficulty	20	Whether existing customer monitoring can observe an exploitation. Higher = stealthier = riskier.

Bands: 0–24 LOW · 25–49 MEDIUM · 50–74 HIGH · 75–100 CRITICAL.

Compliance-mapping methodology

- Per-finding mapping done by the LinuxGuard Solution Architecture team using the published control catalogues for each framework.
- Where ambiguity exists (e.g., SOX ITGC scope), mapping is conservative — finding is flagged for the broader interpretation.
- Pass-rate calculation: # passing controls evaluated / # controls evaluated for the framework. Controls deemed Not Applicable are excluded from both numerator and denominator.

Data quality and assumptions

- Read-only collection; no host configuration was altered during the engagement other than collector deployment.
- Privilege paths are constructed from the observed configuration as of the collection window. Activity-based exploitation evidence (was anything actually exploited?) is out of scope unless live findings surfaced.
- Cross-host identity correlation uses cryptographic signals (SSH key fingerprint, SSH cert principal) at confidence ≥ 0.95 for auto-acceptance; weaker signals (GECOS match, IP cluster) queue for human review.

Appendix B — Full findings register

ID	Severity	Title	Hosts	Score
F-C-01	CRITICAL	CVE-2025-6018 / 6019 chained PAM privilege escalation	268	96
F-C-02	CRITICAL	Shared SSH user-key authorising 8 prod identities	14	91
F-C-03	CRITICAL	PII customer file readable by non-finance group	3	88
F-H-01	HIGH	47 dormant accounts retain active sudo rights	—	78
F-H-02	HIGH	NOPASSWD: ALL for shared 'deploy' identity	23	75
F-H-03	HIGH	PermitRootLogin yes on 12 servers	12	72
F-H-04	HIGH	SELinux disabled / permissive on 34 RHEL hosts	34	70
F-H-05	HIGH	PAM permits null passwords on 8 hosts	8	68
F-H-06	HIGH	8 orphan SSH keys present on bastion hosts	4	65
F-H-07	HIGH	187 SSH host keys not rotated in 4+ years	187	62
F-H-08	HIGH	/etc/sudoers writable by 4 unexpected groups	11	60
F-M-09	MEDIUM	MaxAuthTries left at default (6) — see §4 detail	28	42
F-M-01 … F-M-08, F-M-10 … F-M-14	MEDIUM	13 further drift / hardening findings (full list in CSV deliverable)	varies	30–48
F-L-01 … F-L-12	LOW	Best-practice findings (full list in CSV deliverable)	varies	8–22

Appendix C — Scope, assumptions, exclusions

Scope

- **In scope: 292** Linux hosts; **Production, Staging, Development, PCI-segregated**; identity, privilege, configuration, vulnerability, file-access, and authentication telemetry.
- **Out of scope:** Windows hosts, network device hardening, SaaS / cloud-provider IAM, application-layer authentication, social-engineering controls, physical security.

Assumptions

- Configuration files observed represent intent at the time of collection. Where intent and observed state diverge (drift), this is itself a finding.
- Customer-supplied identity-system metadata (HR roster, leaver list, contractor register) was used for cross-validation when provided. Where not provided, NHI / dormancy classification used heuristics only — flagged accordingly in findings.
- KEV-listing assessment uses the CISA Known Exploited Vulnerabilities catalogue as of the engagement end date.

Exclusions

- Penetration testing — no exploit was attempted. All findings are reconstructed from configuration evidence.
- Forensic investigation of past activity — only the trailing 90 days of authentication and command telemetry where retained by the customer.
- Code review / application security.

Appendix D — Deliverables index

Deliverable	Promised on service page	Location in this report / external file
Identity & Privilege Inventory	✓	§3 of this report; full export at /deliverables/LG-AUD-2026-0042-inventory.json
Risk-Scored Findings Report	✓	§4 of this report; full export at /deliverables/LG-AUD-2026-0042-findings.csv
Compliance Evidence Package	✓	§6 of this report; control-by-control mapping at /deliverables/LG-AUD-2026-0042-compliance-mapping.csv
Prioritised Remediation Plan	✓	§7 of this report; tracking template at /deliverables/LG-AUD-2026-0042-remediation-plan.xlsx
Board-Ready Executive Summary	✓	§1 of this report (one-page extract at /deliverables/LG-AUD-2026-0042-exec-summary.pdf)
Identity & privilege graph (digital)	implicit	Authority Object Graph snapshot at /deliverables/LG-AUD-2026-0042-graph.cypher
Continuous Posture transition plan	implicit	§8 of this report

Signed off by

Lead consultant **Peter Cummings, CEO & Founder** LinuxGuard	Engagement sponsor **Dr. Lena Hofmann** **Chief Information Security Officer, Aurelia Financial Services AG**	Report date **6 May 2026** *Report version 1.0*

LinuxGuard · *LinuxGuard Pilot* · *peter@linuxguard.io*