R2SecuViro™ Security Standard

Rev2IT Secure Virtual & Infrastructure Operating Standard

Document ID: R2-RSV-STD-001
Version: 1.0
Status: Proprietary
Owner: Rev2Group (Pty) Ltd
Classification: Client-Facing / Controlled Distribution

LEGAL & IP NOTICE

---

1. Scope & Applicability

R2SecuViro™ applies to:

- Linux-based systems
- Virtualized, cloud, and on-prem infrastructure
- Environments processing **regulated, sensitive, or business-critical data**
- MSP-managed and co-managed environments

It is **not** a replacement for PCI-DSS, CIS or NIST, but a **unifying operational standard** aligned to all and designed to include Linux regulatory operation of systems within the Rev2IT SecuViro environments.

---

2. Design Principles

1. **Evidence over policy**
2. **Default-deny everywhere**
3. **Least privilege always**
4. **Secure by construction, not by exception**

5. **Linux-first, vendor-neutral**
6. **No shared trust, no shared credentials**

---

3. R2SecuViro Control Domains

Domain ID	Domain Name
RS-01	Governance, Risk & Accountability
RS-02	Asset, Data & Classification
RS-03	Identity & Access Control
RS-04	Secure Configuration Management
RS-05	Network & Perimeter Security
RS-06	System Hardening & Application Security
RS-07	Logging, Monitoring & Detection
RS-08	Vulnerability & Patch Management
RS-09	Incident Response & Recovery
RS-10	Assurance, Audit & Continuous Compliance

---

4. Control Definition Format (ISO-Style)

Each control SHALL include:

- **Control ID**
- **Control Statement (SHALL)**
- **Rationale**
- **Implementation Requirements**
- **Audit Evidence**
- **Mapped Standards**

---

5. Core Controls (Excerpt)

RS-03 – Identity & Access Control

RS-03.1 – Unique Identity Enforcement

Control Statement
All users, administrators, and services SHALL be uniquely identifiable.

Implementation Requirements

- No shared accounts
- Service accounts non-interactive
- MFA mandatory for interactive access
- SSH key-based authentication preferred

Audit Evidence

- IAM export
- MFA enforcement proof
- Account review records

RS-03.4 – Privileged Access Control

Control Statement
Administrative access SHALL be logged, and explicitly approved.

Implementation Requirements

- sudo with logging
- No direct root login
- Privilege escalation justification required

Audit Evidence

- sudo logs
- PAM configuration

- Access approval records

---

6. Security Maturity Tiers

Tier	Name	Description
Tier 1	Baseline	Foundational security
Tier 2	Controlled	PCI-equivalent
Tier 3	Hardened	CIS, NIST-aligned
Tier 4	Resilient	High-threat, high-availability

Tier is assigned per environment, not per company.

---

7. CONTROL-MAPPING APPENDIX (Excerpt)

Appendix A – Standards Alignment

R2SecuViro	NIST 800	PCI-DSS 4.0
RS-01.1 Risk Assessment	RA-3	12.2
RS-02.3 Data Protection	MP-7	3.5
RS-03.1 Identity Uniqueness	IA-2, IA-4	8.2
RS-05.2 Segmentation	SC-7	1.2
RS-07.1 Logging	AU-2, AU-6	10.2
RS-08.2 Vulnerability Scanning	RA-5	11.3
RS-09.1 Incident Response	IR-4	12.10

---

8. R2SecuViro ASSESSMENT CHECKLIST

Identity & Access

- All accounts uniquely assigned
- MFA enforced
- No root SSH access
- Quarterly access review completed

System Security

- CIS-aligned hardening applied
- Unused services disabled
- Kernel parameters hardened

Network

- Default-deny firewall
- Segmentation documented
- Bastion access enforced

Logging

- Central log collection
- 3+ month log retention (Tier 3+)
- Time sync enforced

Vulnerability

- Monthly patching
- Quarterly scans
- Risk-based remediation

Each item maps directly to a **control ID**.

9. R2SecuViro-Compliant Linux Baseline

Mandatory Configuration

Access

- SSH keys only
- MFA for sudo
- Fail2ban / sshguard or equivalent
- PAM hardening

OS Hardening

- SELinux / AppArmor enforcing
- sysctl hardened
- No GUI
- Minimal packages

Logging

- journald persistent
- rsyslog forwarding
- Immutable logs for (Tier 3+)

Network

- nftables default-deny
- Management plane isolated
- No public admin access

Change Control

- Immutable infrastructure preferred
- Drift detection mandatory (Tier 3+)

---

10. Incident Response Model

- Detection
- Containment
- Eradication
- Recovery
- Post-Incident Review (mandatory)