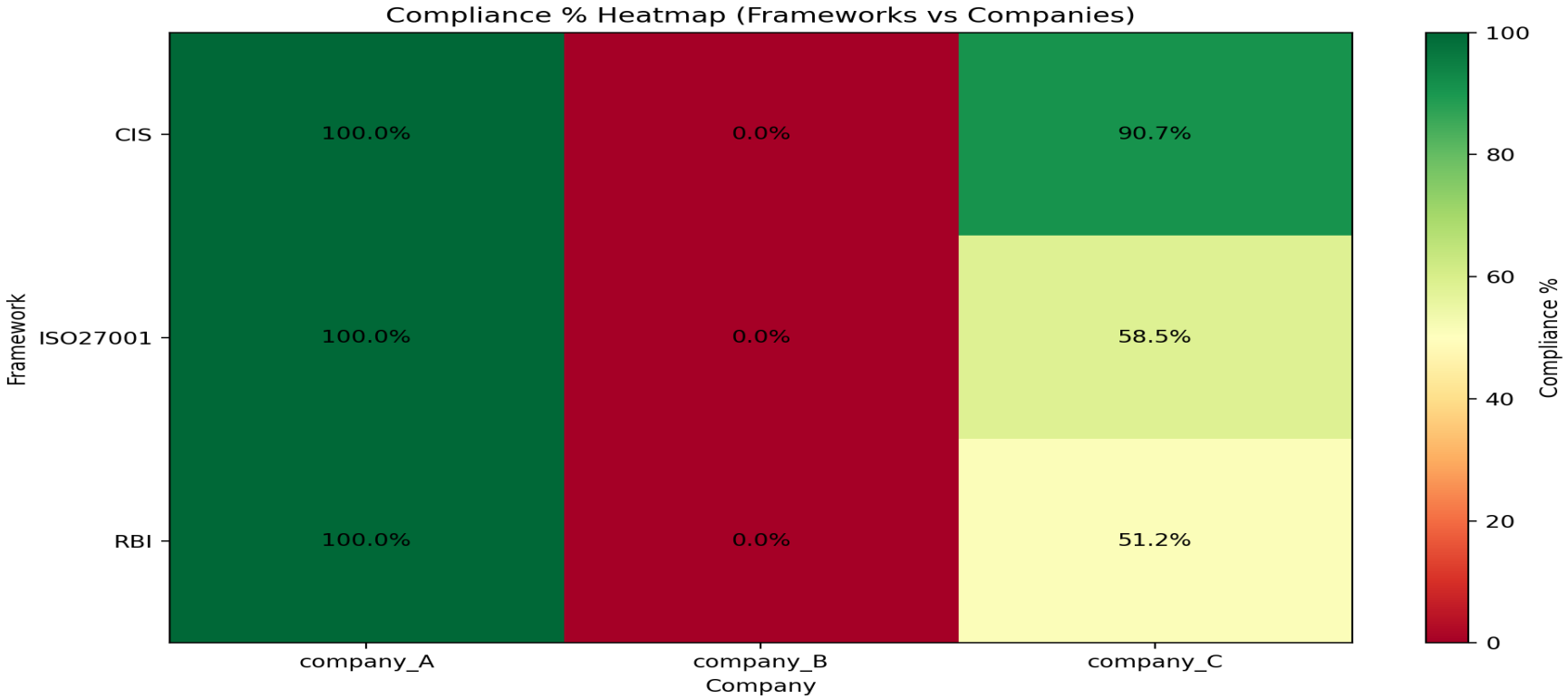
Compliance Automation Report

Generated: 2025-09-03T09:54:09.642797Z

Company	CIS	ISO27001	RBI
company_A	100.0%	100.0%	100.0%
company_B	0.0%	0.0%	0.0%
company_C	90.7%	58.5%	51.2%

Heatmap: Compliance % (Frameworks vs Companies)



Top Non-Compliant Rules & Remediations

[CIS] CIS-1 — Minimum password length >= 12

Remediation: Set system password policy minimum length to 12 or more.

[CIS] CIS-10 — Audit rules present (auditd)

Remediation: Configure audit rules for critical files and processes.

[CIS] CIS-2 — Password complexity required

Remediation: Enable password complexity (upper/lower/digit/special) in PAM/AD policies.

[CIS] CIS-3 — Firewall enabled

Remediation: Enable host/network firewall and ensure default deny rules are applied.

[CIS] CIS-4 — Audit logging enabled

Remediation: Enable auditd or Windows Event forwarders to central SIEM.

[CIS] CIS-5 — Disk encryption enabled

Remediation: Enable LUKS/BitLocker or full-disk encryption for servers with sensitive data.

[CIS] CIS-5 — Disk encryption enabled

Remediation: Enable LUKS/BitLocker or full-disk encryption for servers with sensitive data.

[CIS] CIS-6 — No insecure services like ftp running

Remediation: Stop and remove FTP service; use SFTP or secure alternatives.

[CIS] CIS-7 — SSH root login disabled

Remediation: Set PermitRootLogin no in /etc/ssh/sshd_config and restart sshd.

[CIS] CIS-8 — OS patch age <= 30 days

Remediation: Ensure systems are patched automatically or within 30 days via patch management.

[CIS] CIS-9 — Open DB ports not public (3306 not in open_ports)

Remediation: Close public DB ports or restrict via security groups/firewall.

[ISO27001] ISO-1 — Access reviews performed within 90 days

Remediation: Schedule and record access reviews every <= 90 days.

[ISO27001] ISO-1 — Access reviews performed within 90 days

Remediation: Schedule and record access reviews every <= 90 days.

[ISO27001] ISO-10 — Third-party/vendor risk assessments done

Remediation: Perform vendor risk reviews and track remediation.

[ISO27001] ISO-10 — Third-party/vendor risk assessments done

Remediation: Perform vendor risk reviews and track remediation.

[ISO27001] ISO-2 — Data backup policy exists and tested

Remediation: Implement backup policy and run restore tests periodically.

[ISO27001] ISO-3 — Incident response plan exists

Remediation: Draft & publish an incident response playbook and owner matrix.

[ISO27001] ISO-4 — Incident response tested in last 12 months

Remediation: Conduct IR tabletop/exercise within last 12 months.

[ISO27001] ISO-4 — Incident response tested in last 12 months

Remediation: Conduct IR tabletop/exercise within last 12 months.

[ISO27001] ISO-5 — Endpoint protection (AV) running

Remediation: Deploy endpoint protection on all servers/workstations.