SECURITY CONTROL MAPPING + NETWORK SECURITY CONTROL

Definition: Security Control Mapping

- It is also called "**Automapping**", "**Cross-walking**" of **Security controls.**
- Security Control Mapping is a systematic process used to align and link an organization's technical defenses with multiple security rule-books (frameworks) and threats.
- It takes complex requirements from different sources and translates them into a single, unified list of actions.

Why We Need It: The "Write a policy once and Implement it and Test it once" Approach [Link]

Security control mapping allows an organization to write a security policy once, implement it once, test it once, and use the same evidence to comply with multiple frameworks like NIST, ISO 27001, and CIS.

Currently, organizations faces a major efficiency problem that this project solves:

- **Translating "Framework Speak":** Different frameworks ask for the same thing using different names. For example, a **Firewall** is called *PR.AC-5* by NIST but *CC6.1* by SOC 2. Mapping creates a **common language**.
- **Eliminating Double Work:** Without mapping, teams often waste time implementing the same security feature multiple times to satisfy different auditors.
- **Efficiency Gain:** By mapping controls, an organization can reduce its total compliance workload because one technical setup now covers four different certifications.
- **Closing Security Gaps:** It ensures that every technical tool (like a **VPN** or **IDS**) actually maps back to a real-world threat, like **unauthorized access** or **malware**.

Project Scope

This **report** specifically maps **four major frameworks** across **five critical network controls**:

Frameworks

- NIST
- ISO
- CIS
- SOC2

Security controls

- Firewalls
- VPN's
- IDS/IPS
- Network segmentation
- Traffic monitoring

SECTION 1 FRAMEWORK ANALYSIS

1.1 Purpose: Understand all frameworks and their requirements before implementing them in any organization.
1.2 Different frameworks: This report includes NIST, ISO, CIS, SOC2 security frameworks.

A. NIST CSF (Cybersecurity Framework 2.0) [Link] It is risk-based with six functions: **Govern (GV)**, Identify (ID),
Protect (PR), Detect (DE), Respond (RS) and Recover (RC)

- A voluntary framework developed by National Institute of Standards and Technology (NIST), NIST CSF establishes a common language, or taxonomy, that organizations can use to discuss Cybersecurity with internal and external parties.
- No formal certification required.
- Focus: USA-focus (Government + Enterprise)

B. ISO 27001 (2022) [Link]

- ISO 27001 mandates an Information Security Management System (ISMS) with 93 Annex A controls across organizational, people, physical, and technical themes.
- Requires certification audit.
- International operations → ISO 27001 required

C. CIS Controls V8 [Link]

- CIS Controls V8.1 offers 18 prioritized safeguards in three Implementation Groups (IG1 basic, IG2 progressive, IG3 expert).
- Focuses on highest-impact defenses first.

D. SOC2 [Link]

- Trust Services Criteria (Security, Availability, Integrity, Confidentiality, Privacy).
- SOC2 is a third-party attestation often required by B2B SaaS companies and cloud providers for audit reports.

1.3 Overlaps

Purpose: Proves one unified implementation per control area satisfies NIST CSF, ISO 27001, CIS Controls, AND SOC2 simultaneously—eliminating redundant implementations and reducing compliance effort by 75% across all five control categories.

Control Area	NIST CSF	ISO 27001	CIS Controls	SOC 2
Firewalls	PR.AC-5	A.13.1	Control 12	CC6.1
IDS/IPS	DE.AE-1	A.8.16	Control 8	CC7.2
Segmentation	PR.AC-5	A.13.1.3	Control 12	CC6.6

VPNs	PR.AC-3	A.9.1.2	Control 4	CC6.2
Traffic Monitoring	PR.PT-4	A.12.4	Control 13	CC7.1

Table 1: *Overlapping metrics of each security framework*

What this **Table 1** shows: When **ALL FOUR frameworks** require **firewalls**, they use different "**control names**" but mean the **SAME THING**. **Example:** Firewalls

- ***NIST CSF****: PR.AC-5 = "Protect network traffic with firewalls"*
- ***ISO 27001****: A.13.1 = "Implement network controls (firewalls)"*
- ***CIS Controls****: Control 12 = "Manage network infrastructure securely"*
- ***SOC 2:*** *CC6.1 = "Secure logical access with firewalls"*

Every framework says "block bad traffic at network edges" → ***Perfect overlap***

1.3.1 Nature of Control Overlaps

While Table 1 demonstrates mapping equivalence across frameworks, the overlap is conceptual rather than identical in scope.

For example, NIST PR.AC-5 requires network traffic protection aligned to risk posture, whereas ISO 27001 A.13.1 emphasizes documented network control implementation. CIS Control 12 provides detailed technical safeguards for managing network infrastructure, and SOC 2 CC6.1 focuses on logical access protection from an assurance perspective.

Thus, although all frameworks require firewall implementation, the depth, documentation requirements, and audit expectations vary. The overlap exists at the objective level (protect network boundaries), but implementation granularity differs.

This reinforces the need for unified control normalization rather than assuming identical compliance requirements.

1.4 Unique Framework Requirements

Framework	**Key Unique Elements**
NIST CSF 2.0	- Strategic flexibility and outcome-focused - Maturity tiers (Partial to Adaptive) - New **Govern** function (oversight + supply chain risk) - Less prescriptive; customizable via Profiles - No certification; self-assessment only
ISO 27001:2022	- Formal **ISMS** required - Mandatory processes: audits, management reviews, continual improvement - Third-party certification + **Statement of Applicability** - Broad scope (physical, HR, supplier security) - Audit-intensive for global compliance

CIS Controls v8	- Highly prescriptive “how-to” safeguards - 18 prioritized Controls with Implementation Groups (IG1–IG3) - Tactical focus; less governance/strategy - Strong for rapid operational hardening against common threats
SOC 2	- Audit/reporting framework for service providers - Evidence of design (Type 1) + operating effectiveness (Type 2) - Principles-based Trust Services Criteria (Security mandatory; others optional) - Narrower scope: customer trust & service controls - Ongoing monitoring required; no maturity tiers

Table 2: *Unique requirements for each security frameworks*

1.5 Comparative Framework Analysis

Although NIST CSF, ISO 27001, CIS Controls, and SOC 2 share common security objectives, they differ significantly in philosophy, depth, and implementation approach.

NIST CSF is outcome-driven and risk-based, allowing organizations flexibility in implementation. It emphasizes maturity progression and continuous improvement rather than strict compliance.

ISO 27001 is management-system oriented and audit-driven. Unlike NIST, it mandates formal governance structures such as documented policies, internal audits, management reviews, and continual improvement under the PDCA cycle.

CIS Controls focus on tactical defense mechanisms. They provide prescriptive technical safeguards and are particularly useful for rapid operational hardening, but lack governance depth compared to ISO.

SOC 2 centers on assurance and reporting. While it overlaps technically with other frameworks, its primary purpose is to demonstrate trust and control effectiveness to external stakeholders through independent audits.

This comparison highlights that although technical controls like firewalls and VPNs overlap across frameworks, governance intensity, audit rigor, and implementation expectations differ substantially.

1.6 Implementation guidance

When analyzing frameworks like **NIST CSF**, **ISO 27001**, **CIS Controls**, and **SOC 2**, implementation guidance explains:

- **How controls are introduced** (risk-based, management-based, or technical priority)
- **How organizations move from requirement → deployment**
- **How implementation is verified or audited**

So instead of only stating *what controls exist*, you explain *how organizations apply them on paper.*

Framework	Implementation Focus	Implementation Method	Implementation Process	Implementation Outcome

NIST CSF	Risk-based security improvement	Controls implemented based on risk assessment and maturity levels	Tier-based progression with continuous monitoring	Improved security maturity aligned with organizational risk
ISO 27001	Management-driven security implementation	ISMS-based control deployment	Plan–Do–Check–Act (PDCA) cycle	Auditable and continuously improving security management system
CIS Controls	Technical control prioritization	Implementation based on prioritized safeguards	IG1 → IG2 → IG3 phased implementation	Gradual strengthening of technical security posture
SOC 2	Assurance and compliance implementation	Controls aligned with Trust Service Criteria	Scope definition → Type I/II audit → Reporting	Demonstrated compliance and customer assurance

Table 3. *Implementation Guidance Table*

1.7 Framework Implications for Network Security Controls

From a network security perspective, the frameworks collectively reinforce five key themes:

1. Boundary protection must be enforced and documented.
2. Network activity must be monitored continuously.
3. Access to network resources must be authenticated and authorized.
4. Lateral movement must be restricted through segmentation.
5. Control effectiveness must be tested and evidenced.

However, implementation expectations vary:

- ISO 27001 requires formal policy documentation and audit trails.
- NIST CSF encourages risk-driven prioritization.
- CIS Controls emphasize technical hardening steps.
- SOC 2 demands proof of operating effectiveness.

Therefore, a unified control approach must integrate governance rigor (ISO), risk alignment (NIST), tactical safeguards (CIS), and evidence generation (SOC 2).

This layered interpretation forms the foundation for the Unified Control Catalog in Section 3.

SECTION 2 CONTROL MAPPING METHODOLOGY

2.1 Objective

A systematic and repeatable approach used to link: Threats, Security controls, Security frameworks.

2.2 Process

Step – 1 Identify security controls – **Control Inventory table**

Step – 2 Identify threats and risks – **Threat identification table**

Step – 3 Link Threat to all the security controls - **Threat- control (Security control) mapping matrix**

Step – 4 Gap analysis

2.2.1 Control Equivalence Criteria

To ensure consistency and repeatability in control mapping, equivalence between framework controls was determined using the following criteria:

1. Objective Alignment

The control must address the same primary security objective (e.g., prevent unauthorized access, detect anomalous traffic).

2. Functional Similarity

The control must perform comparable preventive, detective, or corrective functions.

3. Scope Consistency

The implementation scope (perimeter, internal network, remote access, monitoring) must substantially overlap.

4. Evidence Expectation

The control must require similar documentation, logging, or audit artifacts.

Mapping Strength Definitions:

- Exact Match: All four criteria align.
- Partial Match: Objective aligns, but scope or evidence requirements differ.
- Weak/Indirect Match: Conceptually related but not functionally equivalent.

2.3 Control Inventory [Link]

- A data repository of existing security controls implemented within the organization
- A complete and validated control inventory is a **prerequisite** for control-to-threat mapping and gap analysis.

2.3.1 Control Inventory Table

Control ID	Control Name	Control Type	Primary Function	Security Layer	Implementation Scope
NC-01	Network Firewall	Network Security	Preventive	Perimeter / Internal	On-premise / Cloud
NC-02	Intrusion Detection System (IDS)	Network Monitoring	Detective	Network / DMZ	On-premise / Cloud
NC-03	Intrusion Prevention System (IPS)	Network Security	Preventive	Inline Network	On-premise / Cloud
NC-04	Virtual Private Network (VPN)	Secure Access	Preventive	Remote Access	On-premise / Cloud
NC-05	Network Segmentation	Network Architecture	Preventive	Internal Network	On-premise / Cloud
NC-06	Traffic Monitoring & Logging	Monitoring & Visibility	Detective	Network	On-premise / Cloud

Table 4: *Control Inventory Table*

2.3.2 Control Inventory Attributes: Each security control in the “table 3” has its own control type (preventive, detective and corrective), primary function – defines the main security objective of the control. Security Layer identifies where the control operates within the technology stack or architecture and implementation scope specifies the environment or area where the control is applied, such as on-premises infrastructure, cloud environments. This structure enables **consistent mapping across threats and frameworks**.

2.4 Threat–Control Mapping Matrix (Methodology View): Defines the relationship between identified threats and the security controls designed to mitigate, prevent, detect, or respond to them. This mapping is described as **Threat – Control Mapping Matrix.**

2.4.1 Relationship Classification Model

Control-to-threat relationships were categorized using structural mapping logic:

- One-to-Many: A single security control mitigates multiple threats.
- Many-to-One: Multiple security controls collectively mitigate a single threat.
- One-to-One: A control directly addresses a single specific threat.
- Many-to-Many: Multiple controls mitigate multiple overlapping threats.

2.4.2 Threat–Control Mapping Matrix (Example)

Threat ID	Threat Description	Applicable Security Controls	Control Function	Mapping Strength	Relationship Type
T-01	Unauthorized External Access	Firewall, IPS, VPN	Prevent	Exact	Many-to-One
T-02	Network Reconnaissance / Scanning	IDS, IPS	Detect / Prevent	Partial	One-to-Many
T-03	Malware Command & Control Traffic	IDS, Traffic Monitoring	Detect	Partial	One-to-Many
T-04	Lateral Movement Within Network	Network Segmentation, IDS	Prevent / Detect	Exact	Many-to-One
T-05	Denial-of-Service (DoS/DDoS)	Firewall, IPS, Traffic Monitoring	Prevent / Mitigate	Partial	Many-to-One
T-06	Man-in-the-Middle (MITM) Attacks	VPN, Firewall	Prevent	Exact	One-to-Many

Table 5: *Threat–Control Mapping Matrix*

2.4.3 Output (Threat-control Mapping Matrix)

- It provides **traceable input for gap analysis and unified control catalog development**, without representing final compliance or audit conclusions.

2.4.4 Integrated Mapping Workflow

The control mapping process follows a layered evaluation model:

1. Identify Threats

Real-world threats are identified based on network attack vectors.

2. Identify Existing Controls

Technical and procedural controls are inventoried.

3. Evaluate Control Coverage

Each control is assessed against identified threats using defined equivalence criteria.

4. Map Controls to Framework Requirements

Unified controls are cross-referenced against NIST, ISO, CIS, and SOC 2.

5. Identify Gaps

Partial or missing coverage indicates control weaknesses requiring remediation.

2.5 Gap Analysis: Gap analysis is performed by evaluating the threat–control mapping matrix to identify threats with insufficient or absent control coverage. **Controls** marked as **partial or missing indicate potential security gaps** requiring additional preventive, detective, or corrective measures. [Link]

Threat ID	Threat Description	Existing Security Controls	Coverage Level	Identified Gap	Recommended Control / Improvement	Gap Priority
T-01	Unauthorized External Access	Firewall, IPS, VPN	Adequate	No significant gap identified	Continuous rule review and monitoring	Low
T-02	Network Reconnaissance / Scanning	IDS, IPS	Partial	Limited prevention capability	Advanced threat detection / automated blocking	Medium
T-03	Malware Command & Control Traffic	IDS, Traffic Monitoring	Partial	Detection available but limited prevention	Endpoint Detection & Response (EDR), Threat Intelligence Integration	High
T-04	Lateral Movement Within Network	Network Segmentation, IDS	Partial	Limited internal traffic visibility	Network Behavior Analysis (NBA), Micro-segmentation	Medium
T-05	Denial-of-Service (DoS/DDoS)	Firewall, IPS, Traffic Monitoring	Partial	Lack of dedicated DDoS mitigation	DDoS protection service / traffic scrubbing	High

***Table 6** Gap Analysis*

2.5.1 Gap Prioritization Logic: Gaps were prioritized using a risk-based approach considering:

- Likelihood of exploitation
- Potential business impact (confidentiality, integrity, availability)
- Current control maturity
- Detection vs prevention capability

  High-priority gaps represent risks that could significantly disrupt availability (e.g., DDoS) or enable data exfiltration (e.g., malware C2 traffic). Medium-priority gaps indicate areas requiring improved internal visibility and segmentation. Low-priority gaps represent operational refinements.

2.6 Methodology Validation : The mapping methodology was reviewed to ensure:

- Logical consistency across frameworks
- Alignment between threat coverage and control function
- Elimination of duplicate or redundant controls
- Clear traceability from threat to unified control

Section 3: UNIFIED CONTROL CATALOGUE

3.1 Purpose

Unified control mapping identifies overlaps across frameworks and builds a single control library that satisfies multiple frameworks simultaneously. Instead of rewriting “access control” five different ways, you define one access control policy that maps to each framework’s equivalent requirement.

The **Unified Control Catalog consolidates security controls** derived from **multiple Cybersecurity frameworks into a single normalized control set**.

3.2 Unified Control Catalog Formation Process

This process illustrates Identify overlaps → Remove duplicates → Normalize control language → Define unified control objective → Map to threats + frameworks → Assign unique ID → Add to unified catalogue.

3.1.1 Unified Control Catalogue

Unified Control ID	Unified Control Name	Control Objective	Security Technology / Implementation	ISO 27001 Mapping	NIST CSF Mapping	SOC 2 Mapping	CIS Controls v8 Mapping
UC-NET-01	Network Boundary Protection (Firewall)	Prevent unauthorized access and control traffic between trusted and untrusted networks	Next-Generation Firewall (NGFW), Access Control Lists, Stateful Inspection	A.8.20, A.8.21	PR.AC-5 PR.PT-4	CC6.6 CC6.7	Control 13
UC-NET-02	Network Segmentation & Zone Isolation	Limit lateral movement and isolate critical systems to reduce attack impact	VLANs, Internal Firewalls, Subnetting, Micro-segmentation	A.8.22	PR.AC-5 PR.PT-3	CC6.6	Control 12
UC-NET-03	Intrusion Detection & Prevention (IDS/IPS)	Detect and prevent malicious or anomalous network activity	Network IDS, Network IPS, Signature & Behavior Analysis	A.8.16	DE.CM-1 DE.CM-7	CC7.2	Control 13.7

UC-NET-04	Secure Remote Access (VPN)	Ensure secure and encrypted remote connectivity to organizational networks	IPsec VPN, SSL VPN, MFA Integration	A.8.5 A.8.20	PR.AC-1, PR.AC-3	CC6.1 CC6.2	Control 12.3
UC-NET-05	Network Traffic Monitoring & Logging	Provide visibility for threat detection, incident response, and forensic analysis	SIEM, NetFlow Analysis, Log Management, Traffic Analytics	A.8.15 A.8.16	DE.CM-1, DE.AE-1	CC7.2 CC7.3	Control 8 Control 13

Table 7: *Unified Control Catalog/Table (A Sample Table)*

3.1.2 Effort calculation

BEFORE UNIFICATION: There were 20+ Security Controls, each framework has 5+ security controls.

- **NIST**: PR.AC-5, DE.AE-1, PR.AC-3...
- **ISO**: A.13.1.1, A.8.16, A.9.1.2...
- **CIS**: 12.5, 8.1, 4.8, 13.1...
- **SOC2**: CC6.1, CC7.2, CC6.6...

Total effort= 4 Teams × 5 Controls × 4 Audits (per year)

Total effort = 80

- Each framework requires four audits per year.
- Each framework is handled by a separate team.

AFTER UNIFICATION: After consolidation the unification table has only 5 Security Controls.

= 1 Teams × 5 Controls × 4 Audits

Total effort required is = 20

= 75 % reduction in effort **(in theory)**

3.2 Key Outcome of Unified Control Catalog

The unified catalog demonstrates that:

- A single technical implementation can satisfy multiple framework requirements.
- Security controls are mapped to operational technologies rather than compliance language.

- Overlapping requirements across ISO 27001, NIST CSF, SOC 2, and CIS Controls are normalized into implementable security practices.
- The catalog serves as input for gap remediation, control maturity assessment, and compliance reporting.

SECTION 4: IMPLEMENTATION GUIDANCE

4.1 Purpose

- **Section 3 defines what** control exists, **Section 4 defines how** the control is implemented, operated, and verified.

4.2 Implementation Guidance Development Approach [Link]

- The implementation guidance is derived from the Unified Control Catalog by analyzing each control from an operational and technical perspective.
- Appropriate security technologies are identified to enforce the control objective, followed by the definition of operational processes required for deployment, monitoring, and maintenance.
- This approach is executed by the implementation guidance table.

4.3 Implementation Guidance Table

It covers:

- **how CONTROLS** are **IMPLEMENTED → TECHNOLOGY**
- how **CONTROLS** are maintained **OPERATIONAL → PROCESSES**
- how **CONTROLS** are **PROVEN → EVIDENCE**
- and how **EFFECTIVENESS** is **MEASURE** → **METRIC**

This table ensures that controls defined in Section 3 are consistently implemented, monitored, and validated across the organization.

Unified Control ID	Unified Control Name	Technology Implementation	Process Requirement	Evidence / Artifacts	Effectiveness Metrics
UC-NET-01	Network Boundary Protection (Firewall)	NGFW, ACLs, rule filtering, application control	Firewall rule review, access approval workflow	Firewall configuration backup, rule review logs	Blocked unauthorized attempts, rule review frequency
UC-NET-02	Network Segmentation & Zone Isolation	VLANs, internal firewalls, subnet isolation	Network segmentation review, change approval	Network diagrams, segmentation policies	Reduction in lateral movement paths

Table 8: *Unified Control Implementation Guidance Table (Sample Table)*

SECTION 5: CONTROL VALIDATION & CONTINUOUS IMPROVEMENT

5.1 Purpose Ensures that implemented controls (from Section 4) effectively mitigate identified threats and satisfy unified framework requirements (Section 3). **[Link]**

5.2 Gap Assessment Results from Section 2 are validated through operational testing and monitoring metrics.

5.2.1 Gap Remediation Tracking Track gaps (e.g., "partial firewall filtering") and implement corrective actions

5.3 Validation & Monitoring Approach

- **Control Testing:** Periodic technical and procedural tests to confirm that controls (firewalls, IDS/IPS, VPNs, segmentation, traffic monitoring) function as intended.
- **Metrics & KPIs:** Monitor performance indicators defined in Section 4 (e.g., blocked attempts, incident response times, anomaly detection rates).
- **Evidence Collection:** Maintain logs, audit trails, configuration backups, and monitoring reports to support compliance and continuous assessment.

5.4 Control Validation Dashboard

Unified Control	KPI/Metrics	Test Frequency	Status	Evidence
UC-NET-01	Block rate 95%	Weekly	PASS (97%)	Firewall logs
UC-NET-03	False negative < 2%	Monthly	FAIL (3.2%)	Test report
UC-NET-05	Zero lateral paths	Quarterly	PASS	Path analysis

Table 9: *Network Security Control Validation Results*

5.5 Continuous Improvement

- Perform periodic reviews aligned with ISO 27001 PDCA, NIST CSF Tiers, CIS Controls IG progression, and SOC 2 audit cycles.

5.7 Outcome

- Verified, effective security control environment aligned across NIST CSF, ISO 27001, CIS Controls, SOC 2.

6. EXECUTIVE SUMMARY

6.1 Control Posture Overview

This report establishes a **Unified Security Control Framework**, consolidating requirements from **NIST CSF 2.0, ISO 27001:2022, CIS Controls v8, and SOC 2**. By moving from a siloed compliance approach to a unified model, the organization has achieved the following posture improvements:

- **Efficiency Gain:** The consolidation of overlapping requirements (e.g., Firewalls, IDS, Access Control) into a single Unified Control Catalog has reduced the estimated compliance and audit effort by **75% theoretically** (reducing "effort units" from 80 down to 20).
- **Perimeter Security:** The organization demonstrates **Strong** maturity in perimeter defense (T-01), with effective deployment of Firewalls (PR.AC-5/A.13.1) and VPNs ensuring secure external access.
- **Unified Validation:** We have transitioned from disparate audit cycles to a continuous monitoring model. However, validation testing (Section 5) indicates that while **preventive controls** are robust, **detective capabilities require tuning**, specifically regarding false negative rates in intrusion detection.

6.2 Key Gaps & Risk Exposure Through the Threat–Control Mapping and Gap Analysis (Section 2.4) and Control Validation (Section 5.5), the following critical deficiencies were identified:

Priority	Threat ID	Gap Description	Risk Impact
HIGH	**T-05**	**Denial-of-Service (DoS/DDoS)**	**Availability Risk:** Current controls (Standard Firewalls/IPS) lack dedicated DDoS mitigation or traffic scrubbing capabilities, leaving the network vulnerable to volumetric attacks.
HIGH	**T-03**	**Malware C2 Traffic**	**Confidentiality Risk:** While basic detection exists, there is a lack of automated prevention for Command & Control traffic. Reliance on manual traffic monitoring slows response time to data exfiltration attempts.
MEDIUM	**T-04**	**Lateral Movement**	**Propagation Risk:** Internal network visibility is limited. The lack of strict micro-segmentation allows potential attackers to move laterally from a compromised host to critical assets.
MEDIUM	**UC-NET-03**	**IPS Efficacy Failure**	**Performance Risk:** Recent validation testing revealed a failure in Control UC-NET-03, where false negatives exceeded the 2% threshold (actual: 3.2%), indicating the system is missing legitimate threats.

6.3 Automation: There are many GRC tools that can do it all above described tasks automatically.

Tool	Control Mapping	Framework Support	Key Strength
Vanta	Automated cross-framework mapping	ISO 27001, NIST, CIS, SOC 2	Continuous monitoring + evidence reuse
Paracomply	Visual crosswalk mapping	ISO, NIST, SOC 2	Unified control demonstration
Complyance	Pre-built control templates	ISO 27001, NIST, SOC 2	Strong control life-cycle management
CyberCyte	Multi-framework mapping	ISO, NIST, CIS, SOC 2	Enterprise dashboards
United GRC	Unified control repository	ISO, NIST, SOC 2	Shared evidence & reporting
Risk Cognizance	AI-assisted mapping	ISO, NIST, CIS, SOC 2	Gap analysis & risk-based approach