COMPLIANCE MATRIX · 01 · UNIVERSAL FRAMEWORKS

Direct mapping · CSURFACE control × regulatory clause

Seven controls delivered by the CSURFACE platform, each with the specific clause of every framework it addresses — NIST CSF, ISO 27001:2022, CIS Controls v8, PCI DSS 4.0 and NIS2. Brazil and sector-specific on the next page.

Datasheet 2026
CSURFACE

Why this matrix matters. The auditor does not ask "do you have ASM?". The auditor asks "how do you meet requirement X of standard Y?". This matrix answers directly — each control delivered by CSURFACE with the specific clause it addresses, across seven frameworks that appear in RFPs and in regulatory opinions.

CSURFACE CONTROL	NIST CSF v1.1 / v2.0	ISO 27001:2022 Annex A	CIS CONTROLS V8 Center for Internet Sec.	PCI DSS 4.0 PCI SSC	NIS2 EU Directive 2022/2555
Continuous external attack surface discovery Automatic, continuous, agentless inventory of external assets.	**ID.AM-2** software inventory	**A.5.9 · A.8.16** inventory · monitoring	**1.1 · 1.5** asset inventory · discovery	**11.3.2** quarterly+ external scan	**Art. 21.2(a)** risk policy
Asset inventory with classification and owner Automatic assignment of ownership, sector, category and business area.	**ID.AM-1/2/6** hardware · software · roles	**A.5.9 · A.5.10** inventory · acceptable use	**1.1 · 1.4 · 2.1** inventory · tags · software	**12.5.1** inventory within PCI scope	**Art. 21.2(a)** risk analysis
Digital supplier chain mapping Three levels — direct dependency, sub-supplier and the sub-supplier's sub-supplier.	**ID.SC-2 · ID.SC-4** monitored suppliers	**A.5.20/21/22** supplier chain	**15.1 · 15.4** TPSP inventory and contracts	**6.4.3 · 12.8.1** checkout scripts · TPSPs	**Art. 21.2(d)** supply chain security
Continuous vulnerability management · dynamic prioritization Exploitation-likelihood scores and active-exploitation catalogs shaping the queue in real time.	**DE.CM-8 · ID.RA-1** continuous scan · vulns identified	**A.5.7 · A.8.8** threat intel · technical vulns	**7.1 · 7.2 · 7.6** vuln mgmt process	**6.3.1 · 11.3** vulns identified and managed	**Art. 21.2(e)** vulnerability handling
Leaked credential monitoring Breach DBs, dark web, public repositories — with non-destructive active validation.	**ID.RA-3 · DE.CM-7** external threats · monitoring	**A.5.7 · A.8.16** threat intel · monitoring	**17.2** incident reporting channels	**8.3.1** MFA against compromised credentials	**Art. 21.2(g)** cyber hygiene
Financial risk quantification · FAIR ALE and VaR over quantified scenarios — a standard report for the board.	**ID.RA-4 · ID.RA-5** impact · quantified risk	**A.5.4** management responsibilities	**17.1** RM program	**12.3.1** formal risk assessment	**Art. 21.2(a)** formal risk analysis
Auditable exposure → remediation trail Each finding with timestamps for detection, alert, assignment and closure.	**PR.IP-12 · DE.AE-2** remediation plan · analysis	**A.5.24 · A.8.15** incident management · logging	**8.2 · 8.5** audit logs · processing	**10.2.1** event audit logs	**Art. 23** reporting obligation

Mapping built from the official publications (NIST CSF v1.1 and v2.0 · ISO/IEC 27001:2022 Annex A · CIS Controls v8.1 · PCI DSS v4.0 · EU Directive 2022/2555 NIS2). Full adherence to each framework depends on the contracted scope and the organization's internal policy — this matrix indicates where the platform's technical capability connects to each clause.

COMPLIANCE MATRIX · 02 · BRAZIL AND SECTOR-SPECIFIC · EVIDENCE

BACEN, LGPD, SOX · and what comes out as exportable evidence

The same seven controls, now mapped to the Brazilian and sector-specific regulatory set. Alongside, the types of artifact the platform exports — what the auditor receives when they request evidence.

Datasheet 2026
CSURFACE

CSURFACE CONTROL	BACEN 4.557 Operational risk	BACEN 4.893 Cybersecurity policy	LGPD Law 13.709/2018	SOX · ITGCS Sarbanes-Oxley
Continuous external attack surface discovery	**Art. 3 · 38** operational risk management	**Art. 4 · I** identify threats	**Art. 46** technical measures	**Computer Ops** ITGC · monitoring
Asset inventory with classification and owner	**Art. 3 · IV** risk identification	**Art. 3 · II** security guidelines	**Art. 37 · 46** processing records	**Access Control** ITGC · asset control
Digital supplier chain mapping	**Art. 33** material outsourcing	**Art. 5** assessment of critical suppliers	**Art. 39 · 42** processor co-responsibility	**Vendor Mgmt** ITGC · supplier management
Continuous vulnerability management · dynamic prioritization	**Art. 3 · V** monitoring and mitigation	**Art. 4 · III · IV** detect · respond	**Art. 46** technical and administrative measures	**Change Mgmt** ITGC · patch and change
Leaked credential monitoring	**Art. 4** fraud and cyber risk	**Art. 4 · III** detect incidents	**Art. 46 · 48** protection · notification to ANPD	**Access Control** ITGC · privileged access
Financial risk quantification · FAIR	**Art. 3 · II · III** measurement and assessment	**Art. 3 · I** cybersecurity objectives	**Art. 50** governance program	**Sect. 404** assessment of internal controls
Auditable exposure → remediation trail	**Art. 5 · IV** documentation and reporting	**Art. 8** action and response plan	**Art. 48** incident trail	**Audit Logging** ITGC · logs and evidence

Types of exportable evidence · what the auditor receives

1 Timestamped inventory
CSV or JSON of every discovered asset with discovery timestamp, ownership assignment and classification. Versioned.

2 Discovery trail
For each relevant CVE: detection time, alert generated, assignment, ticket opening, closure. Exportable JSON.

3 Audit logs
User actions, configuration changes, evidence access. Full retention throughout the contracted operational window.

4 Regulatory snapshot
Timestamped PDF mapping each CSURFACE control × clause of the target standard (BACEN, ISO, PCI). Ready to attach to an opinion.

5 KRI metrics
Exposure window, MTTD, MTTR, discovery coverage, % of suppliers monitored — historical series for the committee.

6 CRQ report
ALE and VaR P90/P99 with documented assumptions, distribution ranges and alternative scenarios. Ready for the audit committee.

Receive the mapping applied to your environment

Request mapping