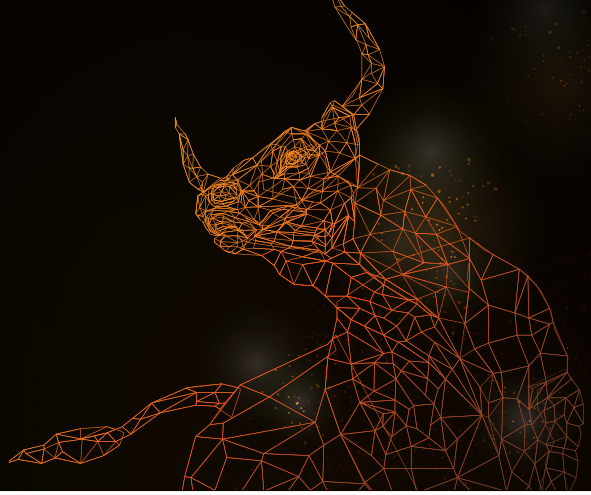
BULLWALL

SARBANES-OXLEY (SOX) QUICK REFERENCE GUIDE



Unlike GDPR or HIPAA, **SOX (Sarbanes-Oxley Act of 2002)** is not a cybersecurity or data protection law per se. It focuses on **financial transparency, internal controls over financial reporting (ICFR), and preventing fraud** within publicly traded companies.

However, **cybersecurity directly intersects with SOX** when it comes to ensuring that **financial systems and records are accurate, available, and tamper-proof** — especially in light of modern threats like ransomware.

How BullWall Supports SOX Compliance

1 Section 302 – Corporate Responsibility for Financial Reports

Executives must certify that:

- Financial data is accurate
- Internal controls are in place
- They are aware of significant changes, including fraud or security breaches

BullWall helps by:

- **Preventing ransomware from encrypting or corrupting financial records**
- Generating detailed logs and alerts if a breach or ransomware event touches finance systems
- Supporting executives in **demonstrating control over key systems**

2 Section 404 – Management Assessment of Internal Controls

Requires:

- Documented internal controls over financial reporting (ICFR)
- Ongoing monitoring and testing of those controls
- Demonstrated resilience against disruption or tampering

BullWall supports this by:

- Acting as a **compensating control** in case AV/EDR fails to stop ransomware
- Ensuring **financial data remains available and intact**
- Providing logs and events that show **resilience and detection capabilities**
- Supporting internal audits and ITGC (IT General Controls) testing

*If ransomware encrypts financial data or disrupts access during quarter-end or reporting, it can be a **SOX violation**. BullWall helps prevent that.*

3 Section 409 – Real-Time Disclosure of Material Changes

If a cyberattack compromises financial data or system integrity, it may trigger disclosure requirements to the SEC.

BullWall helps by:

- **Stopping ransomware attacks before they reach a material impact threshold**
- Offering real-time alerts that give you the chance to **respond quickly and reduce exposure**
- Supporting internal investigations with logs and event history

Relevant Control Categories in ITGCs (IT General Controls)

Auditors commonly assess these areas as part of SOX reviews. BullWall supports them by:

ITGC Area	BullWall Contribution
Change Management	Detects unauthorized encryption attempts that could indicate tampering
Access Controls	Isolates unauthorized or compromised accounts during active attacks
Data Backup & Recovery	Prevents damage to backup files and shares by containing ransomware early
Logical Security	Adds a layer of behavioral monitoring to detect misuse or compromise
Incident Management	Automates detection, containment, and forensics of attacks on financial systems

FINAL TAKEAWAY

While **SOX doesn't mandate cybersecurity controls directly, failure to protect financial systems** from ransomware or data loss **can result in SOX non-compliance,** audit findings, and even regulatory disclosures.

BullWall helps by:

- Preventing **unauthorized modification or encryption of financial data**
- Enabling **strong IT controls** over systems that store or process financial reports
- Supporting **audit trails, internal control documentation, and resilience testing**

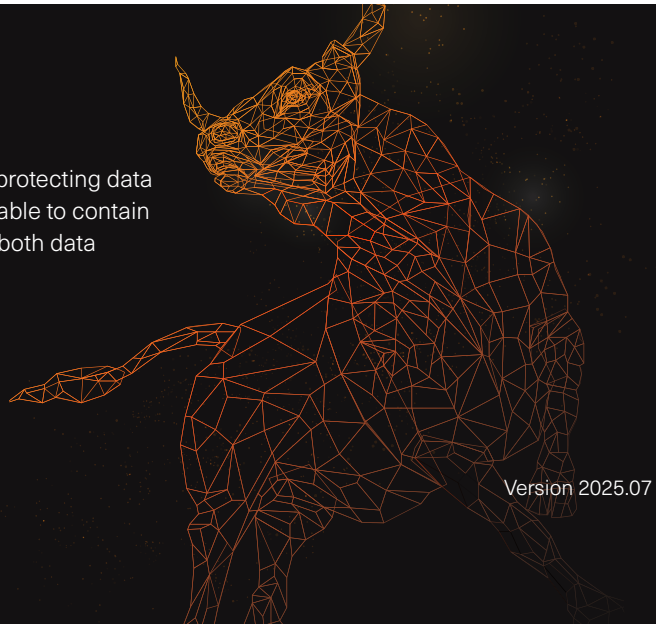
ABOUT BULLWALL

BullWall is a cybersecurity solution provider with a dedicated focus on protecting data and critical IT infrastructure during active ransomware attacks. We are able to contain both known and zero-day ransomware variants in seconds, preventing both data encryption and exfiltration.

BullWall is your last line of defense for active attacks.

Learn more at www.bullwall.com.

BULLWALL



Version 2025.07