ZORB: Compliance Control Mapping

Application Data Theft Prevention Framework Alignment

Version 1.0 | May 2025

Purpose

This document maps ZORB's application data theft prevention capabilities to established compliance frameworks. Use this reference when auditors ask, "which controls does ZORB satisfy?" or when building business cases requiring compliance evidence.

ZORB prevents deliberate data theft from desktop applications—filling the gap that traditional DLP misses while providing audit-ready evidence for multiple compliance requirements.

Cyber Essentials / Cyber Essentials Plus

Direct Control Satisfaction:

Control Theme	Evidence Provided
Theme 1: Firewalls	Outbound data restriction at device level. Validation logs showing only approved applications transmit to verified destinations.
Theme 2: Secure Configuration (Control 4.3)	Application configuration evidence: approved applications only transmit to legitimate vendor infrastructure. Real-time validation of data flow security.
Theme 5: Malware Protection (Control 5.2)	Behavioural detection and blocking of exfiltration attempts. Prevention of C2C communication for botnets, RATs, ransomware.

Complementary Coverage:

Control Theme	Scope
Theme 3: Security Update Management	Detects update poisoning by validating destination infrastructure. Does not replace patch management processes.
Theme 4: User Access Control	Prevents data theft when access controls fail. Does not replace identity/access management systems.

Detailed control-by-control assessment: How ZORB maps to Cyber Essentials controls

ZORB: Compliance Control Mapping

ISO 27001:2022

Information Security Controls:

Control	Description	How ZORB Satisfies
A.8.10	Information deletion	Audit trail of data transmission validation—evidence of controlled data flow lifecycle
A.8.11	Data masking	Validates destination legitimacy before transmission—prevents data reaching unauthorised locations
A.8.12	Data leakage prevention	Primary control: prevents unauthorised application data transmission in real-time
A.5.23	Information security for use of cloud services	Validates cloud service connections—ensures data only reaches legitimate cloud provider infrastructure

Audit Evidence: Real-time logs showing application-to-destination validation, blocked transmission attempts, approved safelist configuration.

Detailed ISO27001 control mapping guide: Coming soon

PCI DSS v4.0

Payment Card Industry Data Security Standard:

Requirement	Description	How ZORB Satisfies
10.4.1.1	Audit logs of unauthorised system modifications	Complete audit trail of unauthorised data transmission attempts with application process identification
12.10.4	Critical systems transmission security	Validates data transmission security for payment processing applications—ensures data only reaches authorised card processing infrastructure

Compliance Note: ZORB complements PCI DSS network segmentation and encryption requirements by validating application-level data flows.

Detailed PCI DSS control mapping guide: Coming soon

ZORB: Compliance Control Mapping

GDPR (General Data Protection Regulation)

Data Protection Requirements:

Article	Requirement	How ZORB Satisfies
Article 5.2	Accountability principle	Demonstrable evidence of technical measures preventing unauthorised personal data transmission
Article 30	Records of processing activities (ROPA)	Real-time audit trail of data flows: which applications transmitted what data to which destinations
Article 32	Security of processing	Technical measure implementing "appropriate security" for personal data protection

ICO Guidance Alignment: ZORB provides evidence of "appropriate technical measures" for preventing unauthorised personal data transmission—key requirement for GDPR accountability.

Detailed GDPR control mapping guide: Coming soon

ZORB: Compliance Control Mapping

What ZORB Does

Core Capability: Application data theft prevention through 3-point validation

1. **Source Verification:** Only approved applications can transmit data
2. **Destination Validation:** Data only reaches legitimate vendor infrastructure (DNS-independent validation)
3. **Transmission Control:** Communication methods validated against security policy

Business Outcome: Operational resilience during security incidents—confidence to make strategic decisions about which systems need shutdown vs which can safely continue.

Stack Position: Complements existing DLP (email/web), firewall (network), and endpoint protection (device). Fills the application data protection gap.

For Auditors

Evidence Package Available:

- Application safelist configuration
- Real-time transmission validation logs
- Blocked exfiltration attempt records
- Application-to-destination correlation data
- Vendor infrastructure verification methodology

Free Proof-of-value Trial: 10 devices, 10 days, zero risk

See actual unauthorised application data flows in your own environment.

ZORB Security Ltd | Cambridge, UK | NCSC for Startups Alumni www.zorbsecurity.com

Technical Questions: support@zorbsecurity.com

This control mapping reflects ZORB capabilities as of December 2024. Compliance requirements vary by organisation and jurisdiction. This document provides framework alignment guidance—consult with your compliance team or auditor for specific certification requirements.