Technical Controls Assessment

Assessing the Effectiveness, Integration & Future Readiness of Security Technologies
Company 86 | www.c86.tech

Executive Summary

The C86 (Company 86) Technical Controls Assessment provides organisations with a clear, evidence-based understanding of the effectiveness of their existing security technology controls. The service evaluates how current technical controls operate individually and collectively to mitigate security risks, threats and comply to regulatory requirements, both internal and external, and how they integrate with people and process.

Technology & Threat Landscape Context

Organisations continue to invest heavily in security technologies to address an increasingly complex and sophisticated threat landscape. However, security risk is not reduced by technology alone. Gaps in configuration, integration, operational maturity, or alignment to business processes can significantly reduce the effectiveness of even best-of-breed tools.

At the same time, digital transformation, cloud adoption, automation, and artificial intelligence (AI) are reshaping enterprise environments. Security controls must not only protect today's environment, comply to regulatory frameworks, but also be capable of supporting secure adoption of future technologies.

Service Overview

The C86 Technical Controls Assessment reviews an organisation's security technology portfolio end-to-end to understand control coverage, effectiveness, cohesion and regulatory compliance. The assessment considers technology, people, and process together, ensuring controls operate as intended and delivering measurable security outcomes, within the risk tolerance for the organisation.

Scope of the Technical Controls Assessment

The assessment can be performed across the full security technology stack, including but not limited to:

- Next-generation firewalling and network security controls
- Identity and Access Management (IAM)
- Privileged Access Management (PAM)
- Endpoint Detection and Response (EDR)
- Managed Detection and Response (MDR)
- Security Operations Centre (SOC) capability
- Security Information and Event Management (SIEM)
- Security Orchestration, Automation and Response (SOAR)
- Cloud security controls
- Quantum controls readiness

Assessment Focus Areas

The Technical Controls Assessment focuses on the following key areas:

- Effectiveness of individual security controls and configurations
- Integration and interoperability between security technologies
- Coverage of relevant threats and attack scenarios
- Alignment of controls to operational processes and people
- Ability to detect, respond to, and contain security events
- Gaps, overlaps, and inefficiencies within the control environment
- The risk tolerance of the organisation and its supply chain

Outcomes & Recommendations

The assessment produces clear, actionable recommendations to improve the effectiveness and efficiency of technical security controls. Recommendations are prioritised based on risk, threat relevance, and business impact.

This may include:

- Configuration and tuning improvements
- Controls gap assessment and recommendations
- Control integration and optimisation opportunities
- Technology rationalisation or enhancement recommendations
- Operational improvements across people and process
- Supply chain recommendations
- Roadmap recommendations for future-state control capabilities

Future-State & Secure Enablement

The Technical Controls Assessment supports organisations as they evolve their technology landscape. Findings and recommendations are designed to enable secure adoption of digital transformation initiatives, including cloud services, automation, and AI, while maintaining strong security assurance.

Delivery & Engagement Models

The Technical Controls Assessment can be delivered as a standalone engagement or integrated with broader security programmes. It can be consumed as:

- A one-off assessment and recommendations engagement
- Part of a wider security transformation programme
- An input into ongoing managed security or virtual security team services

Key Benefits

- Clear visibility of security control effectiveness
- Improved detection and response capability
- Better integration across security technologies
- Reduced risk through optimised technical controls
- Security controls aligned to future business and technology needs

Why C86?

C86 brings deep expertise across security architecture, operations, and risk management. Our pragmatic, vendor-agnostic approach ensures technical controls are assessed objectively and aligned to real-world threats and business outcomes.

Contact Us

www.c86.tech
info@c86.tech