ZERODAYLAB®

Governance, Risk & Compliance Consulting Services

Trusted Advisor for All Your Information Security Needs

GRC: Visibility - Efficiency - Resilience - Reputation

Keeping up with compliance and cybercrime leaves many companies between a rock and a hard place with nowhere to go, but there is a solution.

ROCK: The Pain of Relentless Security Threats

The number of compromises continues to rise exponentially and no vertical is immune. As cyber threats continually evolve it is difficult for organisations to get a full view of the risks posed to their business, how to manage them, or if their systems and processes are still up to the task.

HARD PLACE: Keeping Pace with Regulation & Compliance Standards

Meeting regulatory and best practice requirements such as ISO, SSAE, EU GDPR, NIST, and PCI DSS is a tremendous task for any organisation.

Compliance continues to evolve and many businesses have little, if any, dedicated resources. Combine this with mixed internal IT environments and the demand for business growth, a complex compliance scope emerges. Few companies can get an accurate view of the gaps in controls and policy by assessing from the inside out.

People, Process, Technology

ZeroDayLab's 360° approach to GRC focuses on the strategic alignment of people, process and technology. This analysis drives greater efficiency as well as giving management greater visibility over the factors affecting compliance-readiness and the risks to cyber security.

- Ensure Compliance

- Reduce Risk of Financial Penalties

- Proactively Secure Company Intellectual Property

- Improve Visibility of Controls, Assets & Risk

- Assurance against Potential Incidents

- Minimise Reputational Loss

ZERODAYLAB®

People - Process - Technology
The Foundation to GRC & Security Strategy

Process
Creating good governance and manageable risk competence by aligning policies with best-of-breed standards, procedures and enforceable processes.

People
Ensuring that Information Security responsibilities are understood and implemented in line with best practice by staff at every level of the business.
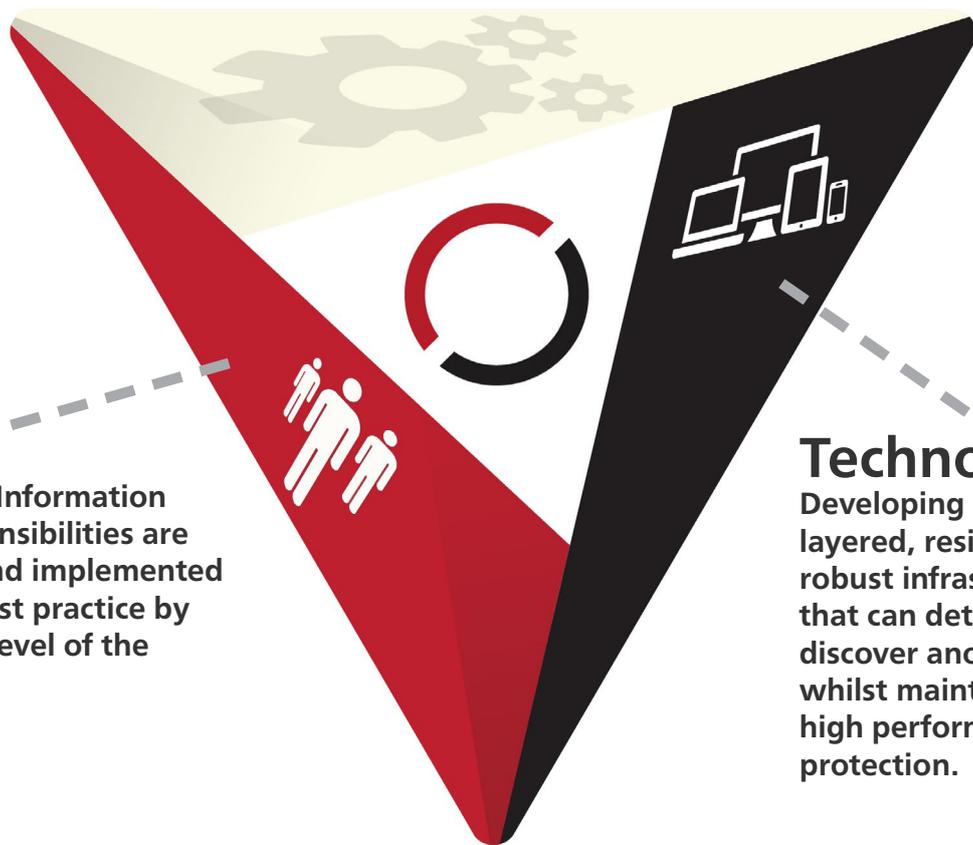
Technology
Developing a multi-layered, resilient and robust infrastructure that can detect and discover anomalies whilst maintaining high performance and protection.

Benchmarking and assessment against national and European Laws and Information Security best practice standards:

- ISO Standards: 9001 / 15489-1 2001 / 27001 / 27002 / 22301 / 27035/ 27031
- NIST 800-53 Rev 4 / NIST 800-61 Rev 2
- EU GDPR
- SSAE 16 - SOC 1 (Type 1 & 2), SOC 2 (Type 1, 2, 3), SOC 3
- EU Directive Legal Protection of Databases 1996
- Directive on Privacy & Electronic Communications
- Cyber Essentials

The 360° Approach to GRC

ZeroDayLab's qualified Information Security consultants bring a robust and impartial approach to analysing your organisation's requirements. Their best practice knowledge and experience from a wide range of verticals enables the development of comprehensive tactical, operational and strategic risk-based plans.

Assessments

Assessments are a measurement of organisational risk looking at the current situation, highlighting vulnerabilities and provides recommendations for improvement.

- Capability Maturity Assessment
- Technical Maturity Assessment
- Supplier Evaluation
  Ensuring suppliers meet your Information Security requirements.

Analysis & Remediation

Defining and measuring gaps between current and the desired security posture and the implementation of remediation projects.

- Risk Assessment
- Business Impact Analysis
- Risk Register Analysis
- Remediation projects and implementation
- Information Security Management Systems

Auditing Assistance

Assisting clients in passing external standards requirements.

- Internal Audit Assistance
- Advice and assessment of policies against numerous information best practice standards, policies and laws including:
  ISO27001, NIST, SSAE16, EU GDPR

Reviews

- 360° Reviews
  Investigation of all controls and the effectiveness of implementation

- Information Security Policy Reviews

- Policy and Procedures
  Procedure updating & development

- Technology
  Assessing & analysing implementation to ensure robust operation.
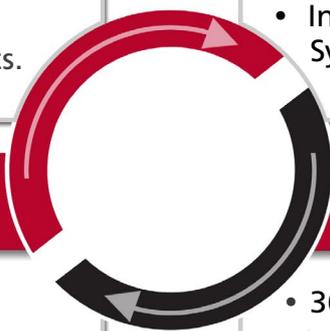
Why Use ZeroDayLab?

As a leading global IT Security Consulting company, ZeroDayLab works as a partner and trusted advisor, delivering IT Security Testing engagements for a broad range of public and private sector organisations internationally.

Our depth and breadth of experience enables us to deliver high quality assignments that both identify all areas of your IT security posture, whilst also providing appropriate remediation and recommendations that move you up the security maturity curve.

We spend every day helping make our clients' infrastructure and applications more secure through the intelligent combination of expert cyber consultants and services alongside complementary security technologies that drive '**Continuous Security Improvement**'.

We maximise ROI by delivering value for money services of the highest and **consistent quality, on time, every time and in budget**.

With a strong set of testimonials across a broad range of industries and sectors, we are **Passionate About Total Security Management** and we would be delighted to discuss your requirements in more depth to help you define an effective IT Security strategy that meets the requirements of your business and defends against both external and internal threats.

Our Services

- Vulnerability Assessment of Desktop, Servers, and Infrastructure
- Penetration Testing of all Internal / External Web Applications and Infrastructure
- Broad Security Review (Architecture and Infrastructure)
- Source Code Reviews
- Firewall Audits
- Desktop and Server Build Reviews
- Blockchain Application Security Audits
- Digital Forensic Analysis
- Security Awareness Programmes
- Security Training for Developers – Secure Coding School, CBT, Online Assessment
- Pre-Breach Incident Response & Runbook Training
- Phishing Resilience Programmes
- Bespoke Senior Executive Security Training
- Red Team Testing
- PCI DSS Remediation Support
- Gap Analysis to ISO, PCI DSS, SSAE16(18), GDPR
- 360° Reviews (Cyber Risk Assessment)
- Virtual Data Protection Officer
- Virtual Information Security Manager
- ISO / NIST / EU GDPR Standards Alignment
- Internal Audits
- SERM – Supplier Evaluation Risk Management
- Cyber Threat Intelligence – Deep & Dark Web
- Protective Monitoring (Managed SOC)
- Security Risk Training for Agile Developers
- ZeroDayResponse – Incident Response Review & Digital Forensics Training

Passionate About Total Security Management