SECURITY FRAMEWORKS CAPABILITY

WHY CHOOSE TORO

Ways in which businesses have benefited from **Toro's** cyber security reviews are:

Avoid a Breach

By understanding risks and supporting the development of a 'roadmap to remediation', it is possible to help reduce the likelihood and impact of a damaging cyber-attack.

Reassure Customers

A comprehensive review of security demonstrates best practice and helps grow an organisation-wide security culture that reassures customers, donors and partners that their reputation, information and assets are in safe hands.

Winning & Enabling Business

By managing risk exposure more effectively, it is possible to demonstrate a tender-winning 'differentiator' over less mature competitor.

Cost Effective Risk Management

By better understanding threats, vulnerabilities and risks, you will be better placed to develop pragmatic business resilience and an effective disaster recovery plan.

Security Optimisation

Understanding what attack pathways to critical activities must be 'hardened', it is possible to optimise security resources and refine spend.

Regulatory Compliance

Investing in cost effective and proportionate security controls prevents the reputational and financial impact of compliance failure. The Information Commissioner's Office (ICO) can fine you up to 4% of global annual turnover per data breach. Examples of recent fines by the ICO are available online.

Achieving Certification

Toro is a Cyber Essentials (& CE+) certifying body. Toro's cyber consultants are also ISO 27001 lead implementer and lead auditor qualified. We work to best practice standards, and we help clients accomplish them and achieve certification.

METHODOLOGY

Our approach to better understanding, quantifying, and managing cyber risk is underpinned by a thorough grasp of the people, processes and technology that are uniquely critical to each organisation.

Toro has developed a methodology, shaped by engagements with clients across multiple sectors, that achieves an optimal outcome. Broadly speaking, there are six conceptual steps as shown in the accompanying diagram.

One of the advantages of Toro's approach is that it can be integrated with most pre-existing organisation-wide risk management methodologies, for example, Enterprise Risk Management or Business Continuity Management. This can provide greater efficiencies, familiarity, and enduring application without the need for specialist training or consultancy.

At a foundational level, Toro is a Cyber Essentials Plus certification body. Further to this, the most used frameworks include ISO 27001 or NIST, but we also work to CIS Critical Security Controls, SOC 2, PRA CQUEST and others.

ISO 27001 METHODOLOGY

Toro will conduct a gap analysis against ISO 27001 to identify areas for improvement measured against this standard. By adopting the ISO standard, you can create and adopt security policies and procedures, and implement security controls, to better protect the confidentiality, integrity and availability of data in a consistent, actionable and measurable way.

ISO 27001 is the world’s most ubiquitous information security standard. First published in 2005, and recently updated in 2022, it provides a framework for identifying information security risks and selecting the most appropriate controls to mitigate them. This framework is known as an Information Security Management System (ISMS). An ISMS enables the efficient management of multiple requirements, such as laws and regulations, contracts, business development, and day-to-day business operations. ISO 27001 is structured into two segments titled “Management of the ISMS” and “Annex A – Information Security Controls”.

ISO 27001 METHODOLOGY

This “Management of the ISMS” segment of ISO 27001 specifically relates to the management, operation and requirements of an ISMS and comprises of the clauses summarised in figure 1.

“Annex A – Information Security Controls” contains a comprehensive list of 93 controls and objectives arranged into control areas (see Figure 2). The primary purpose of these controls is to assist in the management and treatment of risk.

Figure 1. ISO 27001 Management of the ISMS

- Clause 4: Context of the organisation
- Clause 5: Leadership
- Clause 6: Planning
- Clause 7: Support
- Clause 8: Operation
- Clause 9: Performance evaluation
- Clause 10: Improvement

Figure 2. ISO 27001 Annex A Control Areas

- Organisational (37 controls)
- People (8 controls)
- Physical (114 controls)
- Technological (34 controls)

ISO 27001 METHODOLOGY

Toro will interview key staff, suppliers, review all relevant policies, governance procedures and documentation, access networks and systems to assess and test the technical configurations and architecture, and their robustness.

The areas reviewed are:

People Controls

- Screening
- Contractual T&Cs
- Information Security Awareness, Education & Training
- Confidentiality
- Remote Working
- Reporting

Physical Controls

- Perimeters
- Entry
- Offices, rooms & facilities
- Monitoring
- External & Environmental Threats
- Equipment Security
- Storage Media
- Secure Disposal

Organisational Controls

- Information Security Policies
- Information Security Roles & Responsibilities
- Threat Intelligence
- Asset Management
- Information Classification
- Access & Identity Controls
- Supply Chain
- Cloud Services
- Incident Management
- Business Continuity
- Data Protection
- Regulation & Compliance

Technological Controls

- Mobile Devices
- Privileged Access Rights
- Authentication
- Malware
- Technical Vulnerabilities
- Configuration
- Data Leak Prevention
- Backup
- Logging & Monitoring
- Network Security
- Web Security
- Cryptography
- Development & Testing
- Change Management

ISO 27001 METHODOLOGY

The typical roles interviewed as part of this process are:

ISO 27001 Clause / Control	Objectives & Requirements	Typical Roles Responsible
Section 4	Understanding the organisation and its context, the scope, and the needs and expectations of interested parties	• Chief Executive Officer • Chief Operations Officer • Chief Information Officer • Quality Manager / Auditor • Information Security Manager
Section 5	Leadership and commitment to the ISMS, policy, and roles and responsibilities	• Chief Executive Officer • Chief Operations Officer • Chief Information Officer • Quality Manager / Auditor • Information Security Manager
Section 6	Information security objectives, risk assessment, and risk treatment	• Chief Risk Officer • Chief Information Officer • Risk Manager • Information Security Manager
Section 7	Provision of resources, competence, information security awareness, communication and documentation requirements	• Chief Information Officer • Head of HR • Quality Manager / Auditor • Information Security Manager
Section 8	Operational planning and control including near to medium-term planning, risk assessment and risk treatment plans	• Chief Operations Officer • Chief Risk Officer • Chief Information Officer • Risk Manager • Quality Manager / Auditor • Information Security Manager
Section 9	Measurements and metrics, auditing and Management Reviews	• Chief Information Officer • Head of IT • Senior IT Manager • Quality Manager / Auditor • Information Security Manager
Section 10	Managing continual improvement, non-conformity and corrective actions	• Chief Risk Officer • Chief Information Officer • Risk Manager • Quality Manager / Auditor • Information Security Manager

ISO 27001 METHODOLOGY

- The AS-IS Gap Analysis against ISO 27001 will identify the areas of people, process and technology that do not meet best practice.

- Gaps will be risk assessed and prioritised for remediation.

- A TO-BE implementation roadmap will identify the tasks and projects that need to occur to reduce risk to the organisation.

NIST METHODOLOGY

IDENTIFY

- Asset Management
- Business Environment
- Governance
- Risk Assessment
- Risk Management Strategy

PROTECT

- Access Control
- Awareness and Training
- Data Security
- Information Protection Processes and Procedures

DECTECT

- Anomalies and Events
- Security Continuous Monitoring
- Detection Processes

RESPOND

- Response Planning
- Communications
- Analysis
- Mitigation
- Improvements

RECOVER

- Recovery Planning
- Improvements
- Communications

NIST METHODOLOGY

Toro will conduct a Gap Analysis against the NIST Cybersecurity Framework

1. **Identify** — Critical assets and associated risks.
2. **Protect** — Delivery of business functions by applying appropriate security controls.
3. **Detect** — Monitoring and alerting of suspicious activity, intrusion or attack.
4. **Respond** — Incident management and stakeholder communication.
5. **Recover** — Repair damage, restore operations and return to BAU.

NIST METHODOLOGY

Toro will tier the client based on their maturity across the five functions of NIST. Security maturity is impacted by the level of risk, business constraints and the business risk appetite, regulatory requirements and the supply chain.

	Level 1 Initial	Level 2 Repeatable	Level 3 Defined	Level 4 Managed	Level 5 Optimised
Identify	Little to no cybersecurity risk identification.	Process for cybersecurity risk identification exists, but it is immature.	Risks to IT assets are identified and managed in a standard, well defined process.	Risks to the business environment are identified and proactively monitored on a periodic basis.	Cybersecurity risks are continuously monitored and incorporated into business decisions.
Protect	Asset protection is reactive and ad hoc.	Data protection mechanisms are implemented across the environment.	Data is formally defined and protected in accordance with its classification.	The environment is proactively monitored via protective technologies.	Protective standards are operationalised through automation and advanced technologies.
Detect	Anomalies or events are not detected or not detected in a timely manner.	Anomaly detection is established through detection tools and monitoring procedures.	A baseline of 'normal' activity is established and applied against tools / procedures to better identify malicious activity.	Continuous monitoring program is established to detect threats in real-time.	Detection and monitoring solutions are continuously learning behaviours and adjusting detection capabilities.
Respond	The process for responding to incidents is reactive or non-existent.	Analysis capabilities are applied consistently to incidents by Incident Response (IR) Roles.	An IR Plan defines steps for incident preparation, analysis, containment, eradication, and post-incident.	Response times and impacts of incidents are monitored and minimised.	The capabilities of all IT personnel, procedures, and technologies are regularly tested and updated.
Recover	The process for recovering from incidents is reactive or non-existent.	Resiliency and recovery capabilities are applied consistently to incidents impacting business operations.	A Continuity & Disaster Recovery Plan defines steps to continue critical functions and recover to normal operations.	Recovery times and impacts of incidents are monitored and minimised.	The capabilities of all IT personnel, procedures, and technologies are regularly tested and updated.

NIST METHODOLOGY

- The AS-IS Gap Analysis against NIST Cybersecurity Framework will identify the areas of people, process and technology that do not meet best practice.

- Gaps will be risk assessed and prioritised for remediation.

- A TO-BE implementation roadmap will identify the tasks and projects that need to occur to reduce risk to the organisation.

Case Studies

Security Frameworks in Practice

CRITICAL CONTROLS FRAMEWORK

Client Requirements / Problems	Medium sized financial services fund manager suffered ransomware attack
Toro Response	• Incident response and investigation. • Review of monitoring and alerting capabilities. • Review of 3rd party IT MSP and SOC capabilities to respond to an attack.
Outcome	• Identification of gaps in process and technology between supply chain responsible for monitoring, alerting, responding, isolating and blocking attempts at intrusion into the network. • Network segmentation recommendations designed. • Implementation of benchmarked against CIS Critical Security Controls framework. • Ongoing virtual CISO services to management risk and vulnerabilities.

INCIDENT MANAGEMENT

Client Requirements / Problems	Large financial services company needed to assess incident readiness and digital forensic capabilities.
Toro Response	Full cyber review of incident management capabilities against ISO 27001 including monitoring, logging, threat intelligence, detection and response capabilities. Assessment of: • Isolation and preservation of endpoint devices in their entirety • Microsoft Defender for Endpoint monitoring, response and analytics • SIEM and SOAR via Splunk ingesting Microsoft Office 365, Watchguard, Fortinet, Insights and AWS logs • CloudGuard Dome9 • Qualys vulnerability management
Outcome	• Multiple recommendations were identified including: • Communication with business stakeholders • Supply chain risk management • Classification of data • Role based access • Backup regime • Procedural based documentation (as opposed to high level policy documents) • Testing of logs available • Security review of coding and cloud infrastructure configuration

SERVICE ASSET & CONFIGURATION MANAGEMENT

Client Requirements / Problems	Medium sized private bank requested assistance to address internal audit recommendations relating to asset management, in alignment with ISO 27001 and PRA CQUEST.
Toro Response	• Review of asset management against ISO 27001. • Simultaneously assess compliance against PRA CQUEST. • Existing systems, products, policies, procedures and processes were evaluated.
Outcome	• It was identified that 50% controls were non-compliant with ISO 27001. • A practical process for the bank to implement effective asset management was drafted including roles & responsibilities. • A draft asset management policy was drafted. • 24 recommendations were detailed relating to inventory, ownership, acceptable use, handling and disposal of assets. • Detailed implementation instructions were provided to guide the internal IT department in implementing an effective single point of truth CMDB. • A CMDB maintenance process was developed to track assets through procurement, deployment, compliance, maintenance & support, configuration, decommission, disposal, consolidation and reporting.

VULNERABILITY MANAGEMENT

Client Requirements / Problems	Large global think tank lack of visibility of vulnerabilities across their estate. Medium finance asset management company required review of their vulnerability management standard, policies and procedures.
Toro Response	• Reviewed vulnerability management requirements and documentation baselined against Cyber Essentials and ISO 27001. • Assessed the technology and processes in place to manage vulnerabilities. • Worked with internal IT team to push out Qualys cloud agent to servers and endpoints (leveraging centralised device management tools). • Review of documentation, application of industry standard best practice (baselined against Cyber Essentials and ISO 27001), re-write of policies & procedures
Outcome	• Drafted updates to policies and procedures. Made recommendations to process. • Tens of thousands of vulnerabilities reported on. Provided visibility for IT to assess, prioritize, and patch critical vulnerabilities. Continuous processing of telemetry data in real time and customised reporting. • Benchmarked against industry standards to prioritise vulnerabilities and report against frameworks. • Leveraged the newly implemented tooling to supplement vulnerability remediation.

PATCH MANAGEMENT

Client Requirements / Problems	Small financial services company without adequate patch management. Medium sized construction company with no patch management.
Toro Response	• Reviewed existing patch management requirements and documentation. • Assessed technology (or lack of) in place to deliver patching and determined insufficiencies. • Implementation of vulnerability management and RMM tools to report on, prioritise and deliver Cyber Essentials compliant patch management
Outcome	• Implemented products and process to ensure effective patch management. • Solutions utilised a combination of RMM tooling and Intune/Endpoint Manager for Azure AD joined machines, or JAMF Pro for Apple devices, to automate operating system, Microsoft office and 3rd party software and application patching. • Combined with Qualys cloud agent vulnerability scanning to report on and prioritise vulnerabilities related to patch management by CVSS score. • Automated status dashboard and reporting to clients.

NETWORK SEGMENTATION

Client Requirements / Problems	Medium sized manufacturer suffered a ransomware and extortion attack – a contributory factor was the flat structure of their network
Toro Response	• Incident response and investigation. • New network architecture designed to increase security, deter compromise and address the vulnerabilities that contributed to ransomware and extortion. • Benchmarking against ISO 27001 controls.
Outcome	• A zero trust, zonal network with a hybrid approach to delivery of services for business, a secure environment resilient to attack and visibility of the estate for the IT team was designed in detail. • This design was implemented applying the concept of a global area network utilising mesh network technologies and software designed networking.

MACHINE HARDENING

Client Requirements / Problems	Medium sized financial services company required assurance that their 3rd party IT MSP had adequately hardened their machine builds and remote desktop environment which had previously been compromised by attackers.
Toro Response	• Reviewed machine hardening process and procedure. • Reviewed and tested local firewall and group policy applied to remote desktop environment. • Reviewed and tested machine build security controls applied by Microsoft Intune. • Baselined all machine hardening controls against the CIS Critical Security Controls benchmark.
Outcome	• Identification of misconfigured controls and insufficient monitoring, event management and alerting. • Preparation of work packages to implement remediations. • Deployment of endpoint security including EDR/XDR to secure all devices, including continuous monitoring, alerting and event management functions. • Group policy usage to ensure correct configuration for relevant devices, including vulnerability fixes.

BACKUP STRATEGY

Client Requirements / Problems	Professional services company move from on-premises file storage and local/physical offsite backups to cloud platforms and need to evolve backup strategy.
Toro Response	• Reviewed and optimised current backup strategy, solution, process and procedures. • Assessed backup capabilities against disaster recovery and business continuity plans. • Aligned with ISO 27001 and ISO 27002 requirements.
Outcome	• Scoped and tested multiple different cloud backup options as appropriate to the business. • Implemented a new backup solution to meet ISO 27001 and ISO 27002 standards. • Extend backup to include commonly forgotten SaaS resources.

TOOLING

Client Requirements / Problems	A UK-headquartered (re)insurance broker concerned about the security of one of its Nigerian based multinational oil and gas clients.
Toro Response	• Deployed a consultancy team and PMO to Lagos to conduct a comprehensive review of the business's endpoint security (~5,000 computers) • Delivered a NIST based cyber maturity audit of strategy, governance, systems, processes and controls.
Outcome	• Changes in global security policy • Improvements in network security • Mass migration to Windows 10 • Implementation of security incident and monitoring team • A SIEM solution to view and track incidents across multiple sources.

AZURE SERVICES

Client Requirements / Problems	Medium sized challenger Internet Service Provider using Microsoft 365 and Azure infrastructure
Toro Response	• Assessed the threat profile and determine the risk appetite of the organisation to implement appropriate levels of security controls for their Azure and Microsoft 365 environment. • Determined the ISO 27001 controls framework to meet.
Outcome	• Application of Microsoft baselines. • Recommendation for Defender for Cloud to address security posture remediations integrated with Azure. • Recommended implementation Microsoft Cloud Security Benchmark addresses Network security; Identity Management; Privileged Access; Data Protection; Asset Management; Logging and Threat Detection; Incident Response; Posture and Vulnerability Management; Endpoint Security; Backup and Recovery; DevOps Security; Governance and Strategy.