Tom Brown, CISSP, ISO 27001 Lead Auditor

Summary

Tom Brown is a highly experienced cybersecurity assessment, cyber risk, and security engineering leader with more than three decades of experience across government, international programmes, critical infrastructure, finance, energy, aviation, high technology, privacy, and global supply chain security. His background combines hands-on technical depth with strategic judgement, public-sector experience, and a proven ability to deliver practical cyber resilience improvements in complex environments.

Tom is especially well suited to cybersecurity consulting, international cyber resilience programmes, national or organisational cyber risk assessments, ICT security reviews, supplier and cloud security assessments, critical infrastructure protection, vulnerability management, privacy engineering, and security governance engagements.

For international organisations such as the United Nations, Tom offers a rare combination of technical assessment expertise, international cyber capacity-building experience, public-sector credibility, supplier assurance knowledge, and pragmatic risk management. He can help organisations identify material cyber risks, prioritise improvements, strengthen resilience, and develop cybersecurity programmes that are both strategically sound and operationally achievable.

Professional Cybersecurity Assessment Bio

Tom Brown is a UK-based information security, cyber risk, and security engineering specialist with more than 30 years of experience assessing, designing, securing, and improving complex technology environments across government, international programmes, critical national infrastructure, finance, energy, aviation, high technology, privacy engineering, and global supply chain security. His career includes senior technical and leadership roles with Apple, the UK Home Office, and major public and private sector organisations, where he has combined deep engineering expertise with strategic cybersecurity leadership.

Tom brings a strong blend of hands-on technical capability, public-sector experience, international cybersecurity advisory work, and practical risk management. He has supported organisations and governments in understanding their cybersecurity posture, identifying material risks, improving resilience, and making informed investment decisions. His background makes him especially valuable in cybersecurity assessments, cyber resilience reviews, ICT security evaluations, vulnerability management programmes, supplier assurance, privacy engineering, and critical infrastructure protection.

Cybersecurity Assessment and Risk Leadership

Tom's recent work has focused on international cyber risk assessment and cyber capability development. He has delivered cyber risk assessment and improvement programmes for UK Overseas Territories and other national governments, helping senior leaders understand cyber exposure, priorities investments, and strengthen resilience across critical national infrastructure and essential services.

His assessment work aligns closely with the types of responsibilities often required by international organisations, including ICT security assessments, cyber risk management, vulnerability management, security governance, organisational resilience, and practical improvement planning. Tom is experienced in evaluating cyber risk from both a technical and strategic perspective, ensuring that findings are not only accurate, but also usable by executives, operational leaders, engineers, suppliers, and public-sector stakeholders.

Throughout his career, Tom has worked in complex, politically sensitive, and multi-stakeholder environments. He is highly effective at translating technical findings into practical decisions for senior leaders, legal teams, operational teams, engineers, suppliers, and government partners. His ability to communicate risk clearly across these groups is especially valuable in international cybersecurity programmes where technical, political, operational, and funding considerations must be carefully balanced.

International Cyber Risk and Capability Development

Tom has significant experience supporting national and regional cybersecurity improvement efforts. His work with UK Overseas Territories and other national governments has included assessing cyber risk, identifying gaps in resilience, supporting strategic investment decisions, and helping develop practical improvement programmes that reflect local priorities, operational realities, and available resources.

This international cyber capability work requires more than traditional assessment experience. It demands strong judgement, cultural awareness, stakeholder management, and the ability to develop pragmatic recommendations that can be implemented in real-world environments. Tom has demonstrated the ability to work across government, infrastructure, supplier, and technical communities to help organisations strengthen their cyber posture in a sustainable way.

For international organisations such as the United Nations, this experience is particularly relevant. Tom understands how to assess cybersecurity maturity across diverse operating environments, how to prioritise improvements based on risk, and how to support cyber resilience initiatives that must operate across national, regional, and organisational boundaries.

Critical Infrastructure, Security Architecture, and Cyber Defense

Tom’s background includes extensive experience across cyber defence operations, security architecture, industrial control systems, aviation security, power generation, financial services, web systems, enterprise data exchange, and cloud security governance. He has led and contributed to major security assurance and cyber defence programmes involving critical infrastructure and high-value operational environments.

Earlier in his career, Tom designed security detection operations, developed enterprise data exchange architectures, supported cyber collaboration between external organisations, and led security assurance across industrial control systems, airport infrastructure, power generation environments, web platforms, and financial systems. This broad technical foundation gives him the ability to assess environments deeply, understand complex dependencies, and identify risks that may not be visible through policy review alone.

His work has included the assessment and acceptance of new security technologies, supplier management, operational process improvement, and mentoring of security engineers. This combination of assessment, architecture, operations, and leadership experience allows Tom to evaluate cybersecurity programmes from multiple angles, including governance, technical control design, operational maturity, resilience, and implementation feasibility.

Apple Experience: Privacy Engineering and Supplier Trust

At Apple, Tom worked in both privacy engineering and supplier trust roles, contributing to the security and privacy of major products, services, and global operations. His work included improving operational maturity in privacy processes, supporting privacy-by-design approaches, and helping develop practical security and privacy controls for complex environments.

In supplier trust and regional information security assurance roles, Tom supported a large international supplier ecosystem. His work included large-scale supplier risk assessment, acquisition due diligence, compensating control design, and the development of practical risk assessment approaches that improved visibility, prioritisation, and decision-making across global operations.

This experience is especially relevant to organisations that depend on complex supply chains, outsourced technology providers, cloud services, manufacturing partners, and third-party platforms. Tom understands how supplier risk can affect enterprise resilience and how to assess controls in a way that supports both security outcomes and operational needs.

Supplier Assurance, Cloud Security, and Risk Methodology

Tom has strong experience developing and applying risk assessment tools, methodologies, and governance approaches across complex environments. His work has involved supplier assurance, cloud security governance, privacy engineering, acquisition due diligence, and practical compensating control design.

He is skilled at identifying where formal controls may not fully align with operational realities and developing pragmatic approaches that allow organisations to reduce risk while continuing to operate effectively. This is particularly valuable in international and public-sector environments where legacy systems, constrained budgets, supplier dependencies, and critical service obligations often create complex risk decisions.

Tom’s approach to cybersecurity assessment is practical, evidence-based, and business-aware. He focuses on helping organisations understand what risks matter most, what controls are most effective, and what improvements can realistically be achieved.

Executive Communication and Actionable Recommendations

One of Tom's key strengths is his ability to translate complex technical issues into clear, actionable recommendations for decision-makers. He has worked with executives, operational leaders, engineers, legal teams, suppliers, public-sector partners, and government stakeholders to ensure that cybersecurity risks are understood and acted upon.

His communication style is grounded in technical credibility and practical judgement. He is able to explain risk in a way that supports investment decisions, prioritisation, remediation planning, and long-term cyber resilience. This especially important in assessment engagements where findings must be defensible, understandable, and directly tied to business or mission outcomes.

Tom is also experienced in coaching and mentoring security engineers, improving operational processes, managing suppliers, and supporting the introduction and assurance of new security technologies. This combination of leadership, advisory capability, and technical depth enables him to support both strategic planning and hands-on implementation.

Professional Credentials

Tom is a Chartered Engineer and a Member of the Institution of Engineering and Technology. He holds a Bachelor of Engineering with Honours in Electrical and Electronic Engineering and maintains respected professional cybersecurity and assurance qualifications, including CISSP and ISO 27001 Lead Auditor.

His background also includes CESG CHECK Team Leader experience, CESG Listed Advisor Scheme experience, and UK Government systems engineering training. These credentials reflect his strong foundation in technical assurance, secure engineering, information risk management, audit, and government-grade cybersecurity assessment.