RISK LEDGER

Securing Public Sector Supply Chains:

A Comprehensive Guide to the UK Government Cyber Security Strategy

riskledger.com

Introduction

Only last year, the NCSC issued a threat alert warning of escalated threats emanating from cyber attacks by state-sponsored threat actors against UK Critical National Infrastructure. This coincided with a speech by former Cabinet Office minister Oliver Dowden at the CyberUK conference in Belfast, in which he stated that the UK was facing a new adversary, "the cyber equivalent of the Wagner group". These Russian-aligned groups, he explained, initially "focused their attacks on Ukraine and the surrounding region. But recently, they have begun to turn their attention to the UK and its allies". And the UK public sector is a prime target of these stepped up attacks.

The UK government, keenly aware of the scale of the threat, has taken a leadership role in addressing the issue. The Government Cyber Security Strategy (GCSS) 2022-2030, which was already published in January 2022, serves as the backbone of the Government's plan to bolster the public sector's resilience. The Strategy provides a comprehensive framework for strengthening the nation's cyber defences, and places a particular emphasis on supply chain security, where the weakest links in organisations' defences can increasingly be found.

This Regulatory Explainer sets out to provide a comprehensive overview of the GCSS and the NCSC's Cyber Assurance Framework (CAF) that underpins it, and zooms in on their aims and requirements specifically relating to the subject of supply chain cyber risks. It will explain how organisations are expected to harden their resilience to supply chain cyber incidents, and how Risk Ledger's supply chain risk management platform supports public sector organisations in meeting the objectives of the GCSS relating to supply chain security and bolster their collective sectoral resilience through enhanced collaboration. Finally, this white paper will map Risk Ledger's standardised assessment framework for third-party risk management to the Objectives, Principles and Guidance provided by the GCSS and CAF, demonstrating how Risk Ledger enables organisations to harden the security of their supply chains.

The GCSS: An Overview

The GCSS's overarching goal is "for government's critical functions to be significantly hardened to cyber attack by 2025, with all government organisations across the whole public sector being resilient to known vulnerabilities and attack methods no later than 2030." The Strategy set forth objectives, principles and desired outcomes, which are driven by the new GovAssure scheme, and which in turn is underpinned by the NCSCs CAF that defines the objectives and outcomes to be achieved by public sector bodies.

The GCSS is based on two core pillars, with several corresponding objectives.

Pillar 1: Building a Strong Foundation

This pillar focuses on ensuring that government organisations have the right structures, mechanisms, tools, and support to manage their cyber security risks effectively. It is underpinned by the adoption of the National Cyber Security Centre's (NCSC) Cyber Assessment Framework (CAF).

Objectives under Pillar 1

Manage security risk:

Organisations must identify, assess, and understand risks, including those from their supply chains. Clear accountability and robust assurance processes will ensure proper risk management.

Defending against cyber attacks:

Implement proportionate cyber security measures and embed them in government technology and digital services. Shared capabilities and tools will improve overall security and efficiency.

Detecting cyber security events:

Develop capabilities to monitor systems, networks, and services to detect potential threats before they become incidents. Enhanced coordination will allow for rapid and coherent responses.

Pillar 2: Defend-as-One

This pillar emphasises the need for a comprehensive and unified response to cyber security threats. It involves sharing cyber security data, expertise, and capabilities across government organisations to create a stronger collective defence.

Objectives under Pillar 2

Minimising the impact of cyber security incidents:

Be prepared to respond to incidents effectively, restore affected systems quickly, and resume operations with minimal disruption. This includes testing and exercising incident response plans and learning from incidents.

The role of the NSCSs CAF, GovAssure and GovS 007 in the GCSS

GovAssure on the other hand is the new cyber security assurance scheme for Government organisations, designed to support the objectives of the Government Cyber Security Strategy. It is underpinned by the NCSC's CAF and uses the aforementioned government-specific profiles (Baseline and Enhanced) to assess outcomes and identify the extent and success of cyber risk management.

The revised 007 Security Functional Standard will direct organisations to go through GovAssure. This alignment ensures consistency in the government's approach to cyber security assurance. These components collectively support the GCSS's key pillars.

By leveraging the CAF's IGPs, the UK government is working towards a more coordinated and robust cyber security posture across its entire estate. They are therefore the essential tools to harden the government's critical functions to cyber attacks by 2025, and to ensure all government organisations are resilient to known vulnerabilities and attack methods by 2030.

Adapted CAF profiles for different public sector bodies

Depending on the specific requirements of different sub-sectors, the aforementioned sector-specific CAF profiles are determined collaboratively by sector-specific regulators, competent authorities and oversight bodies, often in consultation with the NCSC.

Sector-specific regulators or competent authorities define CAF profiles for their industries. They prioritise contributing outcomes based on what is most critical to manage security risks to essential functions, setting targets for "achieved", "partially achieved" and "not achieved".

Some of the regulators or competent authorities that have already defined their own CAF profiles include, for example:

NHS England

NHS England has adopted a CAF-aligned Data Security and Protection Toolkit (DSPT) for healthcare organisations. They have enhanced the NCSC's existing cyber framework with a health and care CAF overlay that covers data protection, confidentiality, and other information governance disciplines. This will likely remain the guiding framework for UK healthcare providers even after NHS England has been abolished and its operations incorporated into the Department of Health and Social Care (DHSC).

Aviation

The UK Civil Aviation Authority (CAA) has developed the CAF for Aviation, adapting it from the NCSC's core CAF v3.0 to meet aviation-specific needs. It focuses on fourteen principles across four objectives, emphasising outcome-focused assessments rather than rigid compliance checklists. Entities must undergo a verification audit, conducted either by the CAA's Cyber Security Oversight team or an ASSURE cyber auditor, and upon successful completion of all stages, the CAA issues a Certificate of Compliance.

Energy sector

Ofgem has published guidance that clarifies the use of the CAF to assess compliance within the energy sector. In August 2023, it released a "CAF Overlay," which provides detailed guidance on how the CAF principles apply specifically to the energy sector, helping entities demonstrate compliance.

Communications sector

Ofcom uses the NCSC's CAF as a means of systematically and comprehensively assessing the extent to which cyber risks are being managed by Operators of Essential Services (OES). It has developed guidance for the digital infrastructure subsector, which includes information on how the CAF should be applied.

Local Authorities

While not fully implemented yet, the Department for Levelling Up, Housing and Communities (DLUHC) has also adapted the NCSC's CAF to address the unique risks faced by local authorities. This tailored version, known as the CAF for Local Government, helps councils, housing associations and other local authorities assess and improve their cyber resilience by focusing on critical systems and vulnerabilities that could disrupt essential services. The CAF for Local Government is being rolled out in phases. The initial stages, including preparing for the CAF, setting the scope, and completing self-assessments, are already available. The full service, including critical system assessments and independent assurance reviews, is expected to launch in spring 2025.

Meanwhile, the Government Security Group (GSG) oversees the implementation of the Cyber Assessment Framework (CAF) for UK government departments and Arm's Length Bodies. The GSG, in collaboration with the National Cyber Security Centre (NCSC) and the Central Digital and Data Office (CDDO), ensures that core government organisations adopt the CAF. The GSG also coordinates with the Government Cyber Coordination Centre (GCCC), a joint initiative involving the GSG, CDDO, and NCSC, to enhance the sharing of cyber security data and threat intelligence across government organisations. The GSG, in collaboration with the NCSC, also developed the government-specific CAF profiles that outline the outcomes required by these organisations. These profiles include both Baseline and Enhanced levels, tailored to the varying risks faced by different entities.

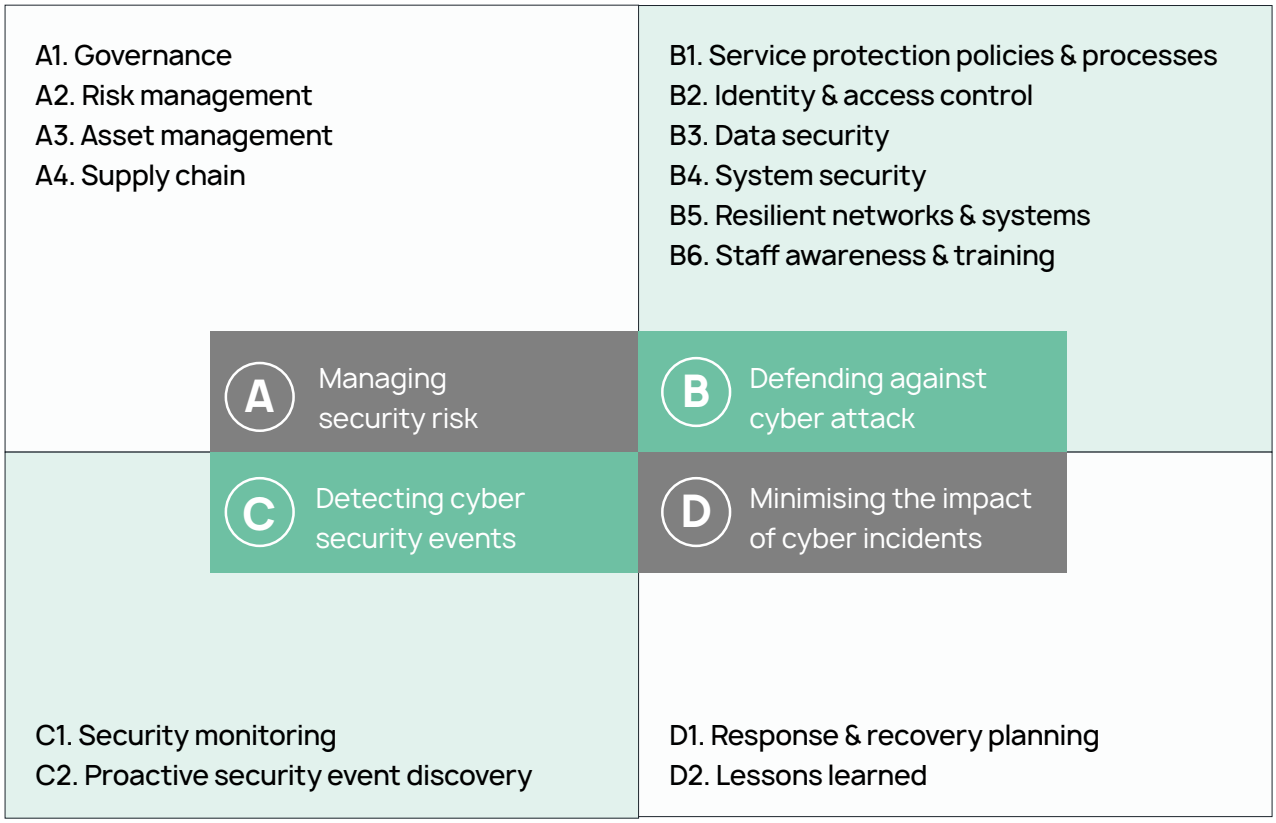
Under the GovAssure scheme, government departments and arm's length bodies are required to review each CAF IGP, provide evidence of compliance, and justify their responses. Independent auditors verify these responses to ensure consistency and accuracy across departments.

What are the expected outcomes

According to the GCSS, the overall outcome the UK government expects is:

> Government organisations that are determined to be responsible for critical functions will meet the outcomes set out in an 'Enhanced' CAF profile by 2025. All central government departments will meet outcomes set out in their designated CAF profiles by 2026. All other government organisations will meet outcomes set out in a 'Basic' CAF profile by 2030.

To drive this overall outcome, the GCSS outlines a set of key principles under each of the Strategy's four main objectives—Manage Cyber Security Risk, Protect Against Cyber Attacks, Detect Cyber Security Events, and Minimise the Impact of Cyber Incidents. These principles are directly linked to the IGPs in the CAF that government departments and arm's length bodies are expected to achieve.



The expected outcomes under each of the four key objectives set out by the GCSS are as follows:

Principle	Expected Outcomes
A. Managing Cyber Risk	1. Government has established governance arrangements with clear accountability enabling effective management of cyber risks at all levels of government 2. Government has comprehensive visibility and understanding of its digital assets enabling it to identify and manage vulnerabilities and the cyber security risks they present 3. Government has comprehensive visibility of the data it handles and shares so that it can appropriately assess and respond to the risks it presents 4. Government understands and manages risks emanating from commercial suppliers 5. Government understands the threat it faces relative to its functions in order to plan appropriate mitigations, at both an organisational and cross-government level 6. Government organisations have timely access to relevant and actionable cyber security data that enhances their ability to make effective risk management decisions 7. Government cyber security assurance provides government with the visibility it needs to make effective decisions and the confidence that it has appropriate cyber security measures in place to manage the risks to its functions 8. Strategic partnerships with the private sector and international partners are further embedded to enhance proactive defence at a global scale
B. Protect Against Cyber Attack	9. Government adopts a common approach to 'secure by design' to ensure that appropriate and proportionate cyber security measures are embedded within the technology government uses, and that the security of digital services is continually assured throughout their lifecycle 10. Government organisations deploy cyber security controls commensurate with their risk profile to ensure that risks to their functions are managed proportionately 11. Government technology is appropriately configured, with standard profiles for common technology and architectures being developed and continuously updated 12. Shared capabilities, tools and services tackle 'common' cyber security issues at scale 13. Government data is classified appropriately and handled and shared in a way commensurate to the risk it presents
C. Detect cyber security events	14. Government networks, systems, applications and end points are monitored to provide proportionate internal detection capability 15. Shared detection capability provides detection at scale across government
D. Minimise the impact of cybersecurity incidents	16. Government is fully prepared to respond to cyber incidents 17. Government rapidly responds to cyber incidents, both organisationally and across government 18. Government restores systems and assets affected by cyber security incidents and resumes the operation of its functions with minimal disruption 19. Lessons learned from cyber incidents drive improvements in government's cyber security
E. Develop the right cyber security skills, knowledge and culture	20. All Government cyber security skills requirements are understood 21. Government attracts and retains the diverse cyber security workforce it needs to be resilient 22. Government continuously develops its cyber security workforce to ensure that it has and retains the skills it needs 23. Sufficient cyber security knowledge and awareness across government's professional functions ensures that cyber security is actively taken into consideration 24. Government has a cyber security culture that empowers its people to learn, question and challenge, enabling continuous improvements in behaviours and resulting in sustainable change

Supply Chain Security in the GCSS and CAF

This Explainer will now take a closer look at the supply chain security aspects of the GCSS. The GCSS places significant emphasis on addressing supply chain risks in the UK public sector in order to safeguard UK public services and the security of critical government and social assets. As already stressed in the Introduction to this Explainer, securing public sector supply chains is a crucial aspect of hardening the sector's overall resilience to cyber security threats, but it is also the most difficult to achieve in practice.

This is not least because of the inherent complexity of government supply chains, as the GCSS acknowledges itself when noting that their size and diversity make effective risk management challenging. This recognition, however, is crucial, as it sets the stage for a measured, yet comprehensive, approach to supply chain cyber security across the UK public sector.

The GCSS overall approach and rationale regarding supply chain security can be found under Principle 4, which states:

> The organisation understands and manages security risks to networks and information systems supporting the operation of essential functions that arise as a result of dependencies on external suppliers. This includes ensuring that appropriate measures are employed where third party services are used.

The detailed outcomes, as set forth in the CAF, on supply chain cyber security are as follows:

Partially achieved (all of the below are correct)	Fully achieved (all of the below are correct)
You understand the general risks suppliers may pose to your essential function(s). You know the extent of your supply chain that supports your essential function(s), including sub-contractors.	You have a deep understanding of your supply chain, including subcontractors and the wider risks it faces. You consider factors such as supplier's partnerships, competitors, nationality and other organisations with which they subcontract. This informs your risk assessment and procurement processes.
You understand which contracts are relevant and you include appropriate security obligations in relevant contracts	Your approach to supply chain risk management considers the risks to your essential function(s) arising from supply chain subversion by capable and well-resourced attackers.
You are aware of all third-party connections and have assurance that they meet your organisation's security requirements.	You have confidence that information shared with suppliers that is essential to the operation of your function(s) is appropriately protected from sophisticated attacks.
Your approach to security incident management considers incidents that might arise in your supply chain.	You understand which contracts are relevant and you include appropriate security obligations in relevant contracts. You have a proactive approach to contract management which may include a contract management plan for relevant contracts.
You have confidence that information shared with suppliers that is necessary for the operation of your essential function(s) is appropriately protected from well-known attacks and known vulnerabilities.	Customer / supplier ownership of responsibilities is laid out in contracts.
	All network connections and data sharing with third parties are managed effectively and proportionately.
	When appropriate, your incident management process and that of your suppliers provide mutual support in the resolution of incidents.

As part of the Strategy, the government also raises expectations for critical and cross-government suppliers, while ensuring requirements remain proportionate and robust for smaller, bespoke suppliers.

Cyber Essentials will serve as a foundational tool to confirm suppliers have appropriate protections. Alignment between commercial and security functions will integrate cyber security into every procurement process, enabling clear articulation of requirements based on risk. Procurement frameworks and contracts will be strengthened to ensure risk-based commercial arrangements, supported by robust clauses for managing subcontractors and procuring secure tools and services by default.

The importance of supply chain visibility and identifying systemic risks

A key focus when it comes to supply chain security and resilience in the GCSS, as is also the case in the new operational resilience regulations such as DORA or NIS2, is the fundamental importance of enhanced visibility into supply chain dependencies beyond immediate 3rd parties, into 4th, 5th and nth parties. In the words of the GCSS, in order to achieve greater resilience and enhanced supply chain security, "visibility is the foundation from which an accurate assessment of risk can be derived", and only an "improved understanding of suppliers and their dependencies will…enable government to better respond to cyber security incidents that emanate from the supply chain."

Implicit in the GCSS and all other new regulations seeking to harden the resilience of operators of CNI is the desire of regulators and governments to also identify shared systemic and concentration risks as well as potential single points of failure that would be impossible for individual entities to identify.

To get into a position to be able to do so, the GCSS, as a first step, aspires to the central mapping of all government's critical and common suppliers, not least in order to identify and manage systemic and aggregate supply chain risks. The central oversight of critical suppliers will also allow regulators to promote standardised requirements, reinforce proportionate cyber security controls, and reduce duplication, driving efficiencies for both government organisations and their suppliers.

Improved understanding of suppliers and their dependencies will also enhance the government's ability to respond to cyber security incidents originating in public sector supply chains. It will enable more focused engagement with suppliers, supporting a swifter and more effective incident management. It is envisioned that the Government Cyber Coordination Centre (GCCC) will play a critical role in facilitating this process.

To summarise, the three key and very much related goals of the GCSS with respect to improved supply chain risk management and greater resilience are thus:

The central mapping of the sector's extended supply chain dependencies;

The identification of concentration and shared systemic risks; and

Enabling a more efficient engagement with suppliers to ensure swift and effective incident management when an incident does occur.

Key challenges with complying with GCSS and CAF requirements

Based on numerous conversations that Risk Ledger has had over the past few months and years with numerous public sector bodies across the UK, ranging from large ministerial departments and their arms length bodies, to local authorities and police forces, some of the key challenges public sector bodies are facing in their efforts to meet the GCSS and CAF requirements include:

Challenge 1: Restricted budgets and limited resource

This challenge is especially pressing for local authorities, which are increasingly asked to do more with less, experiencing severe budget constraints. With such limited resources, local authorities are often limited in how much they can invest in their cyber security defences and TPRM processes to adequately protect the large amounts of sensitive data (think about all the personal details they hold in relation to Council Tax alone) that they hold. In a 2023 survey, more than a quarter of Councils said they had made "no progress" on cyber security, and 59% said their approach to cyber security was "outdated", demonstrating the extent of the challenge they face.

Challenge 2: Lack of supplier engagement

A more commonly shared challenge with bolstering their supply chain security and operational resilience from supply chain incidents is that supplier responsiveness and level of engagement with their clients' security teams often leaves much to be desired. Also, suppliers have little incentive to engage in time consuming manual and often still spreadsheet-based processes. They often receive hundreds of different security questionnaires from their different clients, making this a hugely time and resource-consuming process for suppliers as well. This largely unnecessary duplication of assessments causes bottlenecks in completing requests, impacting both suppliers and their public sector clients. Individual public sector bodies often only have limited leverage against unresponsive suppliers, and are thus unable to influence change. Furthermore, more effective information sharing between clients and their third-parties thus also remains limited as a result.

Challenge 3: Lack of visibility into their extended supply chains

Today, threats can appear anywhere in public sector bodies' vast extended ecosystem of supply chain relationships, far beyond third-parties, in 4th, 5th and nth parties. This could be clearly witnessed during impactful supply chain attacks such as Solarwinds, Log4J or MOVEit Transfer, where organisations were impacted by incidents in suppliers that they didn't even use directly, but which one or more of their critical suppliers relied on.

Assuring the security of direct suppliers is thus no longer enough. But organisations have commonly no easy way to achieve visibility into risks beyond their third-parties. However, understanding dependencies and risks in the wider supply chain ecosystem is a prerequisite for enhanced supply chain security, as well as for identifying hidden concentration risks - which exist, for example, when numerous critical third-parties of an organisation are all dependent on the same fourth party supplier. This kind of dependency, however, could also exist further down the supply chain, in 5th, 6th or nth parties.

Challenge 4: A siloed approach to TPRM

As supply chain dependencies are ballooning, it has become almost impossible for individual security teams to assure the security of each supplier individually and continuously monitor them on their own. The lack of a standardised assessment framework as well as concerns around sharing information on their own organisation's supply chain connections and risk insights, among other factors, hinder greater collaboration between the security teams of different organisations.

This lack of collaboration does not only result in a lot of unnecessary duplication of work and prevents a more scalable and resource-efficient approach to TPRM. It also preempts enhanced visibility into critical sectoral supply chain dependencies. These dependencies could affect multiple critical suppliers of public sector clients at the same time if breached, and thus makes any fallouts even more difficult to respond to when they occur. Having access to this contextual knowledge, as the GCSS recognises, is the essence bolstering operational resilience both for individual organisations and entire sectors.

Challenge 5: Inability to obtain supplier information quickly during emerging threats

During emerging supply chain attacks, public sector bodies need to quickly understand and appreciate the risk to themselves from their supply chain, but they don't usually have the capacity to check all of their suppliers at scale, and they may also not have their full supplier list to hand. In these scenarios, the lack of access to and relationships with the security teams at their suppliers becomes particularly detrimental. Since security teams need to collect data to make informed decisions on the risk a particular supplier might pose to them, they usually put together their own set of questions and send them over email, with a deadline for responding. They then manually track responses via spreadsheets, confluence pages, google documents etc. All of the above takes too long, however, and involves a lot of manual work, significantly delaying response times.

How Risk Ledger is helping the UK public sector enhance sectoral resilience

Traditional Third-Party Risk Management (TPRM) has fundamental limitations. It is time-consuming, resource-heavy, and often reliant on manually completed supplier questionnaires, making it difficult to identify concentration risks and systemic risks. Additionally, TPRM is typically conducted in silos, preventing organisations from sharing intelligence and leading to inefficiencies and duplicated efforts.

To enhance their operational resilience and meet the GCSS and CAF requirements relating to supply chain security, public sector organisations must first gain better visibility into their extended supply chains. As the GCSS argued, visibility is the foundation for greater supply chain resilience. By identifying hidden vulnerabilities, they can implement mitigation strategies or determine whether risks align with their appetite. However, this is a resource-intensive challenge—especially for public sector bodies operating under budget constraints.

A collaborative approach can address these challenges by acting as a force multiplier for public sector bodies. By working together, organisations can map risks across a shared supply chain, leveraging collective resources to uncover systemic risks that would be difficult to detect individually.

Risk Ledger is already actively working to foster communities within the public sector to leverage their collective resources by providing them with the necessary insights to identify concentration risks that may have previously only been possible with significantly more funding.

In one such community, we brought together ten Local Authorities where they can view risks raised by their peers against specific suppliers , discuss best practices to mitigate these risks, and collaboratively engage with suppliers to address these risks. Moreover, they will be able to collaborate on supply chain attacks as they occur, significantly improving their access to up-to-date information from suppliers to determine the extent they may be exposed to any attack or disruption. Finally, by overlaying each of their supply chain maps, they are able to have visibility across the entire supply chain, and identify potential concentration risk that may pose a threat to the entire community, that may not have been known if this had been done in isolation.

This collaborative approach offers significant advantages since public sector bodies often use the same suppliers. This shared oversight ensures multiple entities are monitoring each supplier while eliminating duplicate efforts, ultimately enabling both collective assurance and unified risk management.

To counter the rising risks posed by supply chain vulnerabilities, industry-wide collaboration between threat intelligence teams has become an established practice. There is close collaboration, for example, between such teams at the largest financial organisations, facilitated by the Financial Services Information Sharing and Analysis Center (FS-ISAC). Similar collaboration exists in other industries.

However, the same level of collaboration between peers does not yet exist between third-party risk management (TPRM) teams of different organisations, which continue to work largely in siloes in their own organisations. But TPRM teams must wonder every time they review an existing or prospective supplier: someone else must have clearly done this work already? The solution is to share TPRM efforts with others across industries with often overlapping supply chains and facing similar regulatory and other pressures.

Risk Ledger's social network approach

What allows Risk Ledger to support public sector bodies to Defend-as-One against supply chain risks, and achieve alignment with the supply chain-related requirements set out by the GCSS and the CAF, is its social network-based approach to supply chain cyber security. Through this approach, Risk Ledger enables organisations to leverage their TPRM programmes to gain in-depth contextual insights into the internal security postures of their critical suppliers, achieve enhanced visibility into organisations' extended supply chain ecosystem beyond 3rd parties, and facilitate collaboration between organisations and their suppliers as well as between industry peers for a more effective and holistic approach to supply chain cyber security.

Similar to a social network, each supplier organisation has a profile on the platform, which contains information about their business, but also in-depth assessments of their cyber security controls and other relevant risk areas, including ESG and financial risk. These control questions are based on Risk Ledger's standardised assessment framework, mapped against all leading international standards such as NIST, ISO27001 or the NCSC's CAF, but optimised for supply chain risk management. This in-depth supplier profile, controlled by the suppliers, is then shared with their clients and customers with which they are directly connected on the platform. Clients can set requirements against the assessment framework, as well as label suppliers based on their criticality, whether they hold/handle sensitive company or customer information, whether they have system access and more.

Because of this standardised framework, this means that there are multiple eyes on the same supplier at all times, improving the quality of the data and the validation of their answers and evidence. The second validation layer consists of external scanning of suppliers' security controls, without the need for supplier input. Together, these two validation layers have taken continuous monitoring in TPRM to new qualitative heights.

Most importantly, organisations can interact and collaborate with the security teams of their suppliers on remediation and risk mitigation directly on the platform, building strong partnerships and relationships over time, which is essential for more effective and faster responses during emerging supply chain incidents.

Crucially, suppliers are encouraged to also use Risk Ledger to manage their own supply chain risks by connecting with their own suppliers, thus using Risk Ledger as both a supplier and client at the same time. Organisations acting as both suppliers and clients on the Risk Ledger platform is what uncovers the crucial middle links in supply chains and builds the map of interdependencies within the wider supply chain ecosystem, not just between one client and their third-parties, but far beyond.

Conclusions

Operational resilience is an increasing priority for organisations and regulators, with supply chain security as a key focus. The GCSS and CAF have also zoomed in on the risks of supply chain incidents, and are actively working to reduce the threat across the sector.

Today's supply chains are highly complex and interdependent, with organisations dependent on third party suppliers to provide critical services. Those suppliers rely on their own suppliers, and so on. This creates the need to understand risks beyond direct third parties, extending to fourth, fifth, and nth parties. Every link is important and it is important to gain visibility of all the links to understand the potential cascading impact an incident may have on your operations.

Similar to other new operational resilience rules, the GCSS and CAF are not least interested in gaining a greater understanding of the extended supply chain dependencies of public sector bodies and the sector as a whole. But organisations have no easy way to identify such concentration and systemic risks at the moment.

To gain better visibility beyond immediate suppliers and assess risks across their entire supply chain, this white paper has argued, only a more collaborative approach can address these challenges by acting as a force multiplier for public sector bodies. By collaboratively identifying hidden vulnerabilities, public sector bodies can implement mitigation strategies or determine whether risks align with their appetite. By working together, organisations can map risks across a shared supply chain, leveraging collective resources to uncover systemic risks that would be difficult to detect individually.

Appendix

Risk Ledger's innovative approach, especially the social network-type characteristics has reimagined the speed at which organisations can manage third-party risk. Additionally, for organisations that come under the purview of the UK GCSS, deploying Risk Ledger's capabilities can address many GCSS requirements, primarily as they relate to 'third party risk management' as well as supply chain visibility and resilience.

Below we set out how our dedicated standardised Risk Ledger assessment framework and control questions - the basis of every supplier assessment on Risk Ledger - maps against the various Objectives, Principles and Guidance provided by the GCSS and especially the CAF.

For reference, our standardised assessment framework, with all its control questions, is fully available here: https://riskledger.com/support/framework

Click to view Framework

Objective A - Managing security risk Appropriate organisational structures, policies, and processes in place to understand, assess and systematically manage security risks to the network and information systems supporting essential functions.				Risk Ledger Supplier Assessment Framework (SAF) June 2021
Principle		**Guidance**		**SAF controls mapping**
A1 Governance.	The organisation has appropriate management policies and processes in place to govern its approach to the security of network and information systems.	A1.a Board Direction	You have effective organisational security management led at board level and articulated clearly in corresponding policies.	C2 - C12
		A1.b Roles and Responsibilities	Your organisation has established roles and responsibilities for the security of networks and information systems at all levels, with clear and well-understood channels for communicating and escalating risks.	C17
		A1.c Decision-making	You have senior-level accountability for the security of networks and information systems, and delegate decision-making authority appropriately and effectively. Risks to network and information systems related to the operation of essential functions are considered in the context of other organisational risks.	C2, C17, C21
A2 Risk Management	The organisation takes appropriate steps to identify, assess and understand security risks to the network and information systems supporting the operation of essential functions. This includes an overall organisational approach to risk management.	A2.a Risk Management Process	Your organisation has effective internal processes for managing risks to the security of network and information systems related to the operation of essential functions and communicating associated activities.	C21
		A2.b Assurance	You have gained confidence in the effectiveness of the security of your technology, people, and processes relevant to essential functions.	C1
A3 Asset Management	Everything required to deliver, maintain or support networks and information systems necessary for the operation of essential functions is determined and understood. This includes data, people and systems, as well as any supporting infrastructure (such as power or cooling).	A3.a Asset Management	No further guidance	E1, E2
A4 Supply Chain	The organisation understands and manages security risks to networks and information systems supporting the operation of essential functions that arise as a result of dependencies on external suppliers. This includes ensuring that appropriate measures are employed where third party services are used.	A4.a Supply Chain	No further guidance	J1 - J6

Objective B - Protecting against cyber-attack Proportionate security measures are in place to protect the networks and information systems supporting				Risk Ledger Supplier Assessment Framework (SAF) June 2021
Principle		**Guidance**		**SAF controls mapping**
B1 Service Protection Policies and Processes	The organisation defines, implements, communicates and enforces appropriate policies and processes that direct its overall approach to securing systems and data that support operation of essential functions.	B1.a Policy and Process Development	You have developed and continue to improve a set of cyber security and resilience policies and processes that manage and mitigate the risk of adverse impact on the essential function.	C3-C16
			You have successfully implemented your security policies and processes and can demonstrate the security benefits achieved.	C1, C20
B2 Identity and Access Control	The organisation understands, documents and manages access to networks and information systems supporting the operation of essential functions. Users (or automated functions) that can access data or systems are appropriately verified, authenticated and authorised.	B2.a Identity Verification, Authentication and Authorisation	You robustly verify, authenticate and authorise access to the networks and information systems supporting your essential function.	E4, E9, E10, E12, E13
		B2.b Device Management	You fully know and have trust in the devices that are used to access your networks, information systems and data that support your essential function.	E3, E5,
		B2.c Privileged User Management	You closely manage privileged user access to networks and information systems supporting the essential function.	E11, E14
		B2.d Identity and Access Management (IdAM)	You assure good management and maintenance of identity and access control for your networks and information systems supporting the essential function.	E4, E9, E12, E13
B3 Data Security	Data stored or transmitted electronically is protected from actions such as unauthorised access, modification, or deletion that may cause an adverse impact on essential functions. Such protection extends to the means by which authorised users, devices and systems access critical data necessary for the operation of essential functions. It also covers information that would assist an attacker, such as design details of networks and information systems.	B3.a Understanding Data	You have a good understanding of data important to the operation of the essential function, where it is stored, where it travels and how unavailability or unauthorised access, modification or deletion would adversely impact the essential function. This also applies to third parties storing or accessing data important to the operation of essential functions.	E2
		B3.b Data in Transit	You have protected the transit of data important to the operation of the essential function. This includes the transfer of data to third parties.	G12
		B3.c Stored Data	You have protected stored data important to the operation of the essential function.	E30, E31
		B3.d Mobile Data	You have protected data important to the operation of the essential function on mobile devices.	C4, E26, E27, E28
		B3.e Media / Equipment Sanitisation	You appropriately sanitise media and equipment holding data important to the operation of the essential function	C24, E5, E28

B4 System Security	Network and information systems and technology critical for the operation of essential functions are protected from cyber attack. An organisational understanding of risk to essential functions informs the use of robust and reliable protective security measures to effectively limit opportunities for attackers to compromise networks and systems.	B4.a Secure by Design Y	You design security into the network and information systems that support the operation of essential functions. You minimise their attack surface and ensure that the operation of the essential function should not be impacted by the exploitation of any single vulnerability.	F2, F5, G11
		B4.b Secure Configuration	You securely configure the network and information systems that support the operation of essential functions.	E20, E34
		B4.c Secure Management	You manage your organisation's network and information systems that support the operation of essential functions to enable and maintain security.	E22, E23, E24, E25, F1, G10, G14, G16, G18
		B4.d. Vulnerability Management	You manage known vulnerabilities in your network and information systems to prevent adverse impact on the essential function.	E20, G16 - G21
B5 Resilient Networks and Systems	The organisation builds resilience against cyber-attack and system failure into the design, implementation, operation and management of systems that support the operation of essential functions.	B5.a Resilience Preparation	You are prepared to restore the operation of your essential function following adverse impact.	I1 - I14
		B5.b Design for Resilience	You design the network and information systems supporting your essential function to be resilient to cyber security incidents. Systems are appropriately segregated and resource limitations are mitigated.	F7, G11, G28, G29, I1 - I14
		B5.c Backups	You hold accessible and secured current backups of data and information needed to recover operation of your essential function	C11, E6, E7, E8
B6 Staff Awareness and Training	Staff have appropriate awareness, knowledge and skills to carry out their organisational roles effectively in relation to the security of network and information systems supporting the operation of essential functions.	B6.a Cyber Security Culture	You develop and pursue a positive cyber security culture.	C2, C17, C18, I6
		B6.b Cyber Security Training	The people who support the operation of your essential function are appropriately trained in cyber security. A range of approaches to cyber security training, awareness and communications are employed.	D3

Objective C - Detecting cyber security events Capabilities exist to ensure security defences remain effective and to detect cyber security events affecting, or with the potential to affect, essential functions				Risk Ledger Supplier Assessment Framework (SAF) June 2021
Principle		**Guidance**		**SAF controls mapping**
C1 Security Monitoring	The organisation monitors the security status of the networks and systems supporting the operation of essential functions in order to detect potential security problems and to track the ongoing effectiveness of protective security measures.	C1.a Monitoring Coverage	The data sources that you include in your monitoring allow for timely identification of security events which might affect the operation of your essential function.	F11, G10, G22, H4,
		C1.b Securing Logs	You hold logging data securely and grant read access only to accounts with business need. No employee should ever need to modify or delete logging data within an agreed retention period, after which it should be deleted.	G22
		C1.c Generating Alerts	Evidence of potential security incidents contained in your monitoring data is reliably identified and triggers alerts.	G10
		C1.d Identifying Security Incidents	You contextualise alerts with knowledge of the threat and your systems, to identify those security incidents that require some form of response.	G10, I2
		C1.e Monitoring Tools and Skills	Monitoring staff skills, tools and roles, including any that are outsourced, should reflect governance and reporting requirements, expected threats and the complexities of the network or system data they need to use. Monitoring staff have knowledge of the essential functions they need to protect.	D3
C2 Proactive Security Event Discovery	The organisation detects, within networks and information systems, malicious activity affecting, or with the potential to affect, the operation of essential functions even when the activity evades standard signature based security prevent/ detect solutions (or when standard solutions are not deployable).	C2.a System Abnormalities for Attack Detection	You define examples of abnormalities in system behaviour that provide practical ways of detecting malicious activity that is otherwise hard to identify.	G10
		C2.b Proactive Attack Discovery	You use an informed understanding of more sophisticated attack methods and of normal system behaviour to monitor proactively for malicious activity.	G10

Objective D - Minimising the impact of cyber security incidents Capabilities exist to minimise the adverse impact of a cyber security incident on the operation of essential functions, including the restoration of those functions where necessary.				Risk Ledger Supplier Assessment Framework (SAF) June 2021
Principle		**Guidance**		**SAF controls mapping**
D1 Response and Recovery Planning	There are well-defined and tested incident management processes in place, that aim to ensure continuity of essential functions in the event of system or service failure. Mitigation activities designed to contain or limit the impact of compromise are also in place.	D1.a Response Plan	You have an up-to-date incident response plan that is grounded in a thorough risk assessment that takes account of your essential function and covers a range of incident scenarios.	I1 - I5
		D1.b Response and Recovery Capability	You have the capability to enact your incident response plan, including effective limitation of impact on the operation of your essential function. During an incident, you have access to timely information on which to base your response decisions.	I5, I7, I8
			Your organisation carries out exercises to test response plans, using past incidents that affected your (and other) organisation, and scenarios that draw on threat intelligence and your risk assessment.	I14
D2 Lessons Learned	When an incident occurs, steps are taken to understand its root causes and to ensure appropriate remediating action is taken to protect against future incidents.	D2.a Incident Root Cause Analysis	When an incident occurs, steps must be taken to understand its root causes and ensure appropriate remediating action is taken.	I8
		D2.b Using Incidents to Drive Improvements	Your organisation uses lessons learned from incidents to improve your security measures.	I8

RISK LEDGER

Thank you

Risk Ledger transforms third-party risk management by enabling you to onboard and connect your entire supply chain, bringing every supplier into clear view. Access risk insights, mitigate emerging threats, and manage your supply chain with unparalleled confidence - all from a single, powerful platform.

Learn more at www.riskledger.com