THE AUGUSTA GROUP

The Augusta plan: Thought leadership, an alternative approach to cybersecurity for the DoD and DIB

A strawman for reasserting accountability and responsibility for managing Cyber-SCRM. Leveraging existing financial services, Sarbanes Oxley and financial regulatory practices.

August 2021

Andy Watkin-Child, Ted Dziekanowski

The Augusta Plan

In August of 1941, President Franklin Delano Roosevelt met Prime Minister Winston Churchill for the first time aboard the cruiser U.S.S. Augusta to formulate a strategy for conducting World War Two. Whilst the authors of this paper do not claim the greatness of either leader, our intention is somewhat similar. We propose a strategy outlined in this paper, that has nine objectives, which we hope can lead to better protection of the Intellectual Property (IP) of the Department of Defense (DoD) and a more secure Defense Industrial Base (DIB).

As was recognized 80 years ago, the securing of the critical infrastructure that supports the militaries of the world needs to be an international effort. Our solution attempts to leverage existing global standards used to protect one information type (financial data material to accurate reporting of results) to another information type (sensitive Intellectual Property(CUI)) in a manner that respects the sovereignty of nations while providing oversight to the Department of Defense.

We hope that the strategy outlined in this paper leads to tactical solutions that secure the critical infrastructure and forms the basis for further efforts in other areas of the global economy.

Executive summary

Introduction: The US Government Accountability Office (GAO) and Office of the DoD Inspector General (DoD IG) have highlighted the challenges faced by the Department of Defense (DoD) in securing its Intellectual Property (IP). They identified failures to embed cybersecurity into the Defense Industry Base (DIB), manage weapon system vulnerabilities and protect DoD weapon systems from Cyber-attack[1-6]. Raising concerns within Federal Government that the DoD and DIB are subsidising other Nation States create their own weapon systems. However, managing the complexity of cybersecurity and cyber risk adds a considerable overhead to the DOD and DIB. DFARS 252.204-7012, 7019, 7020 and 7021 requires the DIB to manage its offensive and defensive cybersecurity capabilities. Cyber risk management requires the careful consideration of an organisations inherent and residual risk profile, a process many organisations are unable to resource. Federal government (including the DoD) is working towards the delivery of the Federal Information Security Modernisation Act (FISMA), and the Risk management Framework (RMF – NIST SP 800-37R2). The DoD has adopted RMF principles within its procurement processes (DoDi 5000.90). Many agencies are starting to adopt cybersecurity control frameworks such as NIST SP 800-171 or NIST SP 800-53 as they progress along their risk management journey.

Cybersecurity programmes planned by the Federal government will not deliver the required oversight and assurance for several years and add significant costs to defense contractors. We address these concerns outlined in Objectives 1–9 below and present a cost-effective and efficient solution using existing best practice benefiting the DoD, the DIB and Federal Agencies.

Cyber Oversight and Assurance: There are numerous cybersecurity control frameworks for the DoD to adopt across the DIB, there are however not enough resources to assure compliance nationally or internationally. An issue which can be addressed through existing regulatory bodies, who oversee similar frameworks such as Sarbanes Oxley and System and Organization Control (SOC) 1 and 2. The American Institute of Certified Public Accountants (AICPA) has created Trust Services Criteria (TSC) aligned to COSO, the NIST Cybersecurity Framework (CSF), NIST SP 800–53, ISO 27001 and COBIT 5. SOC reports are designed to provide information to users of outsourced service providers with information about the effectiveness of the service providers' controls over the security, availability, and confidentiality of information processed by those systems. Prepared by independent Certified Public Accountants (CPAs) skilled in both auditing processes and cyber/ IT security, SOC reports reduce compliance burdens by providing one report that addresses the shared needs of multiple users. Today, 5 of the top 14 IT security consultants are CPA firms; there are thousands of qualified CPAs that perform SOC audits. The DoD can request that all DIB contractors submit a SOC 2 report to the DoD, as part of their annual financial audit process? Addressing several oversight and assurance issues including resourcing, reciprocity of assessment and partner Nation oversight and assurance.

Data and Common Control Accountability and Responsibility: The DoD owns the data created by the DIB for the design, manufacture, maintenance, and support of DoD weapon systems. Data the DoD must secure across the procurement process to protect Intellectual Property (IP). The DoD can oversight and assure its data by adopting a risk-based approach for cybersecurity in line with NIST SP 800–37, NIST SP 800-53 and NIST SP 800–171, creating cybersecurity framework profiles. Identifying the appropriate number of cybersecurity controls required for each contract and request Prime contractors to provide oversight and assurance of these controls across the supply chain. The DoD can allow Primes to implement controls based upon a risk-based 'bill of materials' and enable Primes to manage and process controls inherited on behalf of their suppliers. Simplifying the number of components requiring oversight. Requesting that each contractor and subcontractor provide an annual SOC 2 report, assessing cybersecurity framework profile control design and effectiveness. Placing appropriate data in the cloud and applying controls at the source. This will manage the chain of custody of the DoDs IP, increasing data security, efficiency, effectiveness and reduce the cost of control oversight and assurance.

Objectives: This white paper provides options to address the challenges the US Department of Defense (DoD) and the Global Defense Industry Base (DIB) face in addressing cybersecurity compliance for the protection of DoD IP. As required under Defense Federal Acquisition Supplement (DFARS). Objectives considered for supply chain security.

Objective 1: To Leverage oversight and assurance mechanisms which already exist for control design and effectiveness testing.

Objective 2: To rapidly expand the number of assessors capable of providing oversight and assurance of the global DIB.

Objective 3: Encourage the establishment and utilisation of cyber control inheritance. To improve the cost efficiency and reduce the complexity of cybersecurity oversight and assurance of DIB members.

Objective 4: Enable the effective oversight of the DIB, as a component of critical infrastructure.

Objective 5: Improve DoD, contractor, and subcontractor visibility of control effectiveness.

Objective 6: Facilitate Federal Supply Chain Risk Management (SCRM) requirements.

Objective 7: Simplify international reciprocity of cyber risk management oversight and assurance.

Objective 8: Provide the US Congress with the necessary information to improve regulatory oversight.

Objective 9: Support the development of Continuous Diagnostics and Mitigation (CDM)

Existing, Appropriate Regulatory Models and Control Frameworks:

Financial services relative to the commercial Defense Sector is more effective at managing cybersecurity. Financial services has global reach, is part of Critical National Infrastructure (CNI), transaction and process complexity are high, it is a service on which we all depend and is a constant target for cybercrime and Nation State hackers.

A contributing factor to the sectors security posture is the global regulatory environment in which financial services firms such as banks and insurance firms operate. They are regulated to manage risk and protect the stability of global financial markets under the Basel Accords (banks) and Solvency 2 (insurance firms).

Banking regulation has a long history. The Basel Committee on Banking Supervision introduced the Basel Accords in 1988 with Credit risk (Basel I). Market and Operational risk, supervisory oversight, and market discipline (the 3 pillars) in 2004 with Basel II. Basel III updated Basel II introduced in 2010, there is a 4th iteration with Basel IV due for implementation in 2023. The Basel Accords illustrate the recognition of the dynamic nature of risk management in the Financial Services sector.

A key principle of the Basel accords and Solvency II is the requirement for setting and managing minimum regulatory capital requirements (capital ratio). Capital which institutions are required to hold as a percentage of their Risk Weighted Assets (RWA). Oversight is provided by the Basel Committee on Banking Supervision, regional central banks, and national regulators including the Federal Reserve (US), FSA (UK), and BaFin (Germany), all of whom are authorised to manage capital ratios.

Capital ratios are set based upon the effectiveness of institutions to manage Credit, Market, and Operational Risks. The level of capital held is not insignificant, based on RWA and "risk appetite" of the institution. The size of the regulatory capital allocated for a global tier 1 bank can be more than $150 billion. By way of example, regulatory capital held by covered UK banks as of Q4 2020 was £2,025 billion for Credit and Counterparty risk, £379 billion for Market risk and £288 billion for Operational risk which includes cybersecurity risk [7].

Financial regulators assess capital holdings through the Supervisory Review and Evaluation Process (SREP) and supervisory stress testing, valuating an institution's management of risk. Where appropriate, regulators will change capital ratios and the amount of capital institutions hold, capital which must be held for the management of risk.

Incentives to Manage Risk: Cyber risk management is tied to capital, creating an incentive to manage cybersecurity. Firms must demonstrate to regulators that cyber (operational) risk is effectively managed if they want Tier 1 capital ratios reduced. Freeing capital from the balance sheet for use in the market, increasing profit and optimising shareholder value.

Sarbanes Oxley 2002: SoX is a source of regulatory oversight for publicly traded companies, that can include DIB contractors. SoX compliance requires the leadership of public companies registered in the US to individually attest to the accuracy of financial information and the management of material financial controls.

The act established the Public Company Accounting Oversight Board (PCAOB) that is charged with overseeing, regulating, inspecting, and disciplining accounting firms in their roles as auditors of public companies.

SoX section 404 requires management and their external auditors to produce an "internal control report". Affirming the responsibility of management in establishing and maintaining an adequate internal control structure and procedures for financial reporting.

Assessing the effectiveness of the internal control structure and procedures of financial reporting requires management to:

- Assess the design and operating effectiveness of selected internal controls related to significant accounts in the context of material misstatements.
- Document transaction flows, including IT.
- Evaluate entity level controls, controls designed to prevent fraud and period ending financial reporting processes.
- Conclude on the adequacy of internal control over financial reporting.

SoX requires covered organisations to undertake an annual financial audit, assessing material process level and IT general controls which impact financial processing.

SoX has been a contentious act for smaller entities. In many ways with similarities to DFARS and the DIB, mandating regulatory oversight and independent assurance of US public companies. SoX provides investors with a level of confidence in an organisations leadership to manage its material financial entity, process, and IT general controls. SOC provides a level of confidence in organizations' ability to manage effective-security processes and controls to manage their cyber risks.

The DoD as a customer (the investor) seeks assurance that the DIB can effectively manage critical cyber controls across a global supply chain.

Trust Services Criteria (TSC) and System and Organization Control (SOC) Audits: The DIB is a complex global supply chain, adhering to various global financial reporting standards and frameworks including SoX, IFRS, GAAP to assess corporate economic efficiency, and improve capital allocation. Lowering the cost of capital and reducing international reporting costs. Standards which rely on an organisations controls framework to manage the design, manufacture, sale and servicing of products and services.

A source of appropriate international cybersecurity oversight for the DoD and DIB has already been created by the American Institute of Certified Public Accountants (AICPA). The AICPA has created a framework, called the Trust Services Criteria (TSC), to be used to evaluate the suitability of the design and operating effectiveness of controls, relevant to the security,

availability, or processing integrity of information and systems. TSC is aligned to COSO, NIST Cybersecurity Framework, NIST SP 800–53, ISO 27001, COBIT 5 and GDPR[8].

The TSC provide an evaluation and reporting framework that companies of all types and sizes can use to report on their security, availability, and processing integrity controls, regardless of which specific security regulations they have to comply with. In that way, SOC reports provide information that enables comparability. Whilst a SOC audit is not mandatory for public companies it provides stakeholder assurance of an organisation's management of key controls.

A SOC assessment provides a verifiable auditing report which is performed by a Certified Public Accountant (CPA) designated by the American Institute of Certified Public Accountants (AICPA).

SOC reports can be provided globally using the reciprocal arrangements which already exist between global accounting regulators and accounting firms, who manage relationships with DIB Prime contractors and subcontractors through their financial audit processes.

A SOC 2 report is identified in DoDi 5000.90 as an accepted assessment of manufacturers of DoD weapon systems. Where the Program Manager (PM) has determined that there is a high or moderate risk tolerance for a given weapon system.

Recommendations to protect DoD IP and secure the DIB: Cyber risk management, oversight and control is a challenge for the DoD and compliance will be a challenge for the DIB. The DoD as the customer has the right to have its data protected and the DIB must work with the DoD to find a solution which makes data security cost effective. The DoD has tried unsuccessfully to regulate data security as far back as 2016 through DFARS, as documented by the DoD Inspector general and GAO [1–6].

The following is a discussion of 9 steps which the DoD could take to secure the DIB, for the DIB to provide oversight and assurance of the data which it creates, stores and transmits on behalf of the DoD. The DoD has used DFARS 252.204-7012 to flow down cybersecurity requirements through the DIB since 2016.

The DoD supply chain is complex and procures products and services globally from between 250,000 and 300,000 contractors and subcontractors globally. Consuming a forecast annual budget of $700 Billion (2021). Such complexity makes oversight and assurance of cyber risks a significant task.

A task which faces challenges including how to create enough assessors to provide oversight and assurance of 250,000 firms every three years. There is the challenge of assessing global DIB contractors and subcontractors located in other nation states which have their own security requirements. Additionally, Federal government would like to implement Continuous Diagnostic and Mitigation (CDM), to validate the security of the DoDs IP.

The DoDs core requirement is to harden its global supply chain to protect its IP across the DIB. These challenges have solutions utilising existing regulatory standards and frameworks. Requiring a foundation of accountability and responsibility to be in place across the DIB for the protection, oversight, and assurance of the DoDs IP. Which is simple to implement and manage and is cost effective. This is a challenge as it is well documented that cyber security is the most complex non-financial risk to manage. We propose the following steps to build the foundations for cybersecurity and risk management.

1 – Product specific cybersecurity framework profiles and contracts: Each DoD contract should include an agreement as to the threats to CUI held by the supplier, the

vulnerabilities of the supplier environment, and control expectations to create a Cybersecurity Framework Profile (CSFP). Based upon a risk profile which is a function of the weapon system, its operating environment, and supply chain. Using NIST 800-37r2. DODI 5000.90, NIST SP 800–53 R5 and/ or NIST SP 800-171 R2 as the foundations for the profiles. The DoD and the Prime contractor agree on the cybersecurity framework profile for the contract.

The Prime contractor creates a risk-based "Bill of Materials" (BoM) for the product or service supplied to the DoD. Identifying the cybersecurity risk associated with systems and subsystems within the BoM. This gives flexibility to the Prime to identify components considered high, medium, and low risk. Creating an appropriate cybersecurity risk profile and prioritising the level-of-effort and cost of assurance within its supply chain.

Under the DoD Risk Management Framework (RMF) the DoD is required to risk assess the weapon systems product lifecycle. Under DoDI 5000.90 PMs at their discretion can tailor baseline controls based upon operational requirements. Creating bespoke risk profiles supports the deployment of the RMF into the supply chain and a risk based 'bill of materials' reduces the cybersecurity risk oversight and assurance of the weapon system. E.g. an aircraft's PIT system has a higher cybersecurity risk than its undercarriage.

2 – Accountabilities and responsibilities: Primes are accountable and responsible for maintaining cybersecurity of their supply chains, associated with the production and servicing of a weapon system under the DoD contract. Subcontractors perform the same tasks on behalf of the Prime contractor. Creating flow down of cybersecurity oversight and assurance.

Prime's flow-down the agreed cybersecurity framework profiles through their supply chain following the risk-based approach adopted by the weapon system 'Bill of Material'. In agreement with the DoD PM under DoDi 5000.90.

Subcontractor's flow-down the agreed cybersecurity framework profiles through their supply chain following a risk-based approach to their 'Bill of Material' in agreement with their contractor.

This process tailor's cybersecurity oversight and assurance based upon the risk associated with the bill of materials. Reducing the overhead of assurance and compliance testing.

3 – Oversight and assurance (Contractor): Prime contractors and subcontractors assume responsibility for baseline control compliance to NIST SP 800–53 R5 and/or NIST SP 800–171 R2.

The Prime contractor is accountable and responsible for assessing compliance. Managing oversight and assurance to the associated cybersecurity framework profiles based upon the agreed program and associated Bill of Materials. In agreement with the DoD in a contract.

Assessment by Prime contractors and subcontractors could include a SOC 2 report, based upon the risk tolerance of the contracted weapon system. These reports will be incorporated in the Weapon System, System Security Plan (SSP) and provided to the DoD PM.

Prime contractors and subcontractors can take a risk-based audit approach and selectively assess compliance of the cybersecurity framework profiles of its contractors. Performing on-site assessments based upon the components risk profile, providing results to the DoD and Prime contractor as required.

4 – Remediation: Where gaps in compliance have been identified by the Prime contractors or subcontractors, they are to be remediated following a risk-based approach. Based upon the risk associated with the Bill of Materials.

Prime contractors and subcontractors manage and oversight POAMS within their supply chain, ensuring that they are kept up to date, and milestones achieved. POAMS will be made available to Authorizing Officials (AO) and Program Managers (PM) as required. The Prime contractor will provide an aggregated POAM of all subcontractors for the contract to the DoD.

5 – Oversight and assurance (DoD): It is not practical to assess every single organization in the DoD Global DIB. The DoD should sample inspect Prime contractors annually to provide assurance of cybersecurity framework profile contract compliance, performed by DCMA. DCMA already assesses the oversight, assurance, and remediation compliance of the DIB to NIST SP 800-171.

6 – Oversight and assurance (complying with FISMA and RMF requirements): The Office of Management and Budget (OMB) and the Office of the DoD Inspector General (DoD OIG) will assess DoDs oversight of Prime contractors. Required annually and/ or driven by market conditions for DoD compliance to FISMA, RMF and cybersecurity frameworks. Reporting findings to congress for evaluation.

7 – Congress: Congress will write legislation to remediate gaps identified through OMBs oversight and provide incentives to the supply chain to manage supply chain cyber risks through subsidies. This could include tax incentives, support for cybersecurity training and infrastructure subsidies.

8 – Performance based incentives/ penalties: As with Basel and Sarbanes Oxley, penalties and incentives are required to facilitate the program.

Prime contractors and subcontractors should be held accountable for compliance to the appropriate cybersecurity framework profiles within the supply chain. If they satisfy key performance indicators for the management of cyber risk the DoD could allocate contract bonus or penalties for not satisfying the specifications of the cybersecurity framework profile.

A model like that adopted by financial regulators could be applied. Replacing regulatory capital with risk-based incentives, allocating a percentage of the contract value. Released at various stages throughout the product lifecycle for the successful management of cybersecurity and risk.

9 – Continuous Diagnostic Mitigation (CDM)

Several Federal departments want greater oversight of cybersecurity across agencies including the DoD and the DIB. Placing assurance over the management of Defense IP and Critical National Infrastructure (CNI). Centralising the oversight and assurance of the defense supply chain through Prime contractors. Agreeing the data which should be collected to assure SCRM, and cybersecurity provides the mechanism for CDM. If Primes inherit the management of controls over DoD Data in the Cloud it provides a central source for the oversight of cybersecurity compliance. This can be regulated through DFARS and mandated across the global supply chain and delivered by Primes using CDM and validated through SOC 2 reporting.

Summarizing Objectives 1–9: The DoD relies upon a complex arrangement of global DIB contractors and subcontractors. Made up of publicly traded Primes, mid-sized

corporates, SMEs, and often family run enterprises employing less than 10 people. Delivering an array of products and services to the DoD, in line with the DoDs mission to protect US National Security. Products and services ranging from complex weapon systems to facility services at military bases.

The DoD relies upon Prime contractors and subcontractors to satisfy their contractual obligations. These obligations include providing oversight and assurance of their capabilities to protect the DoDs IP. Prime contractors, if enabled appropriately, should have visibility across their supply chain and the level of cybersecurity their contractors apply. Appropriate risk management will enable Primes to manage their cyber risks, providing additional oversight and assurance of control effectiveness to the DoD. A process which contractors and subcontractors are obligated to manage today through the flow down of DFARS 252.204–7012.

The DoD could incentivise Prime contractors through risk related rewards set as a function of the contract value. E.g. using the timely resolution of audit findings identified and placed within a POAM.

Primes can request that their suppliers provide the results of a SOC audit annually based upon the risk tolerance of the weapon system. Utilising the TSC for oversight and assurance of cybersecurity framework profile compliance. Allowing the DoD to leverage the thousands of U.S. CPAs who perform SOC audits under the AICPA regulatory body and governed by the Public Company Accounting Oversight Board (PCAOB). UK Chartered accountants (equivalents) would also be qualified to oversight and assure the UK DIB using SOC 2. Feeding compliance results to the DoD as required and allowing the DoD to complete selective and sample-based oversight of Prime contractors. The benefits of this oversight and assurance process include:

- Subcontractors who inherit controls from Primes can reduce the cost of compliance.
- Primes will have improved oversight of their subcontractors satisfying contract requirements.
- SOC 2 reporting benefits Primes who are required to report their Economic, Social and Governance (ESG) oversight of material risks to the Securities and Exchange Commission (SEC).
- The DoD will have a baseline for cybersecurity over the DIB.
- The Department of Homeland Security (DHS) will gain valuable cybersecurity data from the DoD. Which in turn can use this data to protect the critical infrastructure of the US under CDM.

Addressing objectives 1 - 9

Objective 1: Leverage oversight and assurance mechanisms which already exist for control design and effectiveness testing.

a. The global financial audit community completes SOx and Financial audits of regulated defense contractors. Mandating the submission of a SOC report completed by qualified CPAs will provide contractors and subcontractors with independent assurance of their cybersecurity compliance.
b. There are thousands of CPAs in the US qualified to complete assessments.
c. Reciprocity of oversight can be delivered globally across the DIB using equivalent qualified auditors.
d. CPAs and their equivalents are governed by an appropriate regulatory body.
e. Cloud providers who are SOC 2 compliant can use the TSC to evaluate their security and availability controls in a manner that is consistent and comparable among all providers.

Objective 2: Expand the number of assessors capable of providing oversight and assurance of the global DIB.

a See Objective 1.

Objective 3: Encourage the establishment and utilization of controls inheritance. To

improve the cost efficiency for cybersecurity oversight and assurance of DIB members.

a. Prime contractors can manage inherited controls using public or private cloud. Reducing oversight and assurance requirements across the supply chain and simplifying contractor and subcontractor audits.

Objective 4: Enable the effective oversight of the DIB as a component of critical infrastructure.

a. See Objective 1, 2 and 3. Enabling oversight through regulated financial auditors assures the quality of oversight and assurance of the cybersecurity framework profile. Audit reports can be consolidated by the Prime for the DoD.
b. Prime ownership of contractor and subcontractor oversight and assurance ensures the quality of information sharing, reporting and remediation of control deficiencies.
c. Consolidation of inherited controls by the Prime significantly reduces oversight and assurance.
d. Incentivization through risk weighted funding based upon audit response will over time align contractor and subcontractor compliance to the DoDs needs.

Objective 5: Improve DoD, contractor and subcontractor visibility of control effectiveness.

a. See Objective 1, 2 and 3.

Objective 6: Facilitate Supply Chain Risk Management (SCRM) requirement of the US Government.

a. See Objectives 1 – 5. The chain of custody of cybersecurity information is significantly reduced if Primes take responsibility for securing their supply chain and manage inherited controls. The DoD only needs to direct Prime contractor and does not have to oversee 250,000 DIB contractors.
b. SOC 2 reporting exists and is used by cloud providers to assure security of data for their customers.
c. SOC 2 audits utilize the TSC framework which is aligned to existing cybersecurity control frameworks including NIST CSF, NIST SP 800-53, ISO 27001 and GDPR.
d. SOC 2 audits can be applied globally without requiring reciprocal security agreements.
e. SOC 2 audits can be completed by local qualified CPAs or their equivalents.

Objective 7: Enable international reciprocity of cyber risk management.

a. See Objectives 1 – 6.

Objective 8: Provide the US Congress with necessary information to improve regulatory oversight.

a. Simplifying oversight and assurance reporting to the DoD through Primes will support better communications and improve regulatory oversight for Congress.

Objective 9: Develop solutions to support Continuous Diagnostics and Mitigation (CDM).

a. See Objectives 1 – 7. Continuous Diagnostic Mitigation of DoD CNI requires collaboration and engagement by US Primes and their subcontractors to target specific and agreed DIB infrastructure for the protection of DoD IP.
b. CDM is most efficiently enabled if Primes manage inherited controls across the supply chain leveraging the cloud to host DoD IP.
c. CDM could be enabled through DFARS regulation but would require financial support from the DoD to enable Primes to manage inherited controls in the cloud.

References

1. Government Accountability office (2018): Weapon Systems Cybersecurity: DOD Just Beginning to Grapple with Scale of Vulnerabilities
2. Government Accountability office (2018): Urgent Actions Are Needed to Address Cybersecurity Challenges Facing the Nation
3. Government Accountability office (2021): WEAPON SYSTEMS CYBERSECURITY Guidance Would Help DOD Programs Better Communicate Requirements to Contractors
4. Government Accountability office (2021): Drive to Deliver Capabilities Faster Increases Importance of Program Knowledge and Consistent Data for Oversight
5. Office of the Inspector general US DoD (2019): Audit of Protection of DoD Controlled Unclassified Information on Contractor-Owned Networks and Systems DODIG-2019-105
6. Government Accountability office (2020): 2020 Defense Acquisition Assessment
7. Basel III UK banks regulatory capital: https://www.bankofengland.co.uk/statistics/banking-sector-regulatory-capital/2020/2020-q4
8. AICPA TCS Mappings: https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/mappingsrelevanttotheSOCsuiteofservices.html
9. AICPA SOC for supply chain report: https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/description-criteria.pdf