Defence Cyber
Protection Partnership

Securing the Defence Supply Chain

Christine Maxwell – September 2019

Ministry of Defence

Topics to cover

- Importance of securing the supply chain in today's world
- DCPP and Security Standards
- Working together
- Current status
- Future Plans
- Questions

Ministry of Defence

Ministry
of Defence

Defence Cyber Protection Partnership

Ministry of Defence

- Partnership model
- Working together is our key to success

Defence Cyber Protection Partnership

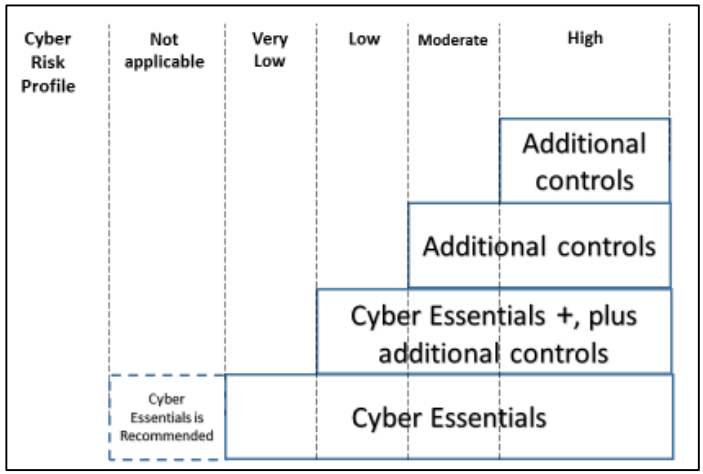
- Collaboration between government and industry to improve the cyber resilience of the UK's defence supply chain:
  - Application of risk based controls;
  - Simplifying cyber assurance;
  - Implementation of a set of coherent and widely recognised standards;
  - Facilitating best practice sharing and learning from experience.

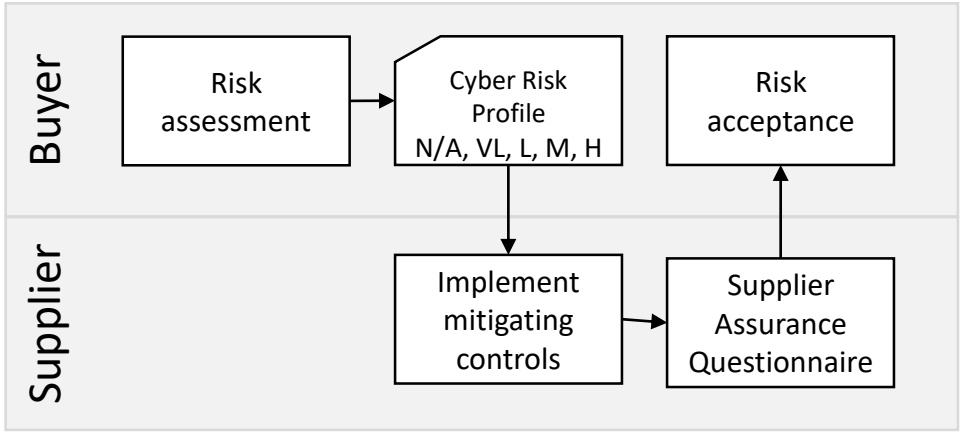
Ministry of Defence

What is DCPP?

Protecting MOD Identifiable Information in the supply chain

DEFSTAN 05-138	Process - Risk assessment - Supplier assurance - Risk acceptance Controls (mitigating actions) - Proportional to risk
	Process automation tool on gov.uk
DEFCON 658	Supplier - Apply DEFSTAN 05-138 - Report incidents - Flow down terms Buyer - Right of audit - Rights in event of breach





Delivering improvement but reducing burden on supply chain

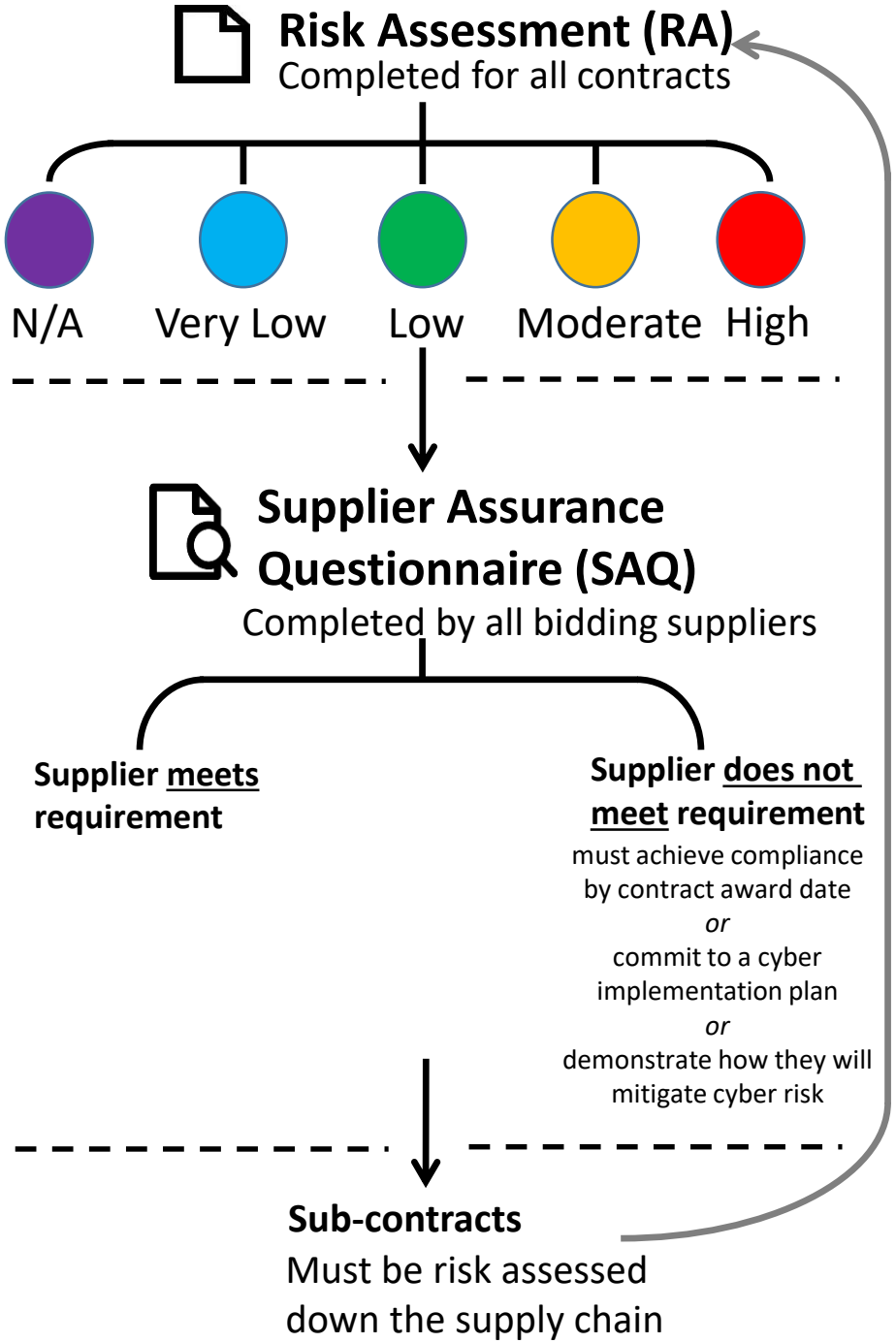
- Proportional to risk but (relatively) prescriptive
- Builds on Cyber Essentials for higher levels of risk
- Uses well-known controls
- Risk acceptance provides for flexibility
- Self-certification

DCPP Process

Buyers and suppliers will engage with the **Cyber Security Model (CSM)** – a three stage process

1. Risk Assessment
   - The buyer conducts a Risk Assessment (assessing the cyber risk) – the process generates a Risk Assessment Reference
2. Supplier Assurance Questionnaire (SAQ)
   - Suppliers complete a SAQ to demonstrate they can meet the requirements of the specific risk level
   - Those not able to demonstrate compliance complete a Cyber Implementation Plan (CIP)
3. Assessment
   - The buyer assesses the submitted SAQs and CIPs

The CSM Process is conducted through online Supplier Cyber Protection (SCP) tool, known as Octavian



DCPP current status

- “Business as usual” for new contracts, flows-down the supply chain until no MODII is shared
- Application of DEFCON658 on Extant contracts has commenced, a number of Authority Change Notices (ACN) have been issued
- Audit of sample set of contracts and associated suppliers
- A new simple risk assessment question set will be released shortly
- Search for a new supplier to provide Supplier Cyber Protection (SCP) tool has commenced

Ministry of Defence

Future Plans

- **Management Information (MI) from Supplier Cyber Protection Tool**
- **Agree an approach for Defence product cyber-security resilience**
  - Assess MOD's desired scope against existing product standards
  - Launch supporting policy
- **Recontract for Supplier Cyber Protection tool**
- **Security monitoring technology used to support supplier auditing**

Continue to…

- **Work across industry and government**
- **Support the NCSC & the evolving Cyber Essentials Scheme**
- **Encourage multi-national reciprocal recognition and convergence**
- **Bring together disparate cyber supply chain activity from across Defence**

Ministry of Defence

Questions?

Ministry
of Defence