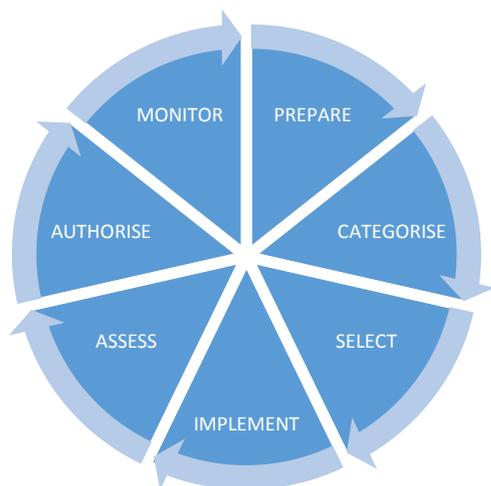# Security Solutions:
# NIST Risk Management Framework

Frazer-Nash has successfully applied the National Institute of Standards and Technology (NIST) Special Publications (SP) on UK and US interconnected systems to reduce the impact of cybersecurity threats.

## OUR APPROACH:



We use our consultants' experience to apply the NIST SP 800-37 Risk Management Framework (RMF) in the context of your business to enable you to take appropriate risk management decisions.

- We will **prepare** your organisation to manage its security and privacy risks, using the RMF to assess essential activities at the organisation, mission, business process and information system levels of your enterprise.

- We will **categorise**, to determine the business impact of compromise or loss of your assets, and to inform subsequent risk management processes and tasks.

- We will **select**, tailor and document the security and privacy controls necessary to protect your systems.

- We will **implement** the appropriate controls defined and will **assess** their effectiveness.

- We will enable your business to **authorise** consistent, well-informed, and ongoing security decisions through appropriate levels of continuous **monitoring**.

## WE UNDERSTAND YOUR CHALLENGES

Cybersecurity risks directly affect your commercial interests by driving up costs, reducing revenue, impeding growth, and damaging reputation.

It's vital that you choose a repeatable and proven cyber risk management approach, which is affordable and can be implemented easily within large and/or complex organisations.

## WHY FRAZER-NASH?

We work with defence suppliers and industries to apply the NIST SP 800-37 RMF to manage risk during the development and in-service life of their products. We pioneered the introduction of the methodology into the UK Ministry of Defence (MOD), and have provided training for MOD staff.

Our risk management specialists are certified and experienced in applying the NIST RMF, and include National Cyber Security Centre (NCSC) Certified Security and Information Risk practitioners.

We have also developed a proprietary tool, tailored to support the use of NIST SPs in the UK accreditation process, which monitors conformity and acceptable risk levels.

## NIST RISK MANAGEMENT FRAMEWORK

### Overview
The RMF was created and developed by NIST to provide a cybersecurity risk framework to identify, assess and manage risk for US critical infrastructure owners and operators. It uses a common language to address and manage cyber security risk in a cost-effective way, based on business and organisational needs, without introducing additional regulatory requirements. It has since been recommended as best practice by several organisations, including the UK NCSC, and has been adopted by utility companies, government departments and related industries.

### Design
Central to the NIST SPs are the NIST 800-37 RMF and the NIST SP 800-53 security controls; the NIST suite of standards are also aligned with ISO27001. We help organisations prepare, categorise, select and implement controls, assess effectiveness, authorise security decisions and continuously monitor their systems to be able to deal effectively with risks and threats. Where required, we will recommend, select and apply appropriate overlays to tailor the generic control set to your business context.

### Implementation
We understand how to use the US process to develop UK accreditation documents that will assist your organisation to embed cybersecurity risk management into the business, to provide evidence for HMG system accreditations, or for audit against ISO 27001:2013.

### Continuous improvement
We help you to maintain an ongoing awareness of information security risks, threats, and vulnerabilities to support organisational risk management decisions, by means of a NIST 800-137 continual monitoring programme.

## BENEFITS

The RMF offers a flexible, repeatable, performance-based, and cost-effective approach, which enables your organisation to prioritise risks according to your business context. It delivers clear information security measures and controls, with associated technical guidance and configuration specifications. It is aligned to the latest International Standards (e.g. ISO 27001:2013), and is regularly updated and continually supported by NIST.

FRAZER–NASH
CONSULTANCY