nccgroup
People Powered, Tech Enabled Cyber Security

Department for Science, Innovation & Technology

White Paper

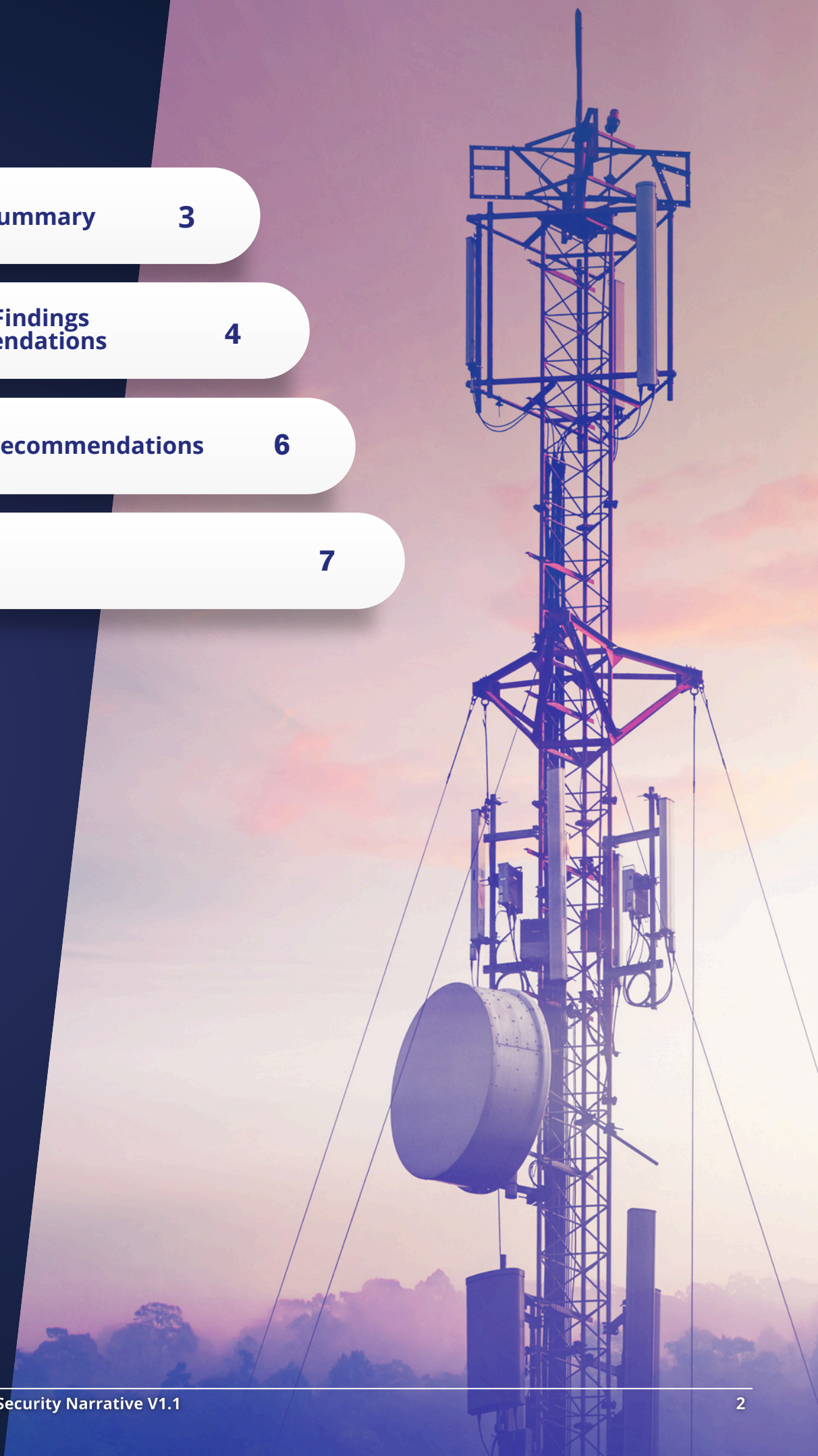
DSIT FRANC Open RAN Security Narrative

Helping to create a more secure digital future

NCC Group Version 1.1

December 2024

Contents



Executive Summary

Introduction

The Department for Science, Innovation and Technology (DSIT)[1] Future Radio Access Network Competition (FRANC)[2] was created to support the Government's 5G Supply Chain Diversification Strategy by providing funding for Open Radio Access Network (RAN) research and innovation. The aim of the programme is to (1) accelerate Open RAN adoption in the UK, (2) diversify the supply chain by supporting projects that could maximise the benefits of Open RAN and (3) create new opportunities for suppliers and users of the technology, while gaining insight into the cyber security challenges presented by such deployments.

It also aims to identify good security approaches that future projects should consider when planning similar development or deployment of Open RAN technology.

This white paper articulates some of the high-level cyber security insights identified in a more detailed non-public report completed by NCC Group for DSIT, following a review of a cross section of the FRANC projects in the programme. This review considered aspects including:

- security procedures implemented.
- security achievements from the projects.
- lessons learned on the application and validation of security across Open RAN technologies

1. Formerly Department for Digital, Culture, Media and Sport (DCMS)
2. https://www.gov.uk/guidance/future-ran-diversifying-the-5g-supply-chain-competition-winners

High Level Findings & Recommendations

The FRANC projects covered a wide range of aspects of Open RAN with only a small subset focusing specifically on Open RAN and telecommunications security. There were key themes across the projects from a security point of view, which are summarised below.

Best practice

Security best practice was observed and there was noticeably more robust engagement on security across the projects than previous funded programmes. This was a positive result of the work that DSIT put into the FRANC bid prior to the project starting, such as requiring all projects to appoint a security lead, and submit a security strategy and final security report.

Four of the projects looked in detail at various aspects of security of Open RAN deployments, which reflects the growing need to ensure telecommunication solutions are secure.

There is always the need for those developing and deploying Open RAN to demonstrate the use case and develop the equipment but this can mean that security may not always be appropriately deployed to achieve project deadlines. The use cases of such projects can have different risk profiles but they always represent opportunities to ensure that security is embraced as an integral component of the approach and solution.

Recommendation - Security is an increasing requirement in the telecoms market, which is driven by UK and other global regulatory pressures and commercial factors such as the growth in ransomware attacks. Therefore, embedding security practices throughout the project cycle will better serve project participants either through better testing practices or indirectly through improved capability for future solutions. Consortiums developing Open RAN solutions should determine which partner is responsible for incident management in the event of a security incident and define clear guidelines for management.

Collaboration

There were positive examples of security collaborative effort both within and across FRANC projects, which helped with the sharing of insights to improve security understanding and implementation.

There can be notable differences in defining a consortium-led security strategy document among projects. With multiple participants involved each with different safety and security compliance requirements, plus varying levels of maturity against these requirements, this can make it difficult to agree how to best to define and assess a project's cyber security posture so that the correct actions can be taken to address any gaps. This typically progresses more effectively when a security governance process is put in place aligned to a security framework that all participants can aim to comply with, which then drives improved security implementation in the final solution.

Similarly, there can be a lack of detail created by those involved in each project on how foreground intellectual property (IP) produced as part of a project should be managed and secured once the project is complete. Projects should consider the handling of foreground IP in some detail between the project participants, including data storage and transmission security practices between partners.

Recommendation – Project participants should develop a jointly agreed security strategy and guidance document, which is underpinned by assessing threats to the solution and using a common framework such as ISO27001 or the NCSC Cyber Assessment Framework [3] (CAF), as ways to improve the security outcome of their Open RAN project. The security strategy developed should ideally include specific details about how the project will secure and handle the background Intellectual Property (IP) among consortium members and how they will store and manage the IP that is produced once the project has finished.

3. https://www.ncsc.gov.uk/collection/caf

High Level Findings & Recommendations

Ecosystem

Within the FRANC projects there were a wide variety of types of project stakeholders from a range of sectors participating in the Open RAN projects, including project testbed leads, RAN / hardware suppliers, universities, and system integrators. This meant that there were varying levels of understanding of the technologies involved and the associated security implications when deployed in the use cases. Whilst such diversity in the projects created opportunities for new insights for those taking part, it also presented challenges in cohering the security requirements to create an acceptable security posture.

There was some excellent work done in this space by FRANC projects defining the security maturity of their consortium members and was typically achieved by having a dedicated security lead. This lead ensured the definition of the security strategy aligned to an agreed security framework underpinned by appropriate security standards with periodic review to measure levels of implementation. This level of co-ordination against an agreed target state based on industry best practice and standards, meant it was possible to measure levels of maturity of each of the participants.

Recommendation - Similar projects should ensure they review the security of their consortium members and have a security lead with a high security ability to ensure that security is appropriately deployed. If a consortium feels it doesn't have an appropriate security lead capability, then a third-party organisation should be considered to aid the project.

Security Architecture

There were examples of projects describing aspects of their security architecture of their test environments within their security documents. Having detailed security architecture diagrams demonstrating security measures for the network environments is fundamental to ensuring that security is being incorporated effectively. Such documents will also enable easier on-going assessment of whether security of an environment and any associated data storage is appropriately protected.

Recommendation - The security architecture of any telecommunications network environments should be documented as it is an important component of security work to ensure secure-by-design principles can be incorporated and validated.

Supply Chain

Some projects had issues with acquiring equipment which led to time constraints and the need for system redesign, both of which could potentially lead to a reduction in planned security implementation. In some cases significant potential security issues were found with suppliers, which led to projects identifying alternatives to be used. It adhered to the requirement to check their supply chains and that no equipment from vendors designated as high-risk vendors was purchased as part of the FRANC funding. Open RAN projects designed to increase supply chain diversification mean it is even more important that security best practices such as secure by design, validation through security testing/auditing, robust intellectual property and supply chain controls are implemented so that such diversification ideally also brings with it improved security alongside commercial gain.

Recommendation - Consortiums deploying new Open RAN solutions should establish third party supplier security best practices and risk management from the outset. Malicious exploitation by threat actors of organisations that operate through third parties (business partners or supply chain) is growing and having a clear approach to third-party cyber assurance in all projects is essential.

Additional recommendations

In addition to some of the recommendations made above the below are aspects that projects undertaking new technology development and Open RAN deployment, especially when working in a consortium, should consider based on the insights gained from the FRANC projects.

Area	Recommendation
Architecture	Undertake detailed documented security architecture reviews to ensure that potential threats and vulnerabilities can be identified and remediated or mitigated.
Best Practice	Use existing best practice guidance, such as that provided by the NCSC, to address security issues including those related to secure development lifecycle, backups, and access controls.
Budget	Set a level of minimum percentage budget to be spent on security such as 5% to 10% of overall project budget. This can vary significantly depending on level of technology readiness levels, but having a suitable defined budget is essential to ensure security is appropriately embodied because of allocated funding.
Cloud	Where cloud-based solutions are involved, clearly define the security requirements and incorporate cloud security hardening. Having secure cloud resources will enable a project to achieve appropriate levels of cyber resilience.
Documentation	Ensure a security strategy, plus policies and standards are documented so that they can be clearly understood by all participants to drive their adoption. This will also ensure that the solution security posture can be validated and improved throughout the project.
Frameworks	Existing security frameworks for threat modelling and risk modelling should be utilised to ease security implementation and assessment of security posture.
Intellectual Property	IP protection guidance should be followed that includes detailed security controls, applied both during the project lifetime and after the project has finished. This will ensure that the value of any IP derived from a project is suitably protected.
Monitoring and Auditing	Ensure appropriate security monitoring is in place and undertake basic auditing to identify potential security events so that they can be rapidly responded to when they occur.
Risk Assessment	Use available tools to assist with managing security risk assessments. Consider the use of Cyber Risk Quantification (CRQ) approaches to risk management, which provide predictions of financial loss from a range of cyber threat scenarios. Such risk assessments will allow for the most appropriate level of security to be better defined and implemented.
Supply Chain	Maintain a clear understanding of the project supply chain and where feasible maintain a list of potential alternatives in case of supply chain issues. Security threats to organisations via their supply chain are ever increasing, so ensuring that the supply chain is understood means that associated risks can be monitored and mitigated.

Summary

It was clear the recommendations from DSIT to implement security controls had been considered by the FRANC projects. They also provided insight that where similar projects embark on development of Open RAN solutions they need to ensure that the drive to achieve timelines does not take precedence over security. Rather, security needs to be a fundamental part of any future Open RAN work by any project especially if developing a productised solution that will need to operate in an environment of increasing threats and regulatory requirements.

Projects can fail to implement risk or threat modelling sufficiently. In the absence of effective risk management governance and adequate resources, Open RAN projects such as these may inadvertently introduce new threats and vulnerabilities. Without proper understanding and approaches to address these risks, a project's Open RAN security posture can be compromised. To ensure that informed decisions can be made at the start of the project, threats and risks have to be defined and aligned with any subsequent security implementation. All Open RAN project stakeholders should be informed in a manner appropriate to their understanding of cyber security, so that all members are aware of the risks to the project and the benefits of implementing security controls.

While there's often a push by projects to rapidly launch Open RAN products and services, it's essential for any project not to adopt an excessively high security risk tolerance. Instead, it's advisable to incorporate the necessary Open RAN specific security measures during the initial stages, aligning them with full-service deployment requirements. This approach provides valuable insights such as any impact on performance or guidance that needs to be documented which will support future product commercialisation. Retroactively adding security to meet regulatory compliance and client demands is almost invariably more costly, less efficient, and may even jeopardise project viability. Using a specific security lead from within the project or from an external third-party company is recommended to improve the quality of the security a project implements.

Several FRANC projects demonstrated that when implementing new Open RAN solutions, adhering to baseline well-established cybersecurity best practices—such as secure-by-design principles, supplier validation, and monitoring — aligned to industry Open RAN security guidance can effectively address the majority of security issues. By consistently applying these concepts across all future Open RAN projects and adapting them based on technology readiness levels (from research to product launch), organisations can design, develop, implement, and maintain the most appropriate cybersecurity posture for their Open RAN solutions.