



INFORMATION
RISK MANAGEMENT

CASE STUDIES

A blurred background image showing several hands holding smartphones, suggesting a theme of mobile technology and connectivity.

IRM IN THE WORLD OF TELCOS.

altran

SECURE CYBER **UNLOCK OPPORTUNITY**

IRMSECURITY.COM

Telecommunications organisations play an important part of the Critical National Infrastructure, and our day-to-day reliance on telecom networks is ever increasing.

With this in mind, the National Cyber Security Centre (NCSC) has recognised that telcos need to provide "the highest practical levels of security."

Maintaining compliance and managing cyber risk is increasingly complex for the telecommunications sector, especially as they operate in a highly-competitive arena. Detailed below are just some of the cybersecurity challenges they face:



HOW CAN IRM ASSIST THE TELECOMMUNICATIONS SECTOR?

.....

Altran's World Class Center for Cybersecurity

For over two decades, IRM have collaborated with a wealth of telecommunications organisations, in both a consultancy and GRC platform capacity. Following our acquisition by Altran in 2017, we were appointed as their World Class Center for Cybersecurity, expanding our global reach to assist telecommunications organisations working across multiple geographies.

Our key services include:

- **Strategic GRC** - we assess your current security stance and make recommendations for improvement and compliance.
- **Security Testing** - our technical consultants will utilise a wide scope of testing to identify vulnerabilities and advise how to fix them.
- **SYNERGI GRC Platform** - our all-in-one platform offers a 360 degree approach to GRC and increases an organisation's visibility of challenges and cyber threats.



CASE STUDY 1

VODAFONE & SYNERGi: CYBER CHANGE PROGRAMME



IRM and Vodafone's collaboration grew from a simple GAP Analysis programme, which identified the primary GRC challenges the organisation was facing: a robust global architecture was required to effectively report back to the Group CISO office.

Context & objectives

- Vodafone's governance was limited to a detailed set of policies but these were not supported by best practice controls; assurance activities; and evidence.
- They had good organisational structure but controls were not fully documented or embedded into daily practice.
- 11 incident, vulnerability, asset and technology solutions were in place but stakeholders were overwhelmed with data and lacked overall visibility.

Approach & deliverables

- Implementation of the SYNERGi GRC platform providing:
 - A single out-of-the-box management for visibility of compliance across ISO27001, SOX, GDPR etc.
 - Visibility of technology and information / data assets, allowing stakeholders to validate compliance
 - A consistent language and methodology for governing risk has been established aligned to Vodafone's objective
 - Confidence that the data sources are both accurate and being managed effectively
 - Ability to quantitatively measure its cybersecurity posture through notification of emerging threats
- Vodafone's implementation of SYNERGi provides an integrated GRC framework- this "prestige" project will eventually encompass all 24 OpCo's and their joint ventures; providing the architecture to give true Insight and Control to the Group CISO office.

CASE STUDY 2

TELEFÓNICA SPAIN & SYNERGi: THE 'CENTINELA' PLATFORM



An initial Modelling project within SYNERGi allowed Telefónica to have a clear overview of their security stance. It became apparent their specific needs would require the evolution of a bespoke, more specialised platform. 'Centinela' (meaning 'guard') was born.

Context & objectives

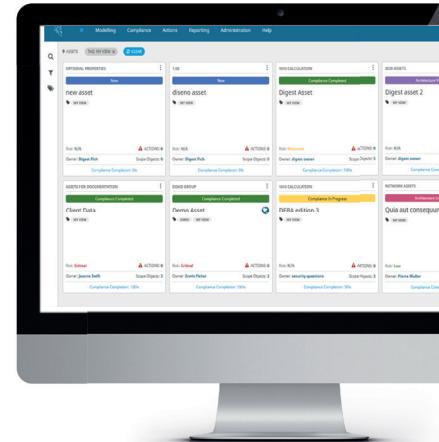
- The four main objectives of the platform were to:
- Integrate with Telefónica's risk analysis.
 - Effectively manage assets.
 - Automate compliance questionnaires.
 - Auto re-assess compliance and risk levels.

Approach & deliverables

Centinela focusses on an asset-centric approach, ensuring that Telefónica have a dynamic dashboard that clearly shows the relation between asset risk and compliance levels so that remediation actions can be easily prioritised.

Having developed the user-friendly interface, IRM and Telefónica worked on the following:

- Enhanced the asset creation process automatically attaching all applicable controls.
- Created automated questionnaires and auto-calculation of compliance and risk levels.
- Pre-defined cross-controls for the security team.
- Created a unified library to streamline mapping.
- Developed recommendations to the user as to what to prioritise and autogenerate recommended solutions for each non-conformity.



CASE STUDY 3

TELEFÓNICA UK & IRM: CONSULTANCY SERVICES



For five years, IRM has been working alongside Telefónica UK to support their security management.

..... Projects to date

With our team of 35+ penetration testers accredited to CHECK standard, IRM has been able to support Telefónica across a number of projects including:

- Web application testing
- Internal infrastructure testing
- Build reviews
- Log reviews
- Database reviews
- Network testing
- Mobile application testing
- Vulnerability assessments

All security testing with Telefónica is aligned to standards relevant in the telecommunications industry, such as the Commodity Assurance Services (CAS) Telecommunications scheme. This standard sets out the recommendations and considerations for technical consultants when conducting testing, helping to align to ISO27001:2005 controls.

..... Upcoming projects

As of February 2020, IRM has embarked on its largest project yet with Telefónica. The engagement is made up of 17 phases and involves various technical consultancy requirements including build reviews, mobile app testing and configuration reviews.

This project requires IRM to carry out the annual end-to-end tests on Telefónica's UCaaS (Unified Communications as a Service) platform. The platform combines cloud-based telecommunications with collaboration and conferencing tools enabling Telefónica to simplify their operations, improve user support and reduce costs. The project we are embarking on will include the testing of their Skype and Mitel hosted offerings.





**Think cyber.
Think security.
Think data.**

For more information on how IRM can help telecommunication organisations please contact hello@irmsecurity.com

**SECURE CYBER
UNLOCK OPPORTUNITY.**