IRM INFORMATION RISK MANAGEMENT
•ALTRAN GROUP

CASE STUDY

RISK MANAGEMENT: CASE STUDIES.

ALTRAN

SECURE CYBER **UNLOCK OPPORTUNITY**

IRM**SECURITY**.COM

EXAMPLES OF IRM'S RECENT RISK MANAGEMENT PROJECTS

Leading Financial Services Company - GDPR Assessment

Context and Objectives

The client wanted to achieve compliance with the European best-practices and regulations regarding the security of customer personal data.

They also wanted to identify and characterise all personal data being handled by its systems, develop processes and implement measures that mitigate the risk of data breach in accordance with the GDPR.

The client had no deep knowledge on how to address the GDPR from a technical perspective and but understood the benefits it could bring.

Approach and Deliverables

We adopted a joint development of a methodological approach to address key requirements of the GDPR. We used technical knowledge, ITIL best practices, ISO 27001 and BS 10012 standards to help client assess its IT service catalogue and infrastructure regarding GDPR comprising areas such as information systems, data centre (managed services), network engineering, operations & supervision and service platforms.

We interviewed around 30 stakeholders for a complete assessment regarding personal data on more than 200 different systems. A risk analysis assessment was carried out regarding personal data and development of policies and methodologies to monitor and control personal data.

This process enabled us to advise senior management on which measures to take such as privilege access management, event correlation, GRC framework implementation and database hardening and auditing.

Global Insurance Company - Information Security Control Framework

Context and Objectives

In a heavily regulated financial services market, the client needed to demonstrate it had a robust control framework in place to address information security challenges and that business information (including that of its clients and customers) was sufficiently protected from unauthorised access, misuse or alteration.

The client had pockets of good practice and defined processes but were unable to show consistency across the global group of companies. Their policies and standards had not been managed and maintained and as such there was a lack of clarity around the baseline security expectations within the organisation.

Approach and Deliverables

An initial assessment was completed to determine the maturity and implementation of existing controls and identify where uplift was required.

We carried out a formalisation of a control framework benchmarked against industry best practice and mapped to security control frameworks widely used across industry (including ISO 27001, NIST Cyber Security Framework and the COBIT 5 methodology).

This enabled us to develop a suite of information security, IT policies and standards to provide complete clarity of the mandatory baseline expectations. We designed and delivered training packages to ensure staff were clear on their personal responsibilities in upholding policies and standards. Finally, we integrated this practice into existing frameworks including risk management, procurement and internal audit to ensure the control set complemented the already embedded governance structures and ways of working.

MORE THAN JUST AN 'RISK MANAGEMENT PROJECT'...

Private Client Fund and Wealth Manager - Cybersecurity Maturity Assessment

Context and Objectives

The client was aware of changes being driven externally resulting in more scrutiny from their regulators – the Securities & Exchange Commission (SEC) in the U.S. and the Financial Conduct Authority (FCA) in the UK.

They needed to establish a current baseline of maturity allowing an understanding of their current stance with respect to cybersecurity and the protection of critical information assets.

They also wanted to establish an overall security improvement programme to identify key risks and a plan for mitigation activities to drive a programme of change and increased cybersecurity maturity.

Approach and Deliverables

We undertook a cybersecurity assessment to understand the security current control maturity with regards to cybersecurity. This was based upon various standards and control frameworks including the NIST cybersecurity framework, the UK Government's 10 Steps to Cybersecurity, ISO27001/2 and PAS555. We took the salient elements from each of these to undertake the assessment.

This process enabled us to develop a tailored approach to identifying key cyber risks at the client that was proportionate their risk profile. As part of the process, we conducted interviews with over 20 key stakeholders and personnel, and conducted interviews where appropriate with third party service providers.

We reviewed documentation containing information about the client's security processes and procedures and also reviewed the results of internal audits. We presented a report back to the client to provide an overview with recommendations and observations.

IRM INFORMATION RISK MANAGEMENT
•ALTRAN GROUP

Think cyber.
Think security.
Think data.

For more information on our cybersecurity services please contact:
hello@irmsecurity.com

SECURE CYBER
UNLOCK OPPORTUNITY.