



# ALTERNATIVE SOLUTIONS

## Information Security for Alternative Solutions and our Clients

Alternative Solutions has implemented an Information Security Management System (ISMS) based on the ISO/IEC Standard 27001:2013. The objective of the ISMS is to ensure business continuity and to minimise business damage by preventing and minimising the impact of security incidents.

## Why is an ISMS Necessary?

### GFSC- Data Security – Regulated entities

Many of Alternative Solutions Customers and Clients are Guernsey Financial Services Commission (GFSC) licenced/ regulated entities.

Alternative Solutions therefore needs an awareness of what the regulator expects of a licensed/regulated company and by understanding this ensures that we are in a position to offer best advice. Whilst we are not a regulated entity we must provide assurance giving confidence to our clients and customers that we take security seriously. Not only that, we believe the regulator will be aware who the IT Service Provider is for each such company. Therefore we consider that our clients and customers must show their IT service provider is able to demonstrate that they have completed due diligence and a risk assessment. By adopting an ISO 27001 framework we are sending out a clear message that we understand the risks and we follow best practice.

### GFSC - Data Security Thematic Reports – The Banking and Fiduciary sectors

The GFSC has published two reports, one relating to the Banking Sector in February 2012 and more recently one relating to the Fiduciary Sector, in April 2014.

The theme running through these publications endorses that **“the ISO 27001 sets the standard for several areas of good practice ..... would encourage licensees to bench mark their own data security practices against the ISO standard”**. Interestingly the most recent Fiduciary Sector Thematic Report refers to the Data Security practices in the banking sector report and concludes **“In that sector robust data security is regarded as fundamental to confidence in private banks. We believe that this applies equally to trust and company service providers.”** The foreword ends with the words **“ ....the outcome of this report should be an active response and not a passive one.”**

The Executive Summary concludes **“Overall, the Boards of licensees need to take a more active approach to managing information security risk. This requires the establishment of an effective governance structure for data security risk .....Risk assessments, control reviews, and remedial plans are then executed in a continuous cycle of improvement”**.



# ALTERNATIVE SOLUTIONS

## **Security Management Services**

Gaining a full understanding of the ISO standard and the implementation of an effective ISMS takes considerable time. Alternative Solutions have taken a year to plan and implement its own ISMS and the skills we have learned and knowledge we have acquired can be used to help our clients improve their security standards.

## **Benchmarking**

To establish if existing security management systems are in line with ISO27001:2013 requires knowledge of the standard. We can provide a service to benchmark your systems against the standard and highlight any areas of concern.

## **Security Risk Management and Assessment**

Security Management risk assessments/risk measurements based upon the ISO 27001 standard methodologies. These could either test specific risk areas (e.g. physical building security, procedures or access control) or across the whole of the ISO 27001 series gambit.

## **Technical IT security risk assessment**

Alternative Solutions has long had the technical knowledge to evaluate the security risk to systems and to identify products to mitigate such risk. The implementation of ISMS allows us to provide this in a more structured manner against agreed procedures.

## **ISMS Implementation**

Alternative Solutions have tested policy and procedures; risk testing regimes, asset registration templates. These can be used along with our expertise to expedite the implementation of ISMS in client sites.

## **“Security Officer” - Provision to Clients**

The provision of a Security Management System requires expert supervision, audit and a regime of continual improvement. These ISMS requirement therefore need a permanent resource to be responsible for oversight. However in the same way as regulatory compliance and IT Services can be contracted out by companies, the services of a “Security Officer” could be shared.

## **About the author**

Rob Prow worked for the Guernsey Border Agency, formerly Customs and Immigration, for over forty years, reaching the post of Chief Officer. Much of the work involved complex investigations working closely with other agencies. Creating effective policies and procedures was critical to efficient working. Since leaving the Agency, Rob has worked for Alternative Solutions primarily on the implementation of ISMS, although his organisation skills made the recent office move very efficient. He has gained an excellent knowledge of the ISO 27001:2013 standard. Rob can be contacted on 01481 701234 or by email [rob.p@asl.gg](mailto:rob.p@asl.gg)