2

Business Case for An  
Information Security Management System (ISMS) Based On The ISO/IEC 27000 Series Standards (ISO27k) For Crown Bank

Executive summary

**Benefits**

The ISMS will place Information security under strict management supervision, allowing for guidance and Improvement where necessary. Improved Information security reduces the risk (of occurrence and/or negative consequences) of events, lowering incident-related losses and expenses.

Other Benefits,

A organized, consistent, and professional approach to Information security management, in line with other ISO management systems

Demonstrable governance utilizing globally known good security practices

Comprehensive information security risk assessment and treatment according to business and security priorities

**Costs**

Because information security is a business and compliance need, the majority of the expenses associated would be expended anyhow. The following are the specific expenses associated with the ISMS: • Resources required to develop, implement, and run the ISMS, including project management for the implementation project

Various company processes and activities must be changed to confirm ISO standards

Third-Party compliance audits(optional -only necessary if we chose to pursue certification,which we may do after the ISMS is up and running

# Introduction, scope and purpose

The Crown Bank operates all across the island, and they offer, retail banking, corporate banking, international banking, treasury, project funding.

The Crown Bank has more than 250 branches across the island and more than 1000 employees.

(ISMS) will be helpful to ensure that they are following information security laws and regulations.

# ISMS benefits

These are the ways in which an ISO27k ISMS will typically benefit the organization.

## Information security risk reduction

• Using a thorough, well-structured process, all relevant information security risks, vulnerabilities, and impacts are more likely to be discovered, assessed, and treated effectively.

• This approach ensures consistency across various information communications systems (ICT) and corporate processes, while also tackling information security risks in order of importance.

• They get a better understanding of information security terms, hazards, and controls

## Benefits of standardization

• It may be utilized in multiple departments, roles, and organizations without major modifications, avoiding the need to specify the same core rules over and over again.

• If the firm is able to focus its efforts and resources on additional security needs, information assets can be better safeguarded.

• In accordance with globally recognized and acknowledged security standards.

• The ISO27k standard suite is updated and maintained on a regular basis by standards bodies, taking into account new security concerns.

Unnecessary or excessive limitations can be relaxed or removed without affecting the integrity of critical information.

## Benefits of a structured approach

• Assembles a logically consistent and comprehensive framework ogt of various information security controls.

• Allows for the measurement of performance and the gradual improvement of information security over time.

• Creates a unified set of information security rules and procedures

## Benefits of certification[[1]](#footnote-1)

• An independent, trained assessor's certification that the organization's ISMS satisfies ISO/IEC 27001 requirements.

• Assures a company's capacity to deal with data security.

## Benefits of compliance

• By utilizing common characteristics, ISO27k provides a framework for information security management that encompasses a wide variety of needs, both external and internal. • Although stakeholders or authorities may need ISO27k compliance as a condition of doing business or to comply with privacy and other requirements at some point, it is likely to be more cost-effective to implement IS027k on our own terms and timelines.

# ISMS costs

These are the main costs associated with the management system elements of an ISO27k ISMS[[2]](#footnote-2).

## ISMS implementation project management costs

• Develop a comprehensive information security management strategy that is related to other business objectives and imperatives in addition to ISO27k (typically but not always the person who will eventually become the CISO or Information Security Manager).

• To create a project team, you must first seek authorization from management.

• Maintain frequent project management meetings with key stakeholders through hiring/assigning, managing, directing, and tracking varied project resources.

• Include regular status reports and progress updates in the process of comparing actual progress to planned,

.

## Other ISMS implementation costs

• Make a list of all the information assets you have

• Make security risks to data assets a top priority.

• Make. a decision on how to deal with information risks.

• For the organization, create a security architecture and a security baseline.

• Existing security measures and risk treatments can be rationalized, upgraded, supplemented, or retired, as appropriate, in addition to reviewing/updating/reissuing current information security policies and regulations and developing/issuing new information security processes, guidelines,

and contractual conditions.

## Certification costs

After analyzing the issue, choose a suitable certifying body.

• An ISO/IEC 27001 certification agency inspects and audits the system.

## Document history

**2012**: template extensively revised as version 2.

**2008**: first public release of the generic template as part of the free [ISO27k Toolkit](http://www.iso27001security.com/html/iso27k_toolkit.html).

**1995-2008**: underlying concept gradually developed and refined through a number of project proposals, security strategies *etc*. with various organizations.

## Copyright

This work is copyright © 2012 [IsecT Ltd](http://www.isect.com/)., some rights reserved.  It is licensed under the [Creative Commons Attribution-Noncommercial-Share Alike 3.0 License](http://creativecommons.org/licenses/by-nc-sa/3.0/).  You are welcome to reproduce, circulate, use and create derivative works from this *provided* that (a) it is not sold or incorporated into a commercial product, (b) it is properly attributed to [IsecT Ltd.](http://www.isect.com/), and (c) derivative works, if shared with third parties, are shared under the same terms as this.

1. The ISMS may optionally be formally audited against and certified compliant with ISO/IERC 27001 by a certification body duly accredited by ISO. Normally management decides whether to go ahead with certification once the implementation project is finished and the ISMS is fully operational. [↑](#footnote-ref-1)
2. Note that the ISO27k standards *recommend* but do not *require* any specific information security controls – it is up to management to determine and treat the organization’s information security risks as appropriate. Therefore, the costs of any information security controls that are implemented through the ISMS as a result of such management decisions are *not* separately identified in this template since they would presumably have been required even without the ISMS in place. However, you may prefer to identify any significant security investments that you know will be required in your business case or project proposal (perhaps with a similar note!). [↑](#footnote-ref-2)