

Information Security Forum Terms of Reference

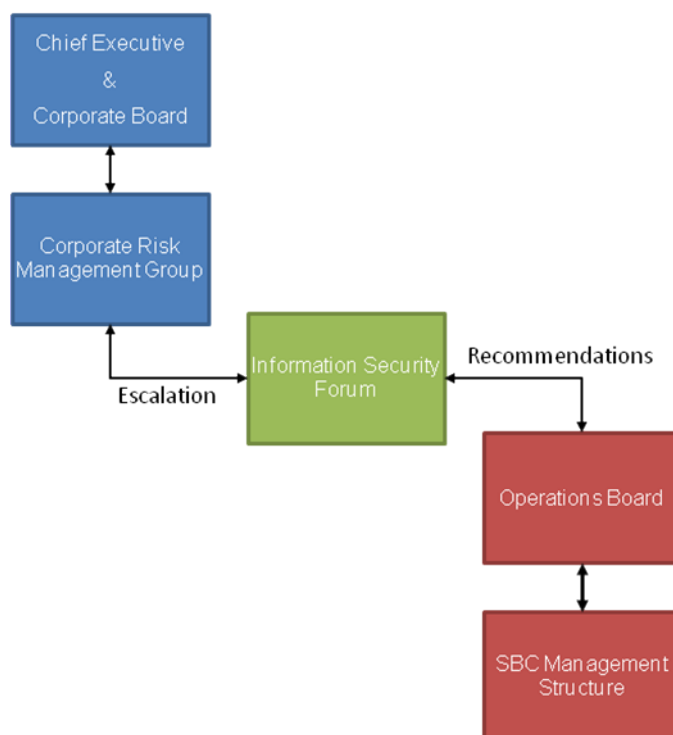
Background

On the 12th January 2009 Swindon Borough Council's Risk Management Group approved the creation of an Information Security Forum (ISF) to coordinate activity on Information Security with an objective of helping the organisation comply with the requirements of International Information Security Standard ISO27001.

One of the key principles within ISO27001 is that appropriate consideration is given to information security issues at senior management level. To facilitate compliance with this principle, a framework will need to be identified within the Council and Capita management structures to initiate and control the implementation of information security and the associated risk management processes. The ISF will present recommendations for this framework.

The ISF will act as a resource to SBC Operations Boards to create and monitor an Information Security Framework. Operations Board will retain responsibility for information security. The ISF will have an escalation path via the Corporate Risk Management Group and responsibility to use this path if it feels that actions or inaction is putting the Council at risk.

Information Security Forum in Context



Purpose

The ISF will provide clear direction, support and consideration to the management of security initiatives and information risk management.

The broad principles are as follows:

- Information Security needs to be a key consideration in everything we do as a Council. The ISF, via Operations Board, will promote this thinking.
- The responsibility for compliance with good practice is with each staff member. The ISF role is to make this responsibility clear.
- The ISF will be convened with subject matter representatives from all business areas of the organisation.

Key Functions

The Forum has the following initial actions as assigned from the Corporate Risk Management Group:

- To Create a Staff Awareness Program with regular updates
- Review existing information security policies to ensure relevance and ease of understanding
- Develop a information security incident management process
- Develop a Risk Based approach to ISO 27001 compliance

The Forum also has the following specific functions:

- To review and recommend the Security Policy and ISF responsibilities. (The Information Security Policy will be reviewed as a matter of course on an Annual basis by the ISF during the first quarter of each Calendar year. However, should any single security incident, or an accumulation of several incidents create a situation where the Policy needs to be reviewed and updated as an exception, then the ISF has responsibility to do so, as required, whether it be at an agreed ISF meeting, or by calling an emergency meeting of the ISF as needs arise)
- To monitor exposure of Council information to major business risks.
- To review security incidents and take action as appropriate.
- To recommend to Operations Board initiatives to enhance the information security management system including policy changes, training programmes etc.

Membership

The membership of the group will evolve as the requirement of the ISF change. Initially the membership of the Forum will consist of the subject matter experts in fields aligned to Information Security. Initial membership will consist of;

- Risk Manager
- Head of Internal Audit
- Computer Auditor
- Data Protection Officer
- Director of HR and Change
- Capita ICT Operations Manager
- Freedom of Information Officer
- Business Architect (ICT Security)

In addition an extended membership will provided additional expertise as specific issues require such as procurement, schools information security etc.

Meeting Frequency

The Forum will meet bi monthly (or else following a major information security incident or at the request of Senior Management). However the forum will put emphasis on communication and delivery in the time between meetings.

Regular Agenda

The Information Security Forum (ISF) will potentially address some or all of the following:

- Results of internal audits and reviews
- Feedback from interested parties
- Techniques, products or procedures which could be used in the organisation to improve the ISMS performance and effectiveness
- Status of preventative and corrective actions
- Vulnerabilities or threats not adequately addressed in the previous risk assessment
- Results from effectiveness measurements
- Follow-up actions from previous management reviews
- Review all security incidents and determine if action is required that could affect the ISMS or the Information Security Policy.
- Recommendations for improvement to be submitted to Operations Board.