MANAGING INFORMATION RISK IS A BUSINESS ESSENTIAL

As information risks and cyber security threats increase, organisations need to move away from reacting to incidents toward predicting and preventing them. Developing a robust mechanism to assess and treat information risk throughout your enterprise is a business essential.

The ISF solution: IRAM2, a methodology to meet today’s challenges.

IRAM2 helps information risk practitioners, as well as other risk, business and technology leaders to:

- **Apply a simple, practical, yet rigorous approach**: focus on simplicity and practicality, while embedding rigour throughout the assessment process. This enables consistent results and a depth of analysis that enhances business decision making.
- **Focus on the business perspective**: guide information risk practitioners’ analysis so that information risk is assessed from the perspective of the business. The end result is a risk profile that reflects a view of information risk in business terms.
- **Obtain a greater coverage of risks**: enable a broader and more comprehensive risk coverage, thereby reducing the chance that a significant risk will be overlooked.
- **Focus on the most significant risks**: allow key business and technology stakeholders to obtain a clear picture of where to focus resources, in order to deal with information risks that are most significant to the organisation.
- **Speak a common language**: provide a common vocabulary and framework, enabling information risk practitioners and management to form a unified view of information risk across different areas of the business and better integrate into enterprise risk management.
- **Engage with key stakeholders**: empower information risk practitioners to engage with key business, risk and technology stakeholders in an organised and enterprise-aware manner.

IRAM2 is supported by four IRAM2 Assistants, each accompanied by a practitioner guide, that help automate one or more phases of the methodology.
The IRAM² information risk assessment methodology is set out in six phases. Each phase details the steps and key activities required to achieve the phase objectives, as well as identifying the key information risk factors and outputs.

**IRAM²: The next generation**

**A** Scoping

Provide a business-centric view of risk

**IRAM²** provides guidance for scoping information risk assessments across both the business and technology. Risk practitioners use this phase to provide an integrated view of risk from the business service layer down to the technology infrastructure.

**B** Business Impact Assessment

Assess realistic and impact scenarios

**IRAM²** provides guidance for impacts. Risk practitioners will use this phase to provide a business-centric view of risk from the integrated view to provide an integrated view of risk from the business service layer down to the technology infrastructure.

**C** Vulnerability Assessment

Understand how well your environment/systems can resist threats

**IRAM²** provides guidance for performing an assessment of vulnerabilities that influence the likelihood of a threat event being successful. Risk practitioners use this phase to determine control strength.

**D** Risk Evaluation

Evaluate risk against your organisation’s wider enterprise risk framework

**IRAM²** provides pragmatic guidance to help evaluate risks following the business impact assessment stage. Risk practitioners use this phase to map the likelihood of successful threat events to the most effective control strengths.

---

Example threat events

- Explicit vulnerabilities in an organisation's information systems
- Unauthorised monitoring and/or modification of communications
- Loss of information systems
- Software malfunction (maliciously produced software)
- Power failure or fluctuation
- Flooding

Example components

- Component A
- Component B
- Component C
- Component D
- Component E
- Component F

<table>
<thead>
<tr>
<th>IRAM² control number</th>
<th>IRAM² control strength</th>
<th>Calculated control strength</th>
<th>Moderated control strength</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Information...</td>
<td>High</td>
<td>High</td>
<td></td>
</tr>
<tr>
<td>2 Users should...</td>
<td>Moderate</td>
<td>Low</td>
<td></td>
</tr>
<tr>
<td>3 The duties of...</td>
<td>High</td>
<td>High</td>
<td></td>
</tr>
<tr>
<td>4 Staff working...</td>
<td>Low</td>
<td>Low</td>
<td></td>
</tr>
<tr>
<td>5 Staff working in...</td>
<td>Negligible</td>
<td>Low</td>
<td></td>
</tr>
<tr>
<td>6 IT staff should...</td>
<td>Negligible</td>
<td>Low</td>
<td></td>
</tr>
<tr>
<td>7 Business users...</td>
<td>High</td>
<td>High</td>
<td></td>
</tr>
<tr>
<td>8 Business users...</td>
<td>Low</td>
<td>Low</td>
<td></td>
</tr>
<tr>
<td>9 Classified information...</td>
<td>Moderate</td>
<td>High</td>
<td></td>
</tr>
</tbody>
</table>
in assessing information risk

Understand and model threats

IRAMz provides guidance for performing a pragmatic assessment of the information threat landscape. Risk practitioners use this phase to identify and profile key threats across different groups by determining associated threat events.

Develop pragmatic risk treatment plans

IRAMz provides practical guidance for treating identified information risks. Risk practitioners use this phase to explore different approaches to treating information risk (i.e. mitigation, avoidance, transference and acceptance).

Assess realistic and worst-case business impacts

IRAMz helps organizations identify and assess business impacts to one of more individuals. It provides guidance for identifying and assessing business responses and use this phase to determine the potential business impact should information assets or systems have their confidentiality, integrity or availability compromised.

Service risk treatment

IRAMz offers guidance to help evaluate risks across a range of impact assessment, threat profiling and risk treatment stages. Risk practitioners use this phase to understanding and modeling threats and to develop pragmatic risk treatment plans.
The *Information Risk Assessment Methodology 2 (IRAM2)* is a simple, practical yet rigorous business essential that helps ISF Members identify, analyse and treat information risk throughout the organisation.

**IRAM2** describes the following:

- **Risk fundamentals**: explains information risk and how it relates to the wider discipline of enterprise risk management.
- **People and engagement**: identifies the people, roles, skills and experience that are vital for effective information risk management and for the application of **IRAM2**.
- **IRAM2 Phases**: provides an overview of the methodology as well as a comprehensive description of the key steps, inputs and outputs accompanied by guidance for effective deployment.

The report also contains detailed supplementary material and further guidance to assist the information risk practitioner. For example, a common threat list, a threat event catalogue and control library are included.

**IRAM2** is supported by a range of deliverables to help Members implement the methodology. These include:

- **IRAM2 Assistants** to help automate steps in the methodology
- **IRAM2 practitioner guides** to support practitioners use of the assistants
- **IRAM2 implementation space** on the ISF Member website, *ISF Live*, which contains a facilitated forum for Members to discuss related issues and solutions, along with additional resources including recorded demonstrations of the assistants.

**IRAM2** is aligned with the *ISF Standard of Good Practice for Information Security* and the *Security Healthcheck*. It also incorporates research findings from *Protecting the Crown Jewels: How to protect mission-critical information assets* and *Threat Intelligence: React and prepare*.

Consultancy services from the ISF provide Members and Non-Members with the opportunity to purchase short-term, professional support activities to supplement the implementation of ISF products including **IRAM2**.

**IRAM2** is available free of charge to ISF Members and can be downloaded from www.isflive.org. Non-Members can purchase the report by contacting Steve Durbin at steve.durbin@securityforum.org.

---

**WHERE NEXT?**

**CONTACT**

For further information contact:

Steve Durbin, Managing Director
US: +1 (347) 767 6772
UK: +44 (0)20 3289 5884
UK Mobile: +44 (0)7785 953800
steve.durbin@securityforum.org
securityforum.org

**ABOUT THE ISF**

Founded in 1989, the Information Security Forum (ISF) is an independent, not-for-profit association of leading organisations from around the world. It is dedicated to investigating, clarifying and resolving key issues in cyber, information security and risk management by developing best practice methodologies, processes and solutions that meet the business needs of its Members.

ISF Members benefit from harnessing and sharing in-depth knowledge and practical experience drawn from within their organisations and developed through an extensive research and work programme. The ISF provides a confidential forum and framework, which ensures that Members adopt leading-edge information security strategies and solutions. And by working together, Members avoid the major expenditure required to reach the same goals on their own.

**DISCLAIMER**

This document has been published to provide general information only. It is not intended to provide advice of any kind. Neither the Information Security Forum nor the Information Security Forum Limited accept any responsibility for the consequences of any use you make of the information contained in this document.