Information Security Forum Updates Information Risk Assessment Methodology

Methodology Helps Businesses Identify, Analyze and Treat Information Risk throughout the Organization

NEW YORK - Aug. 23, 2017 - *PRLog* -- The Information Security Forum (ISF), the world's leading, independent authority on cyber security and information risk management, continues to strengthen its global leadership in providing business-based information risk tools with the announcement of significant updates to the Information Risk Assessment Methodology version 2 (IRAM2). IRAM2 is a practical, rigorous risk assessment methodology that helps businesses to identify, analyze and treat information risk throughout the organization.

Threats, threat events, vulnerabilities and potential impacts are dynamic in any organization, requiring security practitioners and key stakeholders to review risks on a regular basis, particularly when significant change occurs. As information risks and cyber security threats increase, and as Boards take on a greater interest in security and risk, organizations need to move away from reacting to incidents, toward predicting and preventing them. IRAM2 allows key business and technology stakeholders to determine risk versus reward and obtain a clear picture of where to focus resources, to address information risks based on their signi?cant to the organization

"Developing a robust mechanism to assess and treat information risk throughout your organization is essential," said Steve Durbin, Managing Director, Information Security Forum. "Risk assessment is all about balance and IRAM2 allows for teams to assess risk in a realistic manner. IRAM2 focuses on simplicity and practicality, while embedding reliability and steadfastness throughout the assessment process. This enables consistent results and a depth of analysis that improves decision making."

IRAM2 provides organizations with the ability to tailor their threat tables to reflect an organization's overall risk appetite. IRAM2 works by evaluating and assessing a variety of information risk factors that comprise each information risk equation. Its supporting tool, the IRAM2 Assistant, have undergone significant updates and enhancements based on ISF research and member feedback to produce an enhanced suite of IRAM2 products. IRAM2 has the ability to help teams focus on the vulnerabilities as they relate to specific business risks and the Assistant tool takes this one step further. Key updates and enhancements include:

IRAM2

Threat Profiling: Research findings from *Protecting the Crown Jewels: How to protect mission-critical information assets* and *Threat Intelligence: React and prepare* have been incorporated into the supporting information used during this phase, including the common threat list (CTL) and the threat event catalogue (TEC).

Vulnerability Assessment: The approach for determining control strength now includes the extent of 'relevance' and 'implementation' of environmental controls. This enhanced approach is supported with the introduction of control relevance tables (CRT) to provide objectivity and repeatability. The previous IRAM2 control library, consisting of 29 controls, has been replaced with a more comprehensive set of 167 controls based on *The Standard of Good Practice for Information Security* and the *Security Healthcheck.*

IRAM2 Assistants

The single, Excel-based supporting tool, has been split into four integrated modules collectively referred to as the IRAM2 Assistants. Each module supports one or more phases of the methodology. The IRAM2

Assistants provide improved:

· Efficiency: by automating parts of the methodology that would otherwise require a greater amount of manual effort

· Accuracy: by enabling in-depth analysis to enhance business decision making

· Consistency: by delivering specific templates that can be applied for enterprise-wide information risk assessments

· Methods of communication: by leveraging report templates to convey the key risks to stakeholders.

Each IRAM2 Assistant is accompanied by a practitioner guide providing step-by-step instructions on how to use the methodology.

"Managing information risk fundamentally relates to effectively balancing risk against reward," continued Durbin. "IRAM2 empowers information risk practitioners to engage with key business, risk and technology stakeholders in an organized and enterprise-aware manner. With this foundation, they can work more effectively across the organization to assess appropriate risk profiles and provide input to the business to address – or not"

Once de?ned at an organizational level, risk appetite can be communicated and presented differently throughout an organization. If an organization does not have a de?ned risk appetite, the decisions regarding the treatment for each risk will have to be made by the key stakeholders on a risk-by-risk basis. The practitioner should make the key stakeholders aware that the lack of a de?ned risk appetite could result in inconsistent decisions regarding the amount of risk the organization accepts. For more information, please visit the ISF website (http://www.securityforum.org/).

About the Information Security Forum

Founded in 1989, the Information Security Forum (ISF) is an independent, not-for-profit association of leading organizations from around the world. The organization is dedicated to investigating, clarifying and resolving key issues in cyber, information security and risk management and 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 organizations and developed through an extensive research and work program. The ISF provides a confidential forum and framework, which ensures that Members adopt leading-edge information security strategies and solutions.By working together, ISF Members avoid the major expenditure required to reach the same goals on their own. Consultancy services are available and provide ISF Members and Non-Members with the opportunity to purchase short-term, professional support activities to supplement the implementation of ISF products.

For more information on ISF membership, please visit https://www.securityforum.org/.

Contact
John Kreuzer
***@luminapr.com

--- End ---

Source	Information Security Forum
City/Town	New York City
State/Province	New York
Country	United States
Industry	Security
Tags	Information Security, Cyber Security, Risk Management
Link	https://prlog.org/12660022

Scan this QR Code with your SmartPhone to-
* Read this news online
* Contact author
* Bookmark or share online