STREAM

ACUITY RISK MANAGEMENT

HM Government

STREAM For the UK Public Sector

Government Guidance

In March 2015 UK Government updated its guidance on the management of information risk.

The focus of the new guidance is on supporting an effective decision making culture where security is properly considered and integrated with the business. This is a move away from prescriptive approaches of the past to a principles-based approach. Gov.UK website

Risk visibility

Rapid deployment

Easily configurable

On-premise or SaaS

Intuitive

Risk quantification

Six Principles

- Understand the business context
- Decide on the risk management approach
- Understand the key components of risk
- Understand what risks exist
- Communicate risks consistently
- Make informed risk management decisions

Key Elements of this Guidance

Accreditation and IS1/2

- Accreditation and use of previous information risk management guidance – CESG Information Standard 1/2 (IS 1/2) is no longer a mandatory requirement.

Risk Assessment Methods

- Organisations should choose the most suitable method(s) depending on the business need
- Most risk assessment methods can be aligned to the approaches described in the ISO 31000 and ISO 27000 series of international standards.

Key Components of Risk

- Fundamental inputs: Threat, Vulnerability and Impact in relation to Business Assets
- Other inputs: Threat Likelihoods and Asset Valuations
- Output should be meaningful, understandable, realistic, and in context so that it informs risk management decisions and cannot be interpreted in different ways by different people.

Information and Evidence for Informed Risk Management Decisions

- Statements on risks that the organisation will and won't accept in seeking to achieve objectives
- Security controls in place or needed to manage the identified risks
- Evidence of how third parties are managing risk
- Evidence that provides confidence that security controls have been implemented to manage identified risks and will continue to do so throughout the whole lifecycle of the system or service
- Understanding of residual risk - risk that remains after management action has been taken.

Continuous Risk Management

- The focus is on 'ensuring the business understands the risks it is taking' and 'trusting competent people to make decisions' within an environment of continuous risk management instead of one - off risk assessment.

The Need for Automated Support

To meet the new guidance organisations will need access to relevant information. In many cases some form of automated support will be beneficial to:

- Provide visibility of the inter-relationships between risk components in relation to critical business assets
- Communicate risk consistently
- Maintain evidence and a history of decision making
- Be responsive to change and manage risk throughout the lifetime of a system or service.

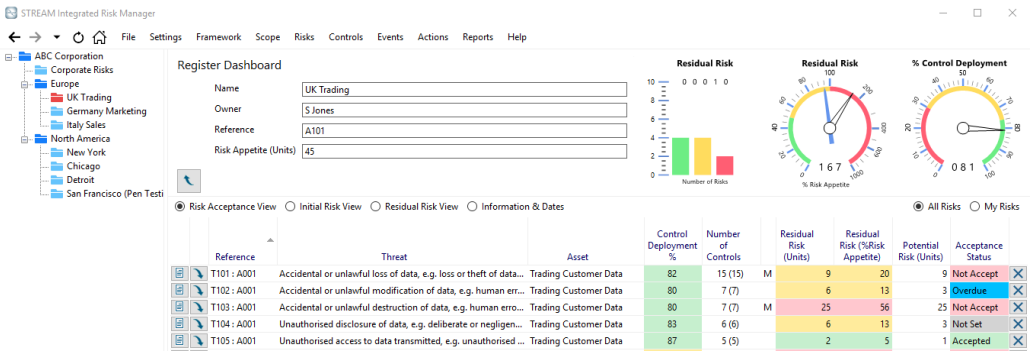
Organisations or CLAS consultants could develop spreadsheet solutions but these suffer from well-documented problems of: scalability; security; errors; dependence on the original author; change management; lack of functionality and lack of workflow.

The Acuity STREAM Proposition

Acuity provides a software solution, STREAM Integrated Risk Manager, combined with an accessible business model which provides public sector organisations and CLAS consultants with flexible automated support for information risk management.

The STREAM Solution

- Asset-based Framework supporting fundamental risk components
- Accommodates HMG Impact Levels and Threat Actors / Models
- Configurable with risk methods, threat lists, vulnerabilities, impacts and security controls to meet business requirements
- History of changes and decisions
- Easy to use with dashboards, graphical reports and a custom report builder
- Action management with scheduling workflow and email alerting.



Contact Us

For further information on STREAM or Acuity Risk Management please contact us:

Info@acurityrm.com

www.acuityrm.com

+44 (0) 20 7297 2086

@AcuityRM

Acuity Risk Management