

STREAM for the Security Policy Framework

STREAM:
A portfolio of products for integrated risk, compliance and performance management

The UK Government's new Security Policy Framework (SPF), launched in December 2008, adopts a four-tiered approach around: business goals; core security principles; key security policies, and; detailed technical standards.

The SPF specifies 70 mandatory requirements but emphasises that these are minimum requirements and that many Departments and Agencies will manage their specific security risks over and above these baseline measures using sound risk management principles, including a detailed risk register.

Acuity's portfolio of STREAM products is an integrated set of software tools for assessing and managing compliance with any set of control standards or risks. Acuity has configured a version of its STREAM product set to help UK Government Departments and Agencies meet the requirements of the Security Policy Framework.



STREAM Risk Registers

Automated Enterprise-wide risk registers

STREAM Compliance Manager

Real-time monitoring and reporting of compliance against control standards

STREAM Metrics Manager

Real-time monitoring and reporting of performance metrics

STREAM Integrated Risk Manager

Enterprise risk management integrated with compliance and metrics management

Features

- ◆ Easy-to-use management dashboards, risk registers and graphical reports
- ◆ Monitor compliance status against the SPF, GSI Code of Connection, ISO 27001, BS 25999 and all other relevant standards
- ◆ Collate all of your Information Assets within STREAM, and use the familiar UK Government IS 1 scale to assess risks
- ◆ Analyse historical trends
- ◆ Track incidents and near-misses with links to risks and controls / actions
- ◆ Available for single-user or Enterprise-wide deployment with extensive user management

Benefits

- ◆ Improve staff productivity by reducing the time required to gather, collate and report on risk, compliance and performance status
- ◆ Reduce the risk of incidents, saving costs associated with incident response, direct losses and reputational damage
- ◆ Reduce the cost of external audits and due diligence by having up-to-date risk, compliance and metrics information immediately available
- ◆ Empower better management decision making through easily accessible risk, compliance and metrics status information.



STREAM Compliance Manager for the SPF

Use STREAM Compliance Manager to help comply with the SPF Mandatory Requirements that Departments and Agencies must :

- ◆ Have a system of assurance of compliance with security policy
- ◆ Comply with oversight arrangements including external audit and compliance
- ◆ Have the ability to regularly audit information assets and IT systems
- ◆ Ensure that main delivery partners are compliant with the framework.

With STREAM Compliance Manager you can:

- ◆ Measure compliance against any control standard or multiple integrated sets of standards, including:
 - ◆ SPF minimum mandatory requirements
 - ◆ GSI Code of Connection
 - ◆ HMG IA Standard No. 6—Protecting Personal Data and Managing Information Risk
 - ◆ ISO 27001, Information Security Management
 - ◆ BS 25999, Business Continuity Management
 - ◆ HMG technical standards
 - ◆ Department's own internal standards.
- ◆ Easily edit or add new control standards
- ◆ Input data input from control self-assessments, audits and / or import from feeder applications
- ◆ Report in real-time on compliance status to management, internal and external auditors with historical trend analysis
- ◆ Record and track improvement actions.

Note: Licenses to use ISO 27001, BS 25999 are included with STREAM. Departments and Agencies are responsible for providing the content, licenses and approval to use HMG and Departmental standards that are not in the public domain.



Users can be allocated permissions to assess the compliance of individual controls or groups of controls, allowing responsibility for assessment to be passed out to control owners.

Control compliance can be linked to performance metrics such that qualitative self-assessments can be verified or modulated by quantitative evidence .

A rich set of real-time graphical compliance reports and charts is available.

Reference	Control	Asset	R	E	D	S	Deployment (%)	Applicable
A.06.3.1 : ENT...	Termination responsibilities	ABC Corporation	50	50	60	30	45	✓
A.06.3.2 : ENT...	Return of assets	ABC Corporation	100	75	60	60	74	✓
A.06.3.3 : AM S...	Removal of access rights	Asset Management System	100	100	100	60	95	✓
A.06.3.3 : FIN S...	Removal of access rights	Finance System	0	50	60	100	55	✓
A.06.3.3 : HR S...	Removal of access rights						59	✓
A.06.3.3 : LEG...	Removal of access rights						61	✓
A.06.3.3 : LIFE...	Removal of access rights						71	✓
A.06.3.3 : P&C...	Removal of access rights						71	✓

Reference	Control	Asset
A.06.3.3 : FIN SYS01	Removal of access rights	Finance System

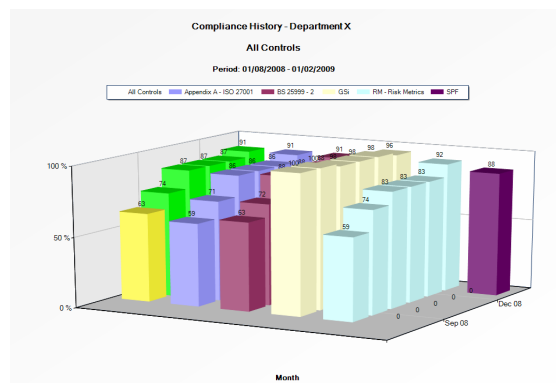
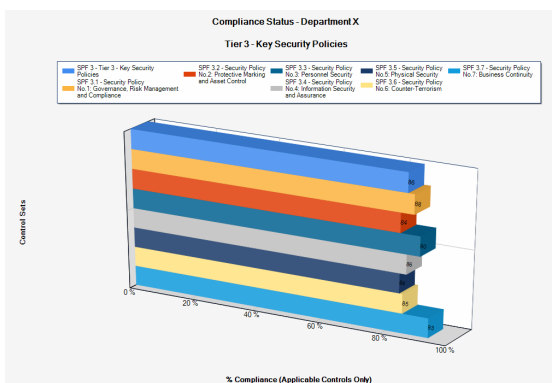
Control Assessment

R: Responsibility: Not Allocated

E: Evidence: Limited

D: Documentation: Published but Out of Date

S: Strength of Impl: Fit for Purpose



STREAM Risk Registers for the SPF

Use STREAM Risk Registers to help comply with the SPF mandatory requirement that Departments and Agencies must adopt a risk managed approach (including a detailed risk register) to cover all areas of protective security across their organisation:

- ◆ Build a hierarchy of risk registers with allocated ownership and responsibility
- ◆ Record and assess all protective security risks
- ◆ Record and assess mitigating controls and actions
- ◆ Monitor residual risk status in relation to risk appetite and see 'at a glance' across the Department where security risks are at an unacceptable level
- ◆ Log incidents, near-misses and actions
- ◆ Report on risk status, mitigating controls, actions and incidents with historical trend-analysis.



Reference	Threat	Asset	Control Deployment %	Number of Controls	Residual Risk (Actual) (£1,000s)	Residual Risk (%Risk Appetite)	Potential Risk (£1,000s)
FR1 : P&C ENT01	Fraudulent Financial Reporting	SD Management Processes	98	3 (3)	52.16	1	16.24
FR2 : P&C ENT01	Inproper or Fraudulent Financial Activity	SD Management Processes	74	6 (6)	251.83	5	7.99
HU1 : P&C ENT01	Human Error	SD Management Processes	75	4 (4)	436.40	9	142.53
HU2 : P&C ENT01	Loss or Unavailability of Key Staff	SD Management Processes	64	2 (2)	281.16	5	36.75
MA1 : P&C SYS01	External Misuse or Abuse	SD System	62	9 (9)	754.16	14	1.25
MA2 : P&C SYS01	Internal Misuse or Abuse	SD System	65	11 (11)	1014.41	18	0.27
MA3 : P&C SYS01	Malicious Software	SD System	79	3 (3)	98.41	2	42.39
PA01 : P&C SITE01	Loss or Unavailability of Premises	SD Premises	63	4 (4)	300.51	5	13.93
SF2 : P&C SYS01	Loss or Unavailability of System	SD System	71	3 (3)	327.81	4	7.38
TP1 : P&C TP01	Insecure 3rd party Relationship	SD IT Service Provider	66	2 (2)	386.19	4	21.49

Local risk registers display the risks for specific business areas, processes, systems or applications'

Local registers can be aggregated to a regional or business area grouping and from there to the Departmental level. All labels and titles are configurable.

The user can drill-down for detailed information.

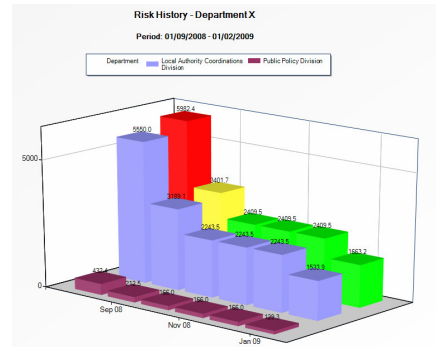
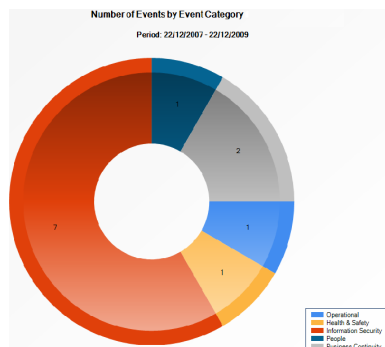
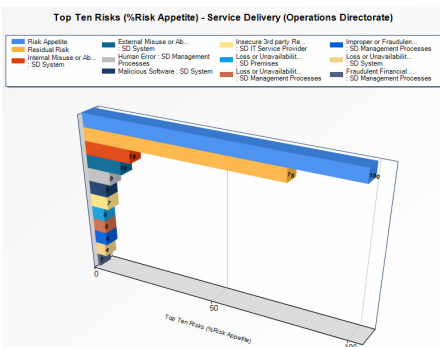
The controls or mitigating actions for a specific risk are displayed.

All registers have a gauge showing the current residual risk (red pointer) and the potential risk (blue pointer) that could be achieved if all controls and mitigating actions were fully implemented and effective.

The user can assess controls and actions, and record owners, target dates and costs.

A rich set of real-time graphical risk reports and charts is available.

Reference	Control	Asset	1	C	2	1	3	A	4	F	Control Deployment %	Applicable
RM02.1	% data backed up securely and tested	SD System	0	0	75	0					72	☑
RM03.3	% team screened prior to access	SD Management Processes	75	75	75	0					77	☑
RM05.1	% components with clearly defined and implemented business access policies	SD System	45	45	45	0					46	☑
RM07.1	% components compliant with baseline configuration	SD System	65	65	65	0					50	☑
RM08.1	% accounts associated with specific users	SD System	35	35	35	0					36	☑
RM08.2	% dormant accounts deactivated	SD System	85	85	85	0					78	☑
RM09.1	% components employing active incident monitoring and reporting	SD System	45	45	45	0					56	☑
RM12.1	% staff (including contractors) that have signed acceptance of security obligations	SD Management Processes	45	45	0	0					79	☑
RM13.1	% audit reviews completed against plan within last 12 months	SD System	25	25	25	0					50	☑
RM15.1	% high risk vulnerabilities remediated within 3 days	SD System	85	85	85	0					76	☑
RM15.3	% components penetration tested within 6 months	SD System	75	75	75	0					54	☑



STREAM Integrated Risk Manager for the SPF

STREAM Integrated Risk Manager provides risk registers, compliance management and metrics management in a single integrated product.

You can measure residual risk status against risk appetite in relation to performance against key protective security metrics and your level of compliance with control standards.

See the STREAM risk gauges move as performance metrics improve (or degrade), as actions to address non-compliances are completed or as audit points are raised, and then dealt with.



STREAM Solutions

STREAM technology is applicable to any business or technical application where management wishes to monitor and manage compliance against control standards, performance against metrics or risk status.



Build your own STREAM solution

Many organisations have existing risk and compliance processes with internal control standards but which are time-consuming or difficult to apply. STREAM has been designed with a fully configurable compliance and risk management meta model which allows easy creation of automated solutions for existing risk processes and any set of control standards. Configurable items include:

- ◆ Business, programme or project hierarchy for aggregation and drill-down
- ◆ Quantitative or qualitative risk assessment for any type or category of risk
- ◆ Units of measurement for impact, risk appetite and residual risk, e.g. £, % service levels, 1 - 10 scale, IS1 scale
- ◆ Criteria such as cost-schedule-quality for project risks, confidentiality-integrity-availability for information risks, strategic-legal-technology-human resources for corporate risks
- ◆ Any internal or publicly available control standards and the criteria by which controls are assessed or performance metrics are monitored
- ◆ Dashboard colour schemes and a tailorable user interface
- ◆ Import and export of data to third party tools

Acuity Risk Management

Acuity Risk Management LLP specialises in the delivery of risk management solutions and services.

Acuity's consultants have implemented risk management processes for hundreds of organisations in every major business sector.

STREAM is the result of this collective experience and the market need for 'easy to use' risk management solutions that provide valuable business information on which key decisions can be made with confidence.

In addition to STREAM, Acuity provides a range of independent consultancy and training services.

For further information on STREAM or Acuity Risk Management please contact us at info@acuityrm.com or visit our website:

www.acuityrm.com

Technology

STREAM is an MS Windows SQL Server 2005 application implemented using the .NET framework and based on a smart client architecture. STREAM is implemented on clients' own networks and within their security domain.

ISO 27001:2005



ACUITY
RISK MANAGEMENT