Incident Management

What is Incident Management?

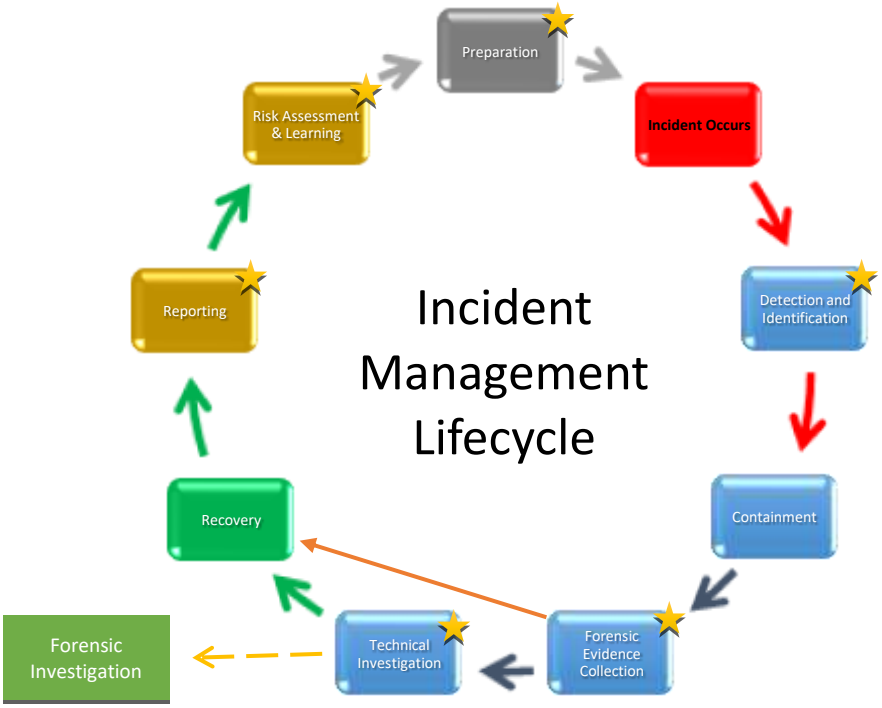
Incident management provides an structured process for handling security incidents. Security incidents are events of sufficient magnitude that need close attention and require effort to resolve. Incident management needs to be factored into a data protection programme because in many instances the confidentiality, integrity or availability of information assets can be at risk. Incident Management provides the process to handle events in a structured and systematic fashion so that information assets are protected from further malicious or inadvertent compromise.

Why is Incident Management needed?

Organisations do implement security controls such as policies, procedures and electronic measures designed to guard against a variety of risks however sometimes the controls fail. Maybe the policy was wrong or the control was incorrectly applied and somehow a security event was triggered. The important outcome is that everyone is safe, the assets affected are restored and the organisation learns how to avoid a repeat of the event in the future.

How is Incident Management supported?

The GRC-ISMS Incident Management module enables Incidents to be managed and tracked as they pass through the Incident Management Lifecycle. Staff can create and manage polices, plans and procedures. Users can report events which are then scrutinised. The system records details of the Incident team and using workflow, notifies relevant members of staff throughout the cycle. The GRC-ISMS directly links via API with several security systems including Data Classification, Privilege management, vulnerability scanning and others.



How GRC-ISMS assists Incident Management

Preparation

The integrated ISMS stores key documents. The Asset Register holds details of information assets. Together these enable the organisation to prepare how they will respond to incidents

Detection & Investigation

GRC-ISMS supports integration with several 3rd Party security tools. Using the inbuilt dashboard visualisations, the incident response team has greater insight to security events.

Forensic Evidence Collection & Technical Investigation

GRC-ISMS Incident Reporting module provides the facility to record key information relating to a security incident. The reports are available to the Incident Team on a controlled basis and track the 'incident life cycle' from detection through to resolution. The GRC-ISMS incident logs are forensically sound and tamper proof.

Reporting & Learning

The GRC-ISMS reporting engine provides extensive incident response reporting. Details of specific incidents can be displayed or made available for printing. Several Dashboards are provided that aggregate data over time. All 'lessons learned' are identified and recorded. The 'Staff Briefings' module is available to help boost awareness once the incident has been resolved.

DLP Assured Services Ltd | Suite B| 29 Harley Street| London| WIG 9QR
E info@dlp-assured .co.uk **T** 0203 397 1090 **W** www.grc-isms.com

What is the GRC-ISMS?

The GRC-ISMS is a cloud based Governance, Risk and Compliance system that is designed to help staff engage with an organisation's information governance programme. The system provides a range of services to automate and simplify governance tasks such as Incident Management.

The GRC-ISMS is a *integrated GRC* as it links to other security products (via API's) so that information can be easily and securely transferred to provide management insight into the organisations overall security posture. This helps overcome the problem of isolated information security silos.

The GRC-ISMS is self-service, meaning staff are encouraged to enter and maintain the information pertinent to themselves. This lessens the burden on key governance staff. The system has extensive reporting and alerting facilities designed to help people 'manage by exception'.

The GRC-ISMS is designed to report on governance by presenting a visual dashboard featuring, real-time displays of pertinent information to relevant staff, to help support better decision making.

At the heart of the GRC-ISMS is the asset register. This facilitates the creation of a record of all assets, which can then be stored and risk assessed. Assets can be anything of value but would typically include Infrastructure assets containing personal information such as databases, and files stores. The assets will also include staff, together with supply organisations etc. The objective is to create records so that the risks to the organisation can be identified and managed more effectively.

The GRC-ISMS consists of a number of integrated modules (see side panel).
Each module can be turned on or off depending upon client's needs. Access is strictly controlled with extensive role based rights management to ensure only authorised personnel have access to the relevant service.

Examples of system dashboards

Main Dashboard

Risk Dashboard

GRC-Modules

- **IG Management**
- ✓ Asset Management
- ✓ Audit engine
- ✓ Authorisation Management
- ✓ Business Continuity
- ✓ Change Management
- ✓ Data Sharing Management
- ✓ FOI Management
- ✓ HR Staff Record Management
- ✓ Incident Reporting & Tracking
- ✓ Joiners Induction Management
- ✓ Learning Management System (LMS)
- ✓ ISMS - Policies, Procedures Display & Management
- ✓ Project & Process workflow
- ✓ Reporting engine
- ✓ Risk Assessment
- ✓ Risk Register
- ✓ SAR Management
- ✓ Service Catalogue
- ✓ Staff Briefing Updates
- ✓ Staff Management
  - ✓ Induction Management
  - ✓ Staff Change Management
  - ✓ Leavers Management
- ✓ Supplier Management
- ✓ Training Record Management
- **Cyber Security**
- ✓ Automatic device discovery
- ✓ Boundary Firewall Testing
- ✓ Data Classification integration
- ✓ Privilege Management integration
- ✓ Secure Configuration Testing
- ✓ Server vulnerability scanning integration
- **End User Dashboard**
- ✓ Incident Reporter
- ✓ My Assets
- ✓ My Details
- ✓ My Induction
- ✓ My Policies, Procedures & Guidelines
- ✓ My transfers of personal information
- ✓ Out of Office Reporter
- ✓ SAR reporter
- **System**
- ✓ Confidentiality Monitoring
- ✓ Dashboards
- ✓ Extensive Audit logging
- ✓ Integration with 3rd party systems via API
- ✓ Modular system
- ✓ Reporting Module
- ✓ Rights Based Management
- ✓ Self-Service
- ✓ Cloud based

www.grc-isms.com

DLP Assured Services Ltd | Suite B| 29 Harley Street| London| WIG 9QR
E info@dlp-assured .co.uk **T** 0203 397 1090 **W** www.grc-isms.com