Romano Security Consulting Limited

Cyber Incident Management and Incident Response Consultancy Service Description

G Cloud 15

© Romano Security Consulting Ltd

Incident Management - Prepare, Respond and Follow Up

Organisations are never going to eliminate the inevitable happening but can prepare an effective response and do all that they can to minimise the impact when it does happen.

Incident response and incident management is now a major factor in regulatory compliance, GDPR, NIS Directive, NHS (DSP) Data Security and Protection Toolkit, CareCERT and the Scottish Cyber Resilience Strategy for Scotland all have mandatory incident reporting requirements and associated fines if breaches are not reporting within certain timeframes.

An organisation's ability to detect, react to and respond to security incidents in a fast, planned and coordinated fashion is of paramount importance to the operation, cyber resilience and continued success of an organisation.

The purpose of incident response is to manage and respond to unexpected, disruptive events with the objective of controlling impacts within acceptable levels. The objective of incident response is to suitably prepare for the cyber-attacks that organisations are likely to face.

Incidents can be technical, such as attacks mounted on the network via viruses, denial of service (DoS), system intrusion or they can be the result of mistakes, human error, system or process failure.

While it is important for organisations to have preventive measures in place to avoid security incidents, it is equally important that there is a robust, tried and tested response plan in place should an incident occur.

Romano Security Consulting Cyber Incident Management Consultancy

Romano Security Consulting delivers cyber incident management consultancy services to help organisations prepare for and respond effectively to cyber security incidents and data breaches. We support businesses through planning, preparation, and response readiness to enable a timely and controlled incident response process.

© Romano Security Consulting Ltd

Romano Security Consulting Cyber Incident Management Consultancy

Romano Security Consulting advocate the implementation of an incident management framework based on ISO 27035 and the CREST (CSIR) guidelines utilising the 3 phase Prepare, Respond and Follow Up approach.

Defend, protect and prepare for cyber incidents and data breaches with our Incident Response Planning and Management Solutions based on the CREST guidelines and ISO 27035. Let us help you Plan for and Prepare for and be ready to Respond to a cyber incident or data breach quickly.

If you are looking to implement an incident management and incident response solution then we can help develop a bespoke solution for you utilising the following milestones:

- Review your current status, perform a gap analysis and recommend suitable controls and appropriate technical measures
- Assist in asset discovery
- Conduct a Business Impact Analysis (BIA)
- Advise on the development of a suitable incident response process
- Develop an incident response team
- Develop a bespoke incident response plan
- Provide incident response training
- Develop bespoke incident scenarios
- Assist and advise on scenario testing
- Advise on a suitable framework for continual improvement and ongoing management

Contact Romano Security Consulting

For further details or a quote please contact us on the details below:

Phone: 01625 315021
Email: enquiries@romanosecurityconsulting.com
Web: romanosecurityconsulting.com

© Romano Security Consulting Ltd