VOX
EXCEL CYBER
PART OF THE DVGA GROUP

Insider Risk Management

Datasheet

An insider risk management program is a set of policies and procedures designed to identify, assess, and mitigate the risk of malicious or accidental actions by individuals with authorised access to an organisation's sensitive information or systems.

Our team will provide guidance on the implementation of policies and a multi-channel risk-based approach to user awareness and behavioural monitoring. The program typically includes employee training, monitoring of employee activity, and incident response plans. The goal is to protect the organisation's assets and reputation from harm caused by malicious or inadvertent human actions.

Our value proposition

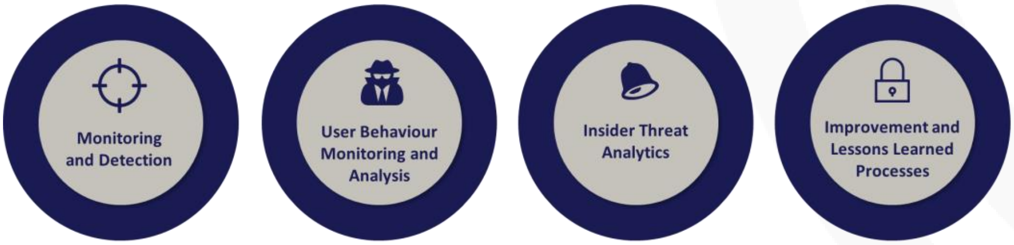
Security awareness maturity review & roadmap

We assess your organisation's security culture and awareness maturity to develop an effective security awareness roadmap that helps achieve your awareness goals.

Insider risk maturity assessment

We conduct a thorough analysis of threats, organisational context, and the maturity of current countermeasures to pinpoint any gaps that may leave your organisation exposed to insider risks. We identify and assist with defining special controls for High-Risk Users (HRUs).

Outthink: Reshaping Cybersecurity through Human Risk Intelligence


Monitoring and Detection
User Behaviour Monitoring and Analysis
Insider Threat Analytics
Improvement and Lessons Learned Processes

To analyse user behaviour patterns and identify anomalies that may indicate insider threats. These tools can detect deviations from normal behaviour.

To continuously monitor and analyse data to establish baseline behaviour for individual users and identify any deviations or suspicious activities.

To leverage advanced analytics to detect and correlate multiple indicators of insider threats. By combining data from various sources, they can identify patterns and behaviours that may suggest malicious insider activity.

To provide valuable insights into user behaviour and insider threat patterns. The data and analytics generated by these tools can contribute to continuous improvement efforts, allowing organizations to refine their insider risk programs.

Highlights

Insider threats have the potential to cause significant harm to an organisation. Malicious insiders can intentionally sabotage systems, steal valuable data, commit fraud, or engage in espionage activities. Unintentional incidents, such as accidental data leaks or human errors, can also result in serious consequences. By addressing insider risk, organisations can mitigate the potential financial, operational, and reputational damage caused by these threats.

Key features

Improved regulatory compliance
Many industries and jurisdictions have specific regulatory requirements regarding data protection, privacy, and information security. Organisations that fail to manage insider risk effectively may face legal repercussions, penalties, or reputational damage due to non-compliance.

Secure work environment
Managing insider risk helps foster a culture of security awareness and accountability among employees, encouraging them to adhere to policies and best practices. This, in turn, reduces the likelihood of insider incidents and enhances overall organisational resilience.

Long-term sustainability, trustworthiness, and success
By proactively addressing potential threats and vulnerabilities posed by insiders, organisations can protect their assets, maintain regulatory compliance, preserve their reputation, and safeguard sensitive information.

Our value proposition

Insider risk program design & implementation

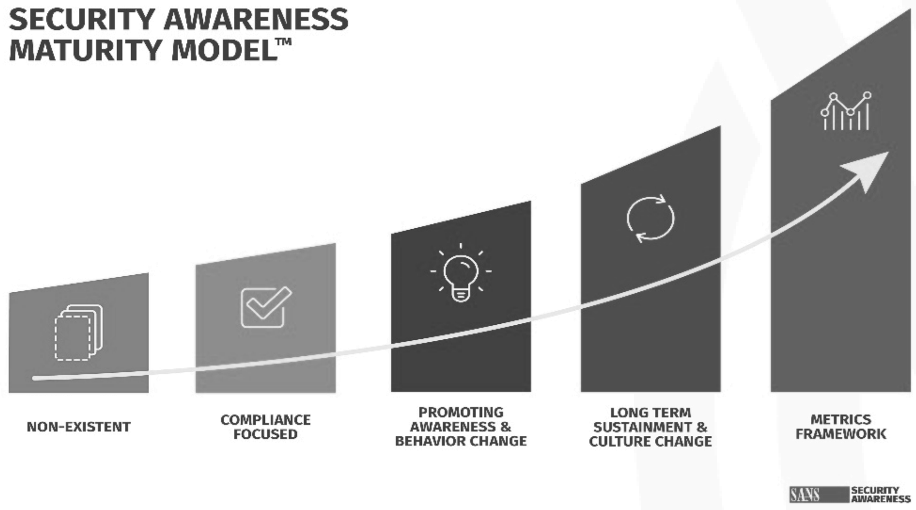
We capture insights from your organisation’s unique culture and business structure and shape an initial program strategy and roadmap. We refine the strategy through a stakeholder validation process and conduct a pilot. We setup the program and transfer it to the business insider risk/security team once fully operational and staff trained.

Hack the human – social engineering tests

We provide a range of tailored testing techniques to conduct both physical and digital tests such as phishing, tailgating, to test the organisations social cyber strength. We benchmark user awareness and measure ongoing progress of your awareness program.

Security awareness-as-a-service

We deliver training and awareness content leveraging on ATL and BTL marketing techniques. We incorporate research and metrics in our approach to deliver measurable programs that ensure maximum coverage and behavioural change. We provide leading security awareness tools that assist with achieving measurable results for any sized organisation.


SECURITY AWARENESS MATURITY MODEL™
NON-EXISTENT
COMPLIANCE FOCUSED
PROMOTING AWARENESS & BEHAVIOR CHANGE
LONG TERM SUSTAINMENT & CULTURE CHANGE
METRICS FRAMEWORK
SANS SECURITY AWARENESS

Key benefits

Increased visibility
Help identify weaknesses in user security awareness or issues in behaviour.

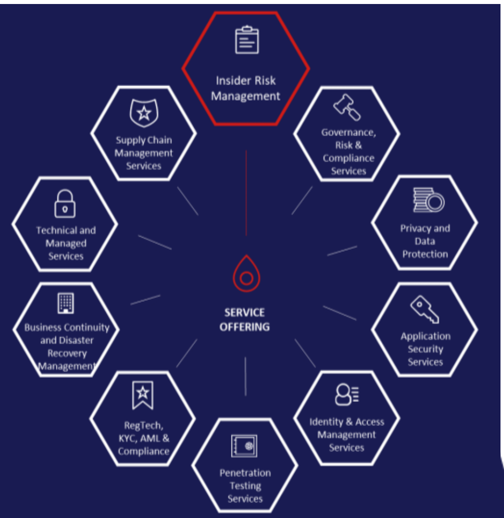
Enhanced monitoring
Help detect anomalous user activities before an incident occurs.

Improved security controls
Train and enable users to be your last line of defence and enabler for adhering to strong authentication processes, better access control, and improved data protection measures.

Faster incident response
Improved user cooperation with incident detection, investigation, and response processes.

Improved employee engagement
Build trust and engagement with employees through security awareness and training.

Better risk management
Identify potential threats and vulnerabilities, assessing the impact of incidents, and developing mitigation strategies.


Insider Risk Management
Governance, Risk & Compliance Services
Privacy and Data Protection
Application Security Services
Identity & Access Management Services
Penetration Testing Services
RegTech, KYC, AML & Compliance
Business Continuity and Disaster Recovery Management
Technical and Managed Services
Supply Chain Management Services
SERVICE OFFERING

ABOUT US

Founded in 2015, VoxExcel Cyber is a leading consulting led cyber security company focused on providing best-in-class, strategic advisory services and innovative technology solutions. We specialise in assisting C-level executives in navigating the complexity of security governance, risk management and regulatory compliance requirements, while bridging the gap between management objectives and the requirements of technical teams.

Our team of consultants and engineers are focused problem solvers with deep technical knowledge and broad industry experience, across many and industry sectors including banking, financial services, retail, airline, government, telco, oil and gas, mining and manufacturing.

Acquired by DVGA in 2022, the company also provides data privacy, supply chain audit, and ISO implementation software solutions, to many major clients. The company operates across Europe, USA, Africa and Middle East.