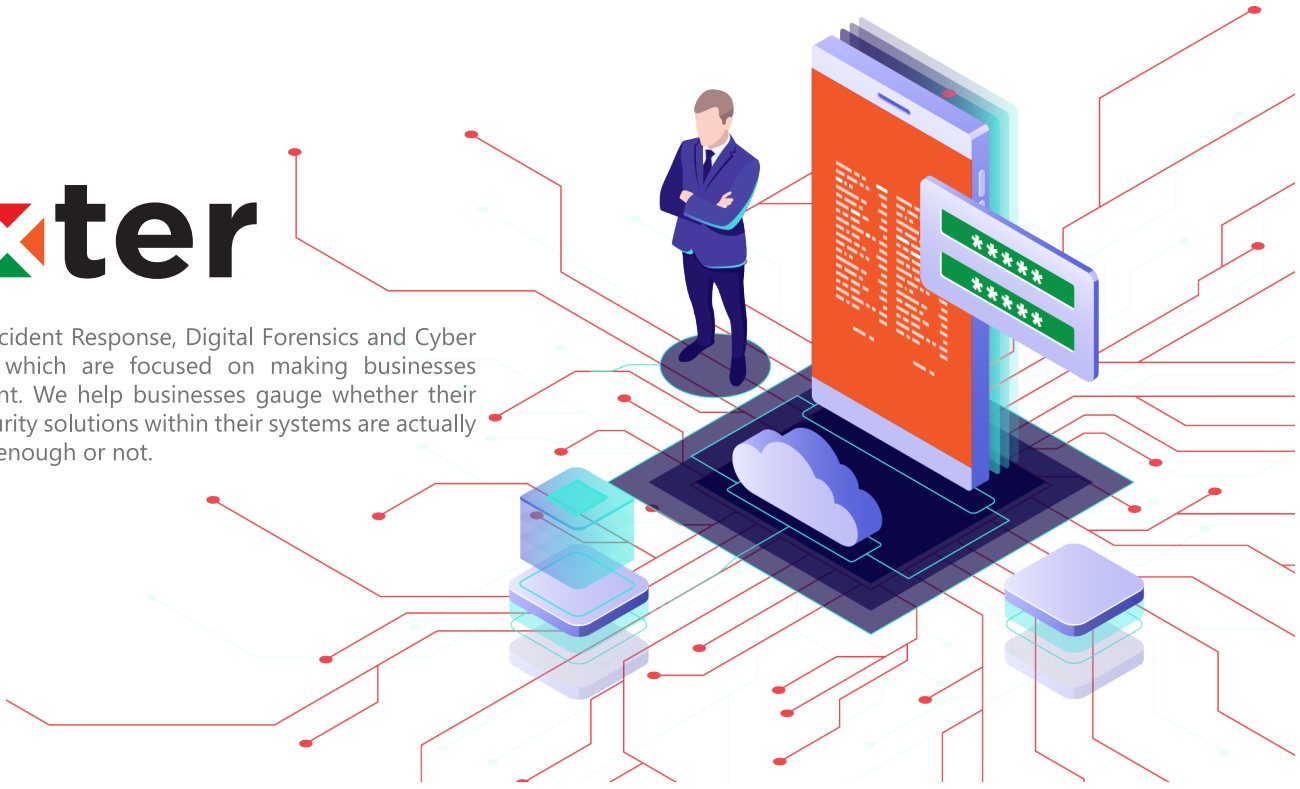
trixter

We specialize in Incident Response, Digital Forensics and Cyber Risk Assessments which are focused on making businesses resilient and vigilant. We help businesses gauge whether their investments in security solutions within their systems are actually robust and secure enough or not.



Cyber Risk Mitigation

Cyber Risk Mitigation involves identifying your risks and vulnerabilities and applying administrative actions and comprehensive solutions to make sure your organization is adequately protected.

Information security **risk management to evaluate** and document current controls.

Security **maturity assessment** to benchmark controls against leading practices and industry standards.

Policy assessment and development to determine the effectiveness of current policies and align new policies with business goals.

Governance, risk and compliance (GRC) consulting and implementation services to automate the management of enterprise GRC programs.

Custom risk mitigation consulting to assess policies, procedures and human involvement and complex risk management systems.

Cyber Fraud Investigation

Cyber Fraud Investigation involves identifying the source of the incident, remediating the damage caused by the incident and evaluating how to best safeguard your system from future attacks.

Prepare to prevent
Internal and external assessments to evaluate clients' systems, applications, and facilities.

Investigate & Identify
Identify vulnerabilities, intrusions and data ex-filtrations and provide recommended solutions.

Incident Response
Devising a systematic response plan to minimize the repercussions from a confirmed attack.

Proactive Monitoring
Analyzing unique personal data points to proactively search for unique personal data including government, insurance and online identifiers – a complete digital footprint.

Regular Assessments
Standards-based assessments (ISO, NIST, HIPAA, etc.) and policy and procedure review and design to identify gaps of any kind.

Cyber Risk Assessment

Cyber Risk Assessment is the next level evolution in enterprise technology risk and security of organizations that increasingly rely on digital processes to run their business.

Cost-effective risk management
The program needs to meet the definition of risk management listed above.

Well-informed decisions
Every decision involves a choice, and in order for those need to be well-informed in time.

Effective comparisons
A decision-maker should be able to compare the options before him/her to make the most effective decision.

Meaningful measurements
Well defined security metrics that help the decision makers drive and make business decisions.

Accurate models
Present/Prepare/Execute accurate models of risk and of explicit risk management that can scale in real-life.

Cyber Incident Response

Cyber Incident Response is a methodology an organization uses to respond to and manage a cyber attack. An efficient incident response plan (IPR) aims to reduce this damage of an attack and recover as quickly as possible

Investigation to crisis management
Carry out Thorough technical investigation, containment and recovery coupled with crisis and communications management to handle internal politics, brand protection and legal liability.

Leverage Threat Intelligence
Understand who is on your network and why, to improve your response to current and future attacks.

Remediation planning and execution
Accelerate recovery time and begin remediation immediately with a well-constructed plan to spend less time planning and more time in executing.

Compromise Assessment
Examine your computing environment for malicious activity to uncover attack history and breach exposure, enabling you to identify or confirm compromised data and initiate proper response.

Tabletop Exercises
Incident scenarios viz. system compromise, unauthorized access of PII, policy violations, inappropriate emails are simulated to evaluate your organization's response processes from detection to closure.

info@trixter.in

trixter.in

CYBER READINESS FRAMEWORK (CRF)

Managing cyber risk to grow and protect business value

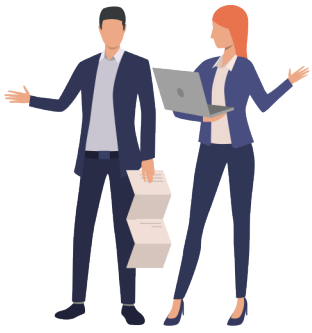
Trixer's CRF is a business-driven, threat-based approach to conduct cyber assessments based on an organization's specific business, threats, and capabilities. CRF incorporates a proven methodology to assess an organization's cyber resilience; content packs that enable us to conduct assessments against specific standards; and an intuitive online platform incorporating a range of dashboards that can be customized for an executive, managerial, and operational audience.

Three fundamental drivers that drive growth and create cyber risks

- Innovation
- Information Sharing
- Trusting People

CEO
I read about phishing in the news. Are we exposed

CIO
Where and how much do I need to invest to optimize my cyber capabilities



Board
What is our level of resilience against these cyberattacks

Organizations need a holistic, business-driven, and threat-based approach to manage cyber risks. While securing assets is important, being vigilant, and resilient in the face of cyberattacks is imperative.

Business risks

- What is my risk appetite
- What is my business strategy
- What are my crown jewels

Threat landscape

- What are they interested in
- What tactics Secure might they use
- Who are my adversaries

Cyber capabilities

Governance
Identify top risks, align investments develop an executive-led cyber risk program

Secure
Take a measured, risk-prioritized approach to defend against known and emerging threats

Vigilant
Develop situational awareness and threat intelligence to identify harmful behavior

Resilient
Have the ability to recover from and minimize the impact of cyber incidents

A strong cyber risk program helps drive growth, protects value, and helps executives to be on top of cyberthreats

- Understand the business context and objectives
- Understand my threat landscape
- Understand current maturity level of cyber capabilities
- Focus on the right priorities
- Define target maturity level of cyber capabilities & recommendations
- Develop cyber strategy roadmap
- Enhance value from cyber security investments
- Communicate with internal and external stakeholders

info@trixter.in

CYBER INCIDENT RESPONSE
& CYBER FRAUD INVESTIGATIONS

CHALLENGES

- Cyberthreats are constantly evolving and increasing in volume, intensity, and complexity making it a major focus point for management and the board
- Hackers and malicious actors are more likely to penetrate an organization due to lack of security controls or misconfigurations
- When a breach happens, businesses must respond quickly and effectively to close and remediate the breach vector

OUR SOLUTIONS

- We provide businesses / organizations with a set of operational and strategic incident response and forensic capabilities in a single comprehensive service, from preparation to monitoring, detection to response
- We help organizations improve their incident response capabilities, establishing readiness through effective simulations, training and assessments
- We provide 24/7 support for a cyber incident that have an impact on the strategic objectives, revenue, reputation, or viability of the business

Cyber Forensic Investigation
Assist | Investigate | Manage

Investigates cybercrimes to determine the nature, extent, means, and origin of an incident. This investigation report helps an organization to take appropriate legal action against the intruder.

Table-Top Exercise
Conduct

Assist and guide teams in evaluating incident response plans and processes, and rehearse their roles and responsibilities. The exercise often focuses on polishing specific skills (such as logging, conducting risk assessments, and run through the decision-making processes) and identify opportunities to improve the prevention of, response to, and recovery from a cyber incident.

Cyber Incident Response
Assist | Respond | Manage

Make available our Incident Response team 24/7 as crisis has no fix time, support and assist clients to respond effectively to a cyber incident. Trixter's team of Incident Response specialists have experience in dealing with a variety of threats and incident types.

Cyber Resilience and Recovery
Assist | Implement

Help implement contingency plans and assist the business in recovering operations to a normal state post cyberattack or an incident

Cyber Workshop and Training
Conduct

The aim is to spread awareness that supports the development of incident management and response plans, guidelines, roles and responsibilities. Our workshops are focused on detailed discussions which involve pre-incident scenarios, evaluation of current processes and tools, validating response and post response steps

trixter

info@trixter.in

trixter.in

CYBER RISK MITIGATION
& CYBER RISK ASSESSMENT

CHALLENGES

Threat vectors are evolving on a daily basis and are increasing in terms of volume, intensity, and complexity

Carrying out intermittent health-checks is not enough. More steps to be followed to check for any loop-holes that may lead to a breach

OUR SOLUTIONS

We help businesses assess and prepare their IT infrastructure, tools, and third-parties by combining traditional technical security reviews along with advanced services in which we adopt a similar approach to that of an attacker

Our services allow organizations to discover and improve/neutralize any detection or response-mechanisms already in place, augment these where necessary, and most importantly, ensure all systems work together faultlessly

Threat Readiness Advisory & Remediation
Assist | Implement | Manage

Helps businesses deal with advanced threats ensuring maximum ROI on existing detection technologies by improving system interactions, fixing misconfigurations , applying realistic use cases, and staff training.

Cyber Compromise Assessment
Advise | Manage

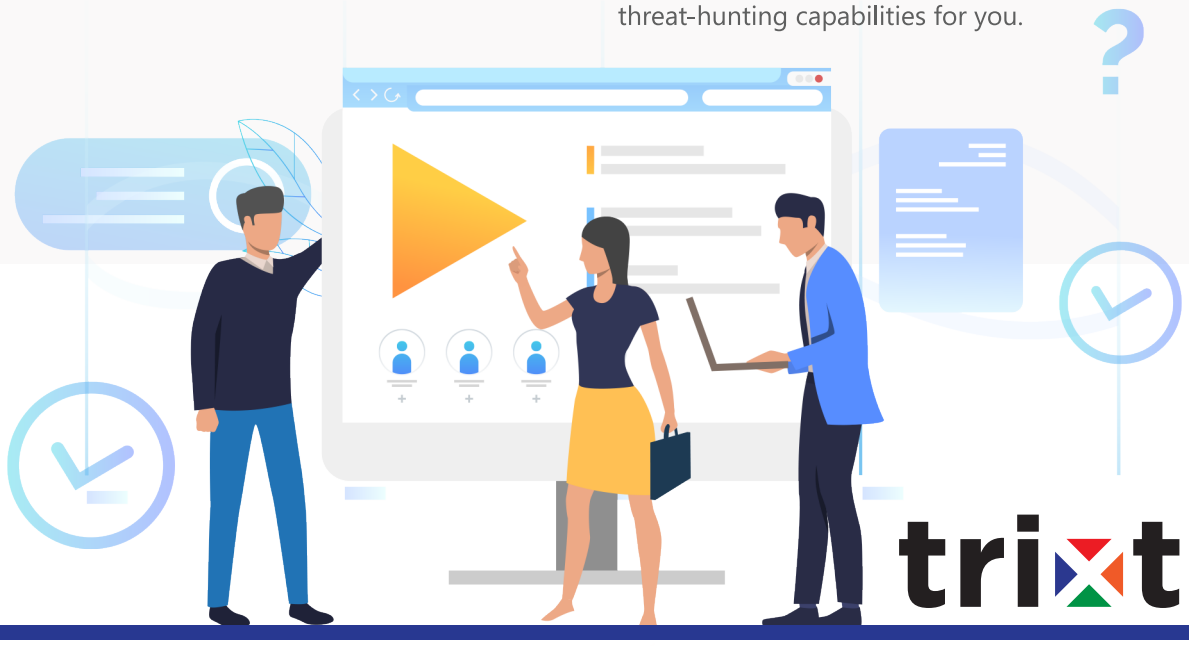
Examines business's network and infrastructure to identify potential/potentially compromised devices by monitoring for malicious network traffic and suspicious network activity.

Endpoint Protection
Implement | Manage

Enables businesses to continuously monitor, protect and remediate threats in real-time. Either through monitoring and correlation of events, log collection with Trixter's Managed Security Services (MSS) platforms deployed on-site where we manage all events 24/7.

24/7 Security threat monitoring
Advise | Implement | Manage

Offers a flexible and easily scalable managed security operations centre in which a team of certified responders work 24/7 to detect malicious activities. Trixter's professionals operate and manage security information and event management (SIEM) platforms allowing threat-hunting capabilities for you.



trixter

info@trixter.in

trixter.in