RISK IMPERIUM CONSULTING (RIC)

"Secure for Success"

Adversaries attack the weakest link…where is yours?

OUR PRODUCTS & SERVICES

- ENDPOINTLOCK KEYSTROKE ENCRYPTION
- INSIDER THREAT PROTECTION PLATFORM
- INFORMATION SECURITY PROGRAM/ FRAMEWORK
- RISK MANAGEMENT SERVICES
- POLICIES, STANDARDS & PROCEDURES
- INFORMATION SECURITY ARCHITECTURE
- CERTIFICATION & ACCREDITATION
- GAP ANALYSIS
- AUDIT
- COMPLIANCE SOLUTIONS
- CLOUD SECURITY
- PHYSICAL SECURITY
- BUSINESS CONTINUITY
- THIRD PARTY RISK MANAGEMENT
- CYBER READINESS
- PROJECT & PORTFOLIO MANAGEMENT

Our Vision

Be a trusted partner that supports delivery of your organizational strategy by identifying and managing risks to information confidentiality, integrity and availability

About Us

Risk Imperium Consulting (RIC) is an Information Security and Risk Management consultancy based in UK & Uganda, but provides products & services globally. Our services range from information security and risk management framework design, implementation and validation to audit and compliance monitoring. We deliver EndpointLock Secure Keyboard—the ONLY SOLUTION to stop zero-day keylogging spyware installed on a device and insider threat protection platform.

The Team

Risk Imperium comprises of a team of CISA, CRISC, CISM, CISSP, CGEIT, CEH, MCSE, MSc. qualified and highly experienced IT Risk and Information Security consultants, with expertise and knowledge of regulatory requirements, information security frameworks, international industry standards, IT governance, risk management and cyber security awareness and training.

Why Risk Imperium?

Risk Imperium's consultants have extensive experience in implementing information security solutions and frameworks, development of IT & Cybersecurity Policies, Standards and Procedures, performing risk assessments, deep dives or audits and would work with you to support the delivery of your company strategy that is resilient to the evolving threat landscape. Risk Imperium's objective is to save your organization money first by analyzing your needs accurately and second by lowering your risk. Risk Imperium consultants would deliver the advanced cyber security solution; EndpointLock Keystroke Encryption for your endpoints and mobile devices; define and implement basic strategies to strengthen your security posture and ingrain security into your organization's culture; prepare your business for timely uncovering of threats, identifying and addressing risk, & and complying with industry & regulatory requirements

Mitigating your company's IT Risk

IT Governance, Risk Management & Compliance

Governance, Risk and Compliance (GRC) efforts are too often disconnected and inconsistent. All organisations have people and functions in place to practice governance, manage risk, and meet compliance requirements to some degree, however, as most of these efforts are developed over time in distinct areas of the organization, they fail to realize benefits of coordination, including better efficiency and improved insight.

The span of a Governance, Risk and Compliance process includes three elements:

- Governance as the oversight role and the process by which companies manage and mitigate business risks.
- Risk management, which enables an organisation to evaluate all relevant business and regulatory risks, and controls as well as monitor mitigation actions in a structured manner.
- Compliance as it ensures that an organisation has the processes and internal controls to meet the requirements imposed by governmental bodies, regulators, industry mandates or internal policies.

In essence, Risk Imperium will ensure that IT governance provides a structure for aligning IT strategy with business strategy for your organization. By following a formal framework, your organisation can produce measurable results towards achieving your strategies and goals. Risk Imperium takes you through a formal program that takes stakeholders' interests into account, as well as the needs of staff and the processes they follow. Largely, IT governance is an integral part of the overall organisation's governance.

IT governance and GRC are essentially the same thing. While GRC is the parent program, what determines which framework is used is often the placement of the Chief Information Security Officer (CISO) and the scope of the security program.

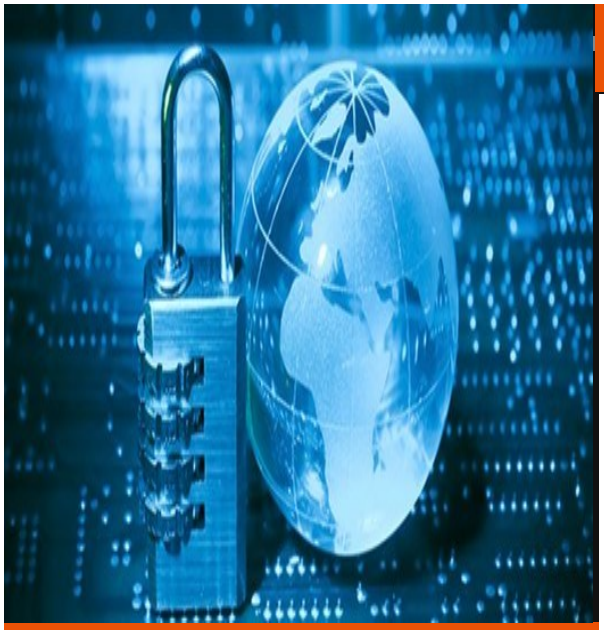
Why IT governance for your organisation?

Organisations today are subject to many regulations governing the protection of confidential information, financial accountability, data retention and disaster recovery, among others. They are also under pressure from shareholders, stakeholders and customers to protect their critical assets; information and guarantee it's confidentiality, integrity and availability.

To ensure your organisation meets internal and external requirements, Risk Imperium supports you with the implementation of a formal IT governance program that provides a framework of best practices and controls. This applies to both public and private sector organisations regardless of business size.

Risk Imperium works with you to phase in an IT governance program with minimal '*speedbumps*' through management services to focus on managing the IT security program and the risk within the organization; operational services to focus on controls implemented and executed by people (as opposed to systems) and technical services to focus on security controls a computer system executes.

SECURELY CONNECTING YOUR BUSINESS TO TECHNOLOGY RESOURCES



SECURELY CONNECTING YOUR BUSINESS TO TECHNOLOGY RESOURCES

Information Security & Risk Management

IT Security Program Services

A comprehensive IT security program service can consist of many elements to identify assets & associated risks, protect the assets, detect issues/anomalies, respond to and recover from incidents based on the specific needs of your organization and the relative maturity of its IT security program.

Risk Imperium can assist your organization's decision makers in achieving the following:

- Develop and Maintain an organization-wide security program, helping to ensure effective implementation of the program
- Evaluate the performance of major organization components, and provide appropriate security training of your employees with significant security responsibilities.
- Perform independent evaluations and audits of your IT security program or components of the program.

Specifically, Risk Imperium will ensure the following elements are completed as part of your organization's IT security program:

- Assess the risk to operations and assets under the organization's control
- Determine the level of security appropriate to protect the organization's operations and assets
- Develop and maintain a current security plan for each system supporting the operations and assets under organizational control
- Develop security incident handling procedures
- Develop processes for sharing information regarding common vulnerabilities, including a description of procedures for external reporting
- Develop a set of effective security controls and techniques
- Develop capital planning and investment control processes that ensure appropriate integration of security controls into IT investments
- Develop a set of IT security metrics that enable an organization to effectively assess the adequacy of in-place security controls, policies, and procedures and to adequately justify security control investments

Information Security & Risk Management

Risk Management Services

Risk Imperium's primary goal is to assist organizations balance the operational and economic costs of protective measures and achieve gains in mission capability by protecting their IT systems and data. Risk management enables an organisation to evaluate all relevant business and regulatory risks, and controls as well as monitor mitigation actions in a structured manner. Risk Imperium offers various combinations of service packages for supporting risk management activities. We develop risk management guidance for supporting your risk management program. Risk Imperium can manage the risk management program as a whole for your organization or simply provide advisory services depending on the level of maturity of the program. Risk Imperium can also perform risk assessments and/or develop risk mitigation plans for your organization. If your organization already has a mature and operational risk management program, Risk Imperium can audit the program for effectiveness.

SECURELY CONNECTING YOUR BUSINESS TO TECHNOLOGY RESOURCES

IT Security Policy Services

Risk Imperium can assist your organization in analyzing existing and developing new security policies, standards, guidelines, and procedures. The authority for approving policy is inherently a core function of your organization and therefore final approval of policies will be performed by your organization. A comprehensive IT security policy service can consist of many elements that will depend on the specific needs of your organization and the relative maturity of its IT security program.

Information Security Architecture

Risk Imperium can help your organization to design a new security architecture in line with the technology and security baseline of your organization's current architecture. We can conduct baselining to identify your organization's business needs, functional requirements, security requirements, and risk assessments, as well as the security controls in place if this has not already been done by your organization. Risk Imperium can identify security controls and identify and assess technologies that will enforce the organization's security policies. We can also develop a methodology for selecting the security solutions that best serve your organization's needs, design a technical architecture and document the security architecture for your organization.

Information Security & Risk Management

Certification and Accreditation

Risk Imperium recommends ISO 27001 certification for your organization as the way in which you look after and use corporate information can mean the difference between success and failure for your business. By becoming ISO 27001 certified your organization will be showing a commitment to ensuring that adequate security controls are in place to protect information and data from being accessed, corrupted, lost or stolen. Risk Imperium can help your organization to prepare for the certification and accreditation. ISO 27001 certification demonstrates your compliance with internationally recognised standards of information security. If your organizations meets the requirements it may be certified by an accredited certification body following successful completion of an audit.

Gap Analysis

Risk Imperium can conduct an information security gap analysis for your organization to provide a comparison of your security program versus overall best security practices. By comparing these best practices to actual practices, we can shed light on areas where vulnerabilities and risks are lurking.

However, it's not only important that a gap analysis be conducted; it's also important that it is done correctly. Risk Imperium will ensure that the critical steps below are correctly followed to achieve this.

- Step 1: Select an industry standard security framework
- Step 2: Evaluate People and Processes.
- Step 3: Data Gathering/Technology
- Step 4: Analysis

Audit

The role of IT audit is to provide independent assurance that an organisation's risk management, governance and internal control processes are operating effectively.

Risk Imperium can comprehensively audit your applications and Infrastructure with focus on your organisation's people, processes and technology to identify gaps and provide remediation recommendations.

A successful audit for the key domains of your organisation can add value and improve your organisation's operations, as well as provide insight based on respective analyses and assessments.

SECURELY CONNECTING YOUR BUSINESS TO TECHNOLOGY RESOURCES

Compliance

Across the different sectors, organisations have a legal requiement to adhere to regulatory requirements. Compliance management is of significant importance in any industry. However, the importance of compliance in the banking industry is even more than in other industries — the below reasons highlight why compliance is integral to the banking industry:

- After the 2008 financial crisis, banks have faced an increase in the level of scrutiny from the governments. The governments requires innumerable statutory and regulatory compliance. Hence, every organization requires a compliance management system to ensure the bank is updated about the requirements and complies with it.

- Regulators aren't just more aggressively pursuing institutions who break the law. Lawmakers are imposing higher penalties on lawbreakers. Compliance has become a pivotal issue for banks because failing due diligence on customers and transactions leaves a company open to scrutiny and litigation

- If banks face legal action for non-compliance the consequences could be catastrophic-ranging from fines, temporary suspension to permanent closure.

- Non-compliance with regulations will have a significant impact on the brand reputation of the bank. For financial institutions, customers are more sensitive to brand reputation and non-compliance would lead to a significant decrease in customers.

Banking compliance and risk has therefore become one of the most significant concerns for financial institution executives. New laws and regulations continue to emerge, such as conduct-risk, next-generation Bank Secrecy Act and Anti-Money Laundering (BSA/AML) risk, risk culture, and third & fourth-party (subcontractors) risk, etc. All banks differ in the way they operate, but one thing they have in common is compliance. So how does Risk Imperium Consulting support organisations in meeting and maintaining their compliance obligations?

As a security-minded organisation, you've likely built a series of defences on your networks, endpoints, and applications, and in the cloud, hoping multiple layers will keep you safe from cyber-attacks. While a layered defence is critical to a sound security strategy, you need context from coordinating across all your layers of defence with the right people, processes, and technology working together in concert. That's how Risk Imperium can help:

- Implement a robust compliance mechanism to monitor the bank's and client's activities and determine whether the banks are compliant with all the required statutory and regulatory requirements; communicate changes in rules or guidelines issued by regulators to all departments

- Integrate Compliance and IT training to create awareness and enhance understanding of the controls required to achieve compliance, how they are operationalised and measured for effectiveness within the banks.

RISK IMPERIUM LEVERAGES THE DEFENCE IN DEPTH SECURITY CONTROLS, RISK MANAGEGEMENT SOLUTIONS & TRAINING TO SUPPORT ORGANISATIONS IN THEIR COMPLIANCE JOURNEY.

Cloud Security

As organisations adopt cloud technology to improve speed, agility, scale and cost-savings, a cloud security assessment can support and guide IT organizations tasked with protecting business-critical assets in the cloud.

Enterprises are adopting a wide number of cloud applications and cloud technologies. From cloud storage, collaboration tools, office suites and enterprise applications, cloud services are adding remarkable computing power to day-to-day operations – as well as significant cloud security risks. The vast majority of cloud applications are not enterprise ready, and IT teams are unable to secure cloud technology at the same rate it is being adopted by enterprise users. Various deterrent, preventative and detective control therefore need to be put in place.

SECURE APPLICATIONS IN THE CLOUD—YOUR ORGANISATION STILL OWNS THE RISK

A cloud security assessment can help by identifying risks, evaluating current controls, identifying gaps or weaknesses and providing recommendations tailored to business priorities. With a superior cloud security assessment, enterprises can successfully navigate the shifting landscape of cloud computing security while developing a mature cloud security architecture to protect data, users and the organization.

That's where Risk Imperium can help. With a bench of security experts well-versed in all aspects of cloud security, we can help to design, plan and implement a cloud security assessment to help organizations achieve cloud strategy goals, improve cloud security and enable new business models.

Elements of Risk Imperium's Cloud Security Assessment
Our cloud security services include a wide range of capabilities for a cloud security assessment, including:

- Identifying cloud security risks.
- Performing a cloud security audit to document current controls and provide visibility into the strengths and weaknesses of current systems.
- Assessing gaps in current capabilities that may weaken cloud security in recommending technology and services to address them.
- Assessing security maturity by benchmarking current controls and practices against leading methods and standards.
- Performing a cloud security assessment of the effectiveness of current policies and their alignment with business goals.

Cloud Security

Cloud security controls

Cloud security architecture is effective only if the correct defensive implementations are in place. An efficient cloud security architecture should recognize the issues that will arise with security management. Risk Imperium ensures that security management addresses these issues with security controls. These controls are put in place to safeguard any weaknesses in the system and reduce the effect of an attack. While there are many types of controls behind a cloud security architecture, they can usually be found in one of the following categories:

Deterrent controls

These controls are intended to reduce attacks on a cloud system. Much like a warning sign on a fence or a property, deterrent controls typically reduce the threat level by informing potential attackers that there will be adverse consequences for them if they proceed. (Some consider them a subset of preventive controls.)

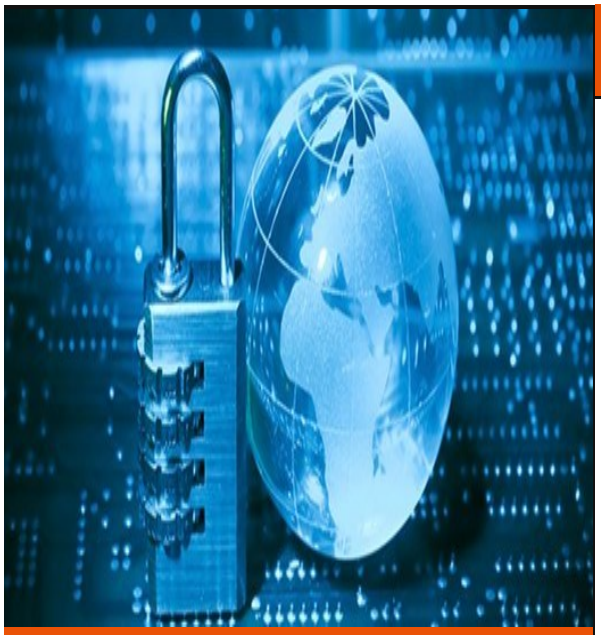
Preventive controls

Preventive controls strengthen the system against incidents, generally by reducing if not actually eliminating vulnerabilities. Strong authentication of cloud users, for instance, makes it less likely that unauthorized users can access cloud systems, and more likely that cloud users are positively identified.

Detective controls

Detective controls are intended to detect and react appropriately to any incidents that occur. In the event of an attack, a detective control will signal the preventative or corrective controls to address the issue. System and network security monitoring, including intrusion detection and prevention arrangements, are typically employed to detect attacks on cloud systems and the supporting communications infrastructure.

SECURE APPLICATIONS IN THE CLOUD—YOUR ORGANISATION STILL OWNS THE RISK



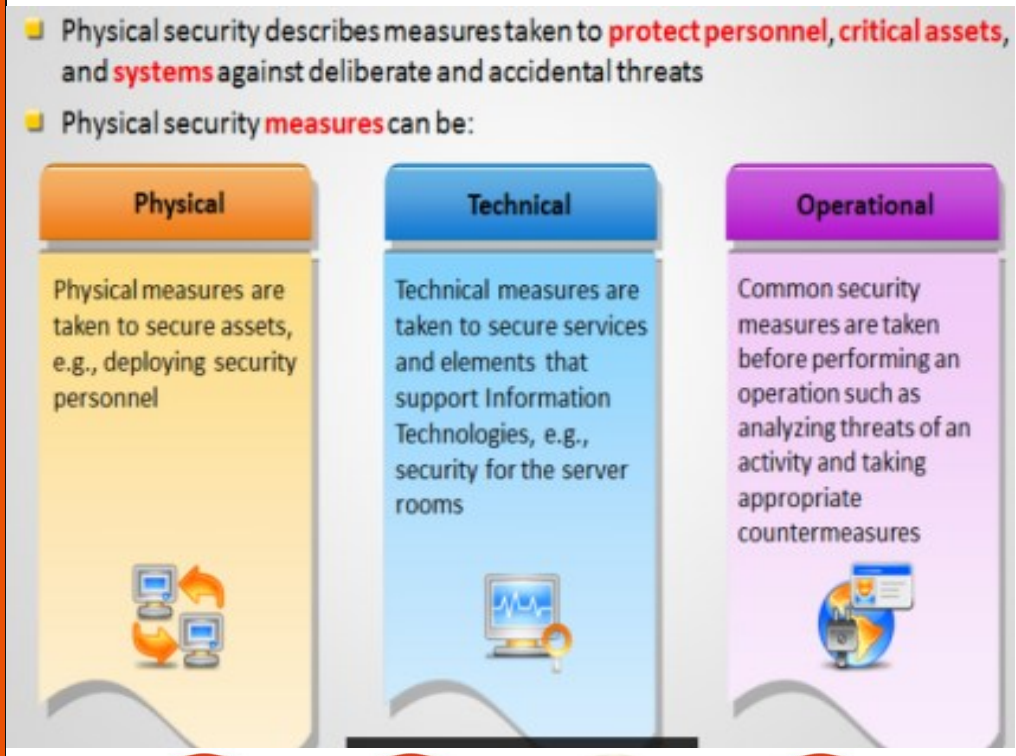
Physical & Environmental Security

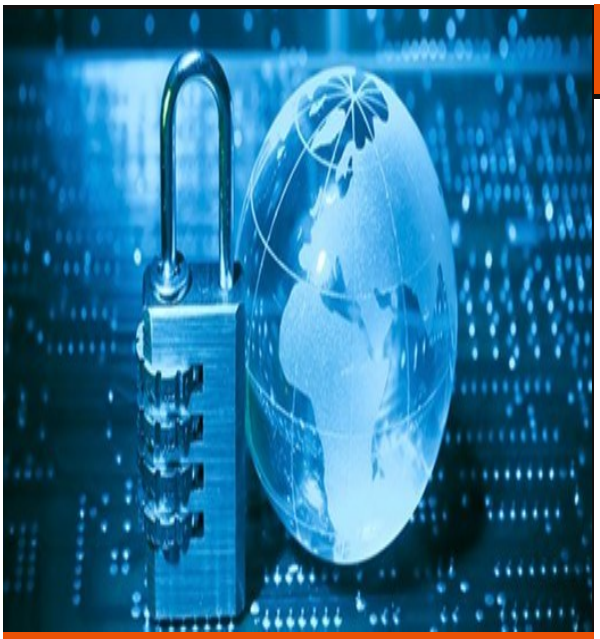
Physical security is the protection of personnel, hardware, software, networks and data from physical actions and events that could cause serious loss or damage to an enterprise, agency or institution. Risk Imperium works with your organisation to achieve the following:

- Determine critical, operational or administrative needs
- Allocate physical security roles and responsibilities
- Conduct physical security risk assessments
- Determine site or data centre security requirements
- Enforce effective access controls - then log and review access
- Detect and respond to physical incidents.
- Procure adequate physical security products and services

Mature governance, risk management, and compliance practices for your physical security go beyond simply reducing policy breaches and risk events. If you properly align your efforts with the unique needs of your organization, they will make it more agile, more resilient, and more respected among your most important internal and external stakeholders.

SECURELY CONNECTING YOUR BUSINESS TO TECHNOLOGY RESOURCES





BUSINESS CONTINUITY MANAGEMENT (BCM) PROGRAM PROVIDES THE ORGANISATIONAL BACKBONE FOR THE MANAGEMENT OF BUSINESS DISRUPTION

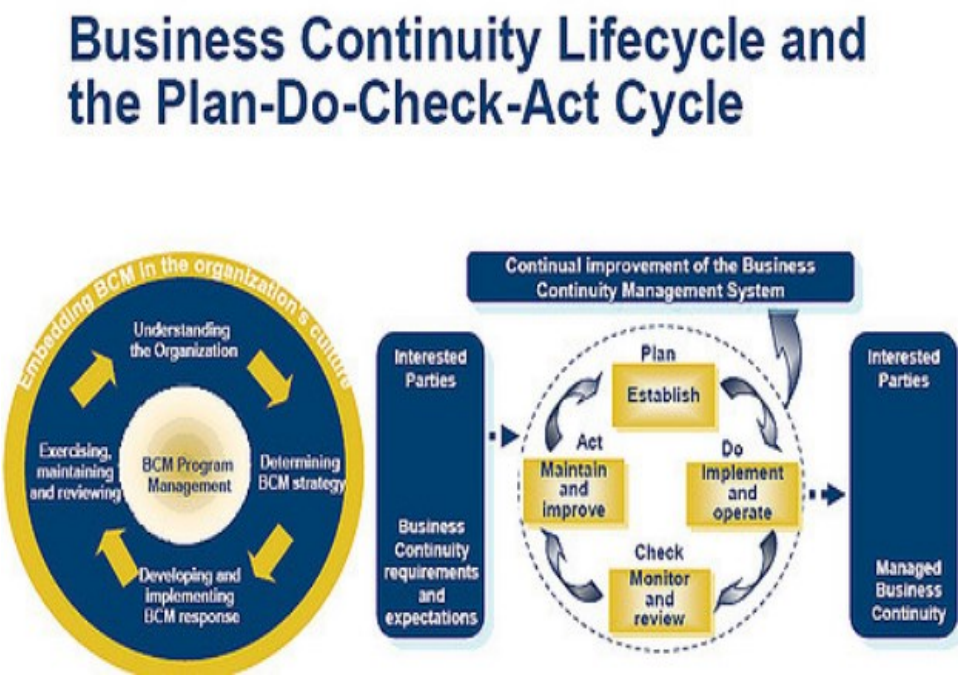
Business Continuity Management

A Business Continuity Management (BCM) program provides the organisational backbone for the management of business disruption. The program includes a business impact analysis to understand the effects of disruption on organization's resources, the identification of appropriate recovery strategies, development and implementation of plans and the essential training and planned maintenance to ensure the solution remains effective.

Risk Imperium works shoulder by shoulder with your organisation to develop and implement a BCM program that best addresses your business needs.

Our consultants can help you with all phases of a BCM program, from defining a BCM strategy that takes a long-term view of organisational continuity needs to developing the over aching policy outlining management direction and support for BCM. Our support would also include supporting the organisation to undertake business impact analysis, develop business continuity plans, perform tests test based on business continuity plans, document reports and maintain procedures for all critical infrastructure.

Risk imperium provides support through the BCM lifecycle illustrated below:



Third Party Risk Management

Risk Imperium's comprehensive Third Party Risk Management (TPRM) framework addresses strategy, structure, people, process and technology issues across the TPRM lifecycle, helping your organisation to:

- Define a TPRM Strategy
- Develop a customized TPRM framework
- Develop the TPRM policy, standards and procedures
- Assess your current environment
- Develop and enforce TPRM processes
- Increase the efficiency and effectiveness of vendor-related risk management
- Develop a risk stratification protocol to highlight risks by vendor
- Implement and conduct effective TPRM activities, such as vendor assessments

WHEN YOU OUTSOURCE OPERATIONS, RISK AND COMPLIANCE REMAIN YOUR RESPONSIBILITY. DON'T BE BLINDSIDED BY A THIRD PARTY'S INADEQUACIES.

Risk Imperium understands vendor risk. We can help your organisation prevent third party-related disruptions by implementing a TPRM program that will strengthen your position and build more effective partnerships that protect your brand and business.

Third Party Risk Management

Risk Imperium works shoulder by shoulder with your organisation in the following areas;

- Strategy & Planning – Develop sourcing strategy, consider costs/benefits and develop business
- Evaluate and select – identify, assess risks and perform due diligence
- Contract and onboard – incorporate risks, compliance and performance requirements in the contract
- Manage and monitor – perform risk management and ongoing monitoring and coordination with each third party
- Terminate and offboard – determine need to terminate the third party and manage the offboarding process

WHEN YOU OUTSOURCE OPERATIONS, RISK AND COMPLIANCE REMAIN YOUR RESPONSIBILITY. DON'T BE BLINDSIDED BY A THIRD PARTY'S INADEQUACIES.

Our TPRM Packages

1. TPRM Training & Awareness
2. Development of the TPRM Framework
    - TPRM Assessments
    - Due diligence in selecting a third party
    - Contract structuring and review
    - Oversight
3. TPRM Policies and Standards
4. TPRM Deep dives, Assessments or Audits to identify gaps and make recommendations

Cyber Readiness

Building your cyber confidence and assessing cyber security helps determine your readiness to detect, prevent, contain and respond to the evolving cyber threats.

With the increasing number of cyber attacks and data breaches affecting companies, the public now demands more from organisations in protecting the confidentiality, integrity and availability of sensitive customer data and systems.

Risk Imperium supports your organisation to:

- Evaluate the latest threat landscape based on your organization's business needs
- Prioritize your plans to combat cyber security risks
- Assess your readiness to handle massive cyber attacks through scenario development
- Provide insights on your readiness with reference to industry standards and training and awareness with regards to the following:

1. People matters— building a robust organisation's culture of cyber security starting from top management to general employees
2. Prioritising what you secure—what are your 'crown jewels' and how well are they protected?
3. Governance—threats evolve. Do you have a process to monitor, learn from and deal with the emerging trends in cyber attacks?
4. Technology—do you have sufficient technologies to deal with cyber attacks such as Advanced Persistent Threat (APT) and Distributed Denial-of-Service (DDoS)?
5. Incident response— it could happen. Are your current internal protocols equipped to deal with cyber crises?
6. What is the most appropriate manner for external communications
7. Connections—their risk is your risk. Are you confident in your supply chains and business partners' security?

CYBER CONFIDENCE AND ASSESSING CYBER SECURITY HELPS DETERMINE YOUR READINESS TO DETECT, PREVENT, CONTAIN AND RESPOND TO THE EVOLVING CYBER

Training and Awareness

Without the right corporate culture, written policies and technical controls are meaningless. Employees need to understand their role and the implication of their actions. When elements relating to culture are not well established, it can lead to enormous fines, poor employee performance and retention, a diminished brand through reputational damage, and weaker investor returns. When it comes to cyber security, the organisation's employees are its greatest asset, but also its biggest weakness.

The risk and information/cyber security behaviours of people within an organisation can be a complex mix of awareness, their personality, the kind of training they receive and the security culture that exist across the organisation.

Risk Imperium's effective training and awareness programs help personnel to actively take appropriate measures that reduce the people risk element of risk and information/cyber security. Risk Imperium prepares practitioners for information security management through training programs and risk assessment workshops that can be customised for their business needs.

WHEN IT COMES TO CYBER SECURITY, THE ORGANISATION'S EMPLOYEES ARE IT'S GREATEST ASSET BUT ALSO IT'S BIGGEST WEAKNESS

Key Steps

Risk Imperium's five step methodology will provide you with a route to successful Cyber Security Awareness by:

1. Defining the scope 2) Designing the content 3) Establishing the baseline 4) Delivering the programme 5) Measuring and evaluating benefits, which include;

A) A focused programme, using real life examples, to enhance the security culture of the organisation. B) Comprehensive understanding of the individual's personal role in protecting data and information. C) Improvements in the security behaviour at all levels to reduce the risk to the organisation. D) The organisation moves from a reactive to a proactive approach to current and future threats.

Risk Imperium's Information Security Services Catalog

Governance, Risk & Compliance	Identity & Access Management	Security Operations	Systems Security	Cloud Security	Application Development
Information Security Program/Framework	Access Management Lifecycle	Data Loss Prevention	Threat Modelling	Business Assessments	Application Portfolio Management
Policies, Standards, Procedures and Metrics	Entitlement Attestations	Antivirus	Security Architecture	Architecture Design	Enterprise Application Selection & Implementation
Risk Management Framework	IDM Platform Implementation	Data Encryption & Erasure	Social Engineering	Security Testing and Validation	Application Development Throughput
Support to IT Audits	IDM Maintenance and Support Services	IDS/IPS/Firewall Monitoring	Vulnerability & Patch Management	Virtual Environment Audits	Application Development Quality
Regulatory Compliance Audits		Fraud Prevention & Anti Money Laundry	Penetration Testing		Application Quality
Compliance Solutions		Security Intelligence	Cyber Threat Monitoring		
Third Party Risk Assessments			Security Configuration		
Business Continuity & Disaster Recovery Plans					
Training and Awareness					
Gap Analysis					
Certification and Accreditation					
Physical Security Assessments					

Contact Us

RISK IMPERIUM CONSULTING LIMITED

Sanyu Business Arcade| Frobel Road | Ntinda | Kampala.

Tel: + 256 7520 12115
Email: Info@riskimperium.com

Web: https://www.riskimperium.com

20 - 22 Wenlock Road | London | N1 7GU | (UK)

Tel: + 4420 3612 9787
Mobile: +4474 7569 1350

Email: Info@riskimperium.com

Web: https://www.riskimperium.com

Cyber Security Products

EndpointLock Keystroke Encryption

EndpointLock Secure Keyboard—the ONLY SOLUTION to stop zero-day keylogging spyware installed on a device.

PROBLEM: KEYLOGGING SPYWARE is a main component of malware used to steal identity and credentials from a user's device, helping to advance the breach. Keyloggers are difficult to detect by traditional anti-virus, even if these programs are up-to-date.

As mobile online activities hit record highs, Risk Imperium in partnership with ACS (Advanced Cyber Security) answer the growing demand for security by availing EndpointLock Keystroke Encryption for every smartphone and tablet. Other key feature include the following:

- EndpointLock™ KTLS™ delivers Keystroke Transport Layer Security: While SSL and TLS begin strong cryptography at Layer 4 or, the Transport Layer within OSI, KTLS™ begins strong cryptography from the kernel level at ring 0 and encrypts all keystrokes.
- ACS EndpointLock™ will automatically detect if a PC has an Intel TMP (Trusted Platform Module) chip, which is designed to secure hardware and software integrity by integrating cryptographic keys into devices, and will install directly to the TPM on the PC.
- Warns the user of a kernel breach by detecting the presence of any unsigned software or if a driver has been altered since it was released.
- Anti-subversion technology prevents ACS EndpointLock™ from being bypassed by other software by reinstalling itself in the first position in the kernel level.
- Hides the screen from screen loggers and sends them a black screen. Makes the invisible, visible. Hackers can embed invisible objects into iFrames and wireFrames. ACS EndpointLock™ can detect this type of attack and unhide the invisible object, and paint a red border around the object, alerting the user not to click on this object.

Attached below is a literature on EndpointLock Encryption solution for desktops

And mobile devices

Adobe Acrobat Document

WHEN IT COMES TO CYBER SECURITY, THE ORGANISATION'S EMPLOYEES ARE IT'S GREATEST ASSET BUT ALSO IT'S BIGGEST WEAKNESS

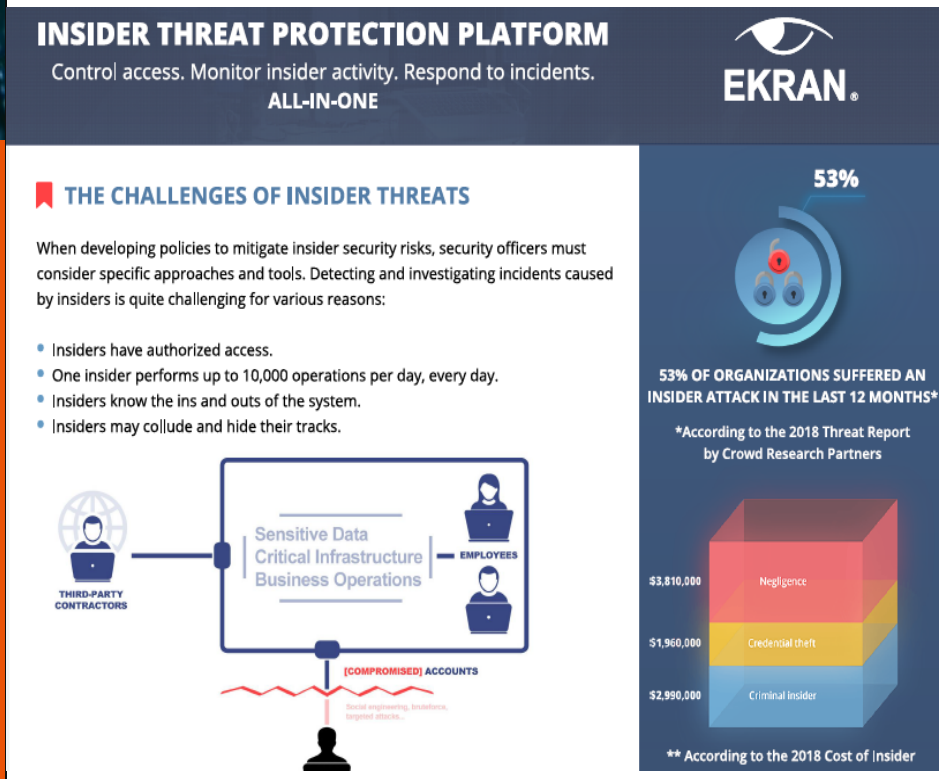
Cyber Security Products

Insider Threat Protection Platform

The Insider Threat Protection Platform enables organisations to control access, Monitor insider activity and respond to incidents. Detailed in the product litera ture below id more intormatio

Adobe Acrobat Document

WHEN IT COMES TO CYBER SECURITY, THE ORGANISATION'S EMPLOYEES ARE IT'S GREATEST ASSET BUT ALSO IT'S BIGGEST WEAKNESS



Ris Imperium's Partners

Contact Us

RISK IMPERIUM CONSULTING LIMITED

Sanyu Business Arcade| Frobel Road | Ntinda | Kampala.

Tel: + 256 7520 12115
Email: Info@riskimperium.com

Web: https://www.riskimperium.com

20 - 22 Wenlock Road, London, N1 7GU (UK)

Tel: + 4417 02894400
Mobile: +4474 7569 1350

Email: Info@riskimperium.com

Web: https://www.riskimperium.com