INFORMATION SECURITY

SERVICES TO SUPPORT YOUR ORGANISATION

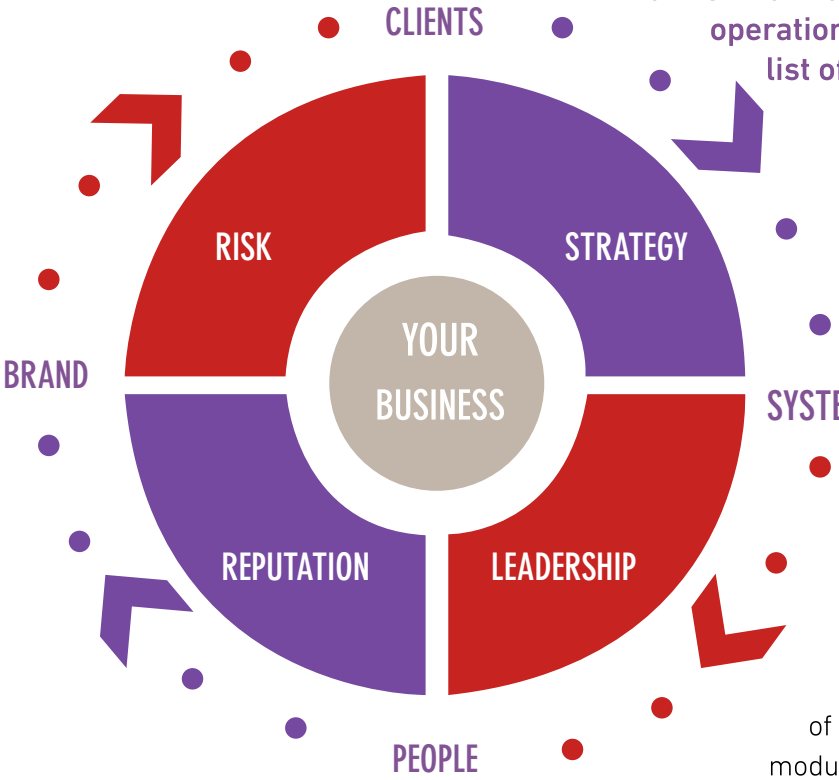
MAZARS

YOUR CHALLENGES

We live in an information society where the demand for data is high, and where it is widely available and accessible by many, to many. It is safe to say that, as in any organisation, information flows in and out of your business consistently.

- Are trust and reputation the cornerstones of your business model?
- Does your organisation handle sensitive commercial information?
- Do you hold and process personal data?
- Does your organisation hold a duty of care towards third party data?

Business relationships are built on trust. Your brand reputation is in all probability your greatest asset and key market differentiator.



How is information security embedded within your operation, and does it feature at the top of your list of risks?

Mazars can assist you in strengthening your defenses and creating proactive information security awareness in your organisation. We have a team of specialised and dedicated information security specialists who can put together a comprehensive service offering tailor-made to your requirements, whether you represent an SME or a larger entity that holds and manages sensitive information.

We understand and talk your language because, as a firm, Mazars also shares many of your challenges. Moreover, as part of our modus operandi, we will work closely and build meaningful relationships with your internal teams and outsourced service providers.

Our expertise is based on years of experience providing assurance services to entities of all shapes and sizes. As in everything we do at Mazars, our independence is a cornerstone of our service offering, ensuring that we remain objective and free from any conflict of interest.

OUR RESPONSE

Our Information Security ('InfoSec') offering is comprehensive and includes:

Our service offering is based on industry developed best practices to provide an up-to-date assessment of your organisation's cyber security status, ensuring that risks and threats to the IT environment are routinely mitigated.

IT RISK ASSESSMENTS

IT Risk Assessments allow entities to identify key risks that pose a threat to their organisation and provide an understanding of the strength of the mitigating controls put in place. Risk assessments allow management to prioritise time and investment on those issues that pose the highest risk.

Mazars can assist clients in assessing and evaluating their IT environments. Such a review will allow entities to gain a high-level understanding of their current security status. Mazars will draw up a report that provides a current threat overview, followed by recommendations, a risk matrix and risk register.

The IT Risk Assessment will cut across all significant areas of the IT environment and will include a full Internal Procedures Review:

- High-level reviews of the organisation's current security footprint
- Review organisation's IT infrastructure against current security best practices
- Understanding of the company's current IT processes
- Identification of high level risks and associated recommendations
- Review of available data classification strategy
- Review and analysis of segregation of user rights
- Employee awareness and training

HEALTH CHECK

Health checks are an in-depth, technical review of a client's IT environment using industry developed best practices, methodologies and technical tools which are used to assess an organisation's exposure to IT threats and provide recommendations based on the outcome of detailed vulnerability analysis.

VULNERABILITY ASSESSMENTS

Routine vulnerability assessments are critical to an organisation's ability to identify and mitigate current cyber security threats to their IT environment. Vulnerability assessments consist of using specialist tools to scan an organisation's IT infrastructure to detect security weaknesses and flaws that can be rectified through maintenance and process reviews.

The vulnerability assessments consist of the following:

- Routine system checks
- Internal scans of an organisation's infrastructure including infrastructure patch levels, malicious software detection, anti-virus update levels
- External infrastructure scanning
- Current high-level security state and threat level reporting
- In-depth technical reports for IT teams
- Identification of organisation's data which is exposed to the public
- Logical and physical securitys control assessments
- Open Source intelligence gathering

PENETRATION TESTING

Penetration tests are the second stage in the health check service offering and allow Mazars to demonstrate a client's state of vulnerability to IT threats by simulating cyber attacks against an organisation's IT environment. The Mazars InfoSec team will attempt to probe and breach a client's security infrastructure to discover and analyse any weaknesses in their cyber-defences and provide recommendations to mitigate any related risks.

The penetration testing phase includes the following elements:

- Incident response testing
- Internal vulnerability exploitation
- External vulnerability exploitation
- Social engineering attempts
- Logical and physical access tests
- High level reports
- Technical reports for IT teams
- Recommendations

PROCESS REVIEW

Good governance, best practice, and in various instances, regulatory requirements, require entities to document their policies and procedures and to review them regularly. Clear, concise and up to date policies and procedures are at the heart of every healthy control environment and successful business.

Mazars can assist entities in this task. We bring to the table expertise, experience, best practice and objectivity. Our service offering is flexible and may include:

- Assistance in drafting policies and procedures
- Reviewing and updating of existing policies and procedures
- Auditing organisation compliance with established policies and procedures

Our focus may, amongst others things, point on the following areas:

- Understanding of the company's key business processes which have a high dependency on IT controls
- Mobile Device Management
- Incident Response Management
- Change Management Controls
- Backup and Recovery Management
- Business Continuity Procedures
- IT Governance
- Authentication Controls
- Logical and Physical Access Controls

TRAINING

Often cited as the weakest link and the easiest way through the back door, organisations are made up of people – *the human firewall*. Investment in hardware and systems will only provide the required assurance if the human element is addressed comprehensively and effectively. An informed and alert team throughout your organisation (from board level to shop floor) will result in a much more resilient entity and better management of risk.

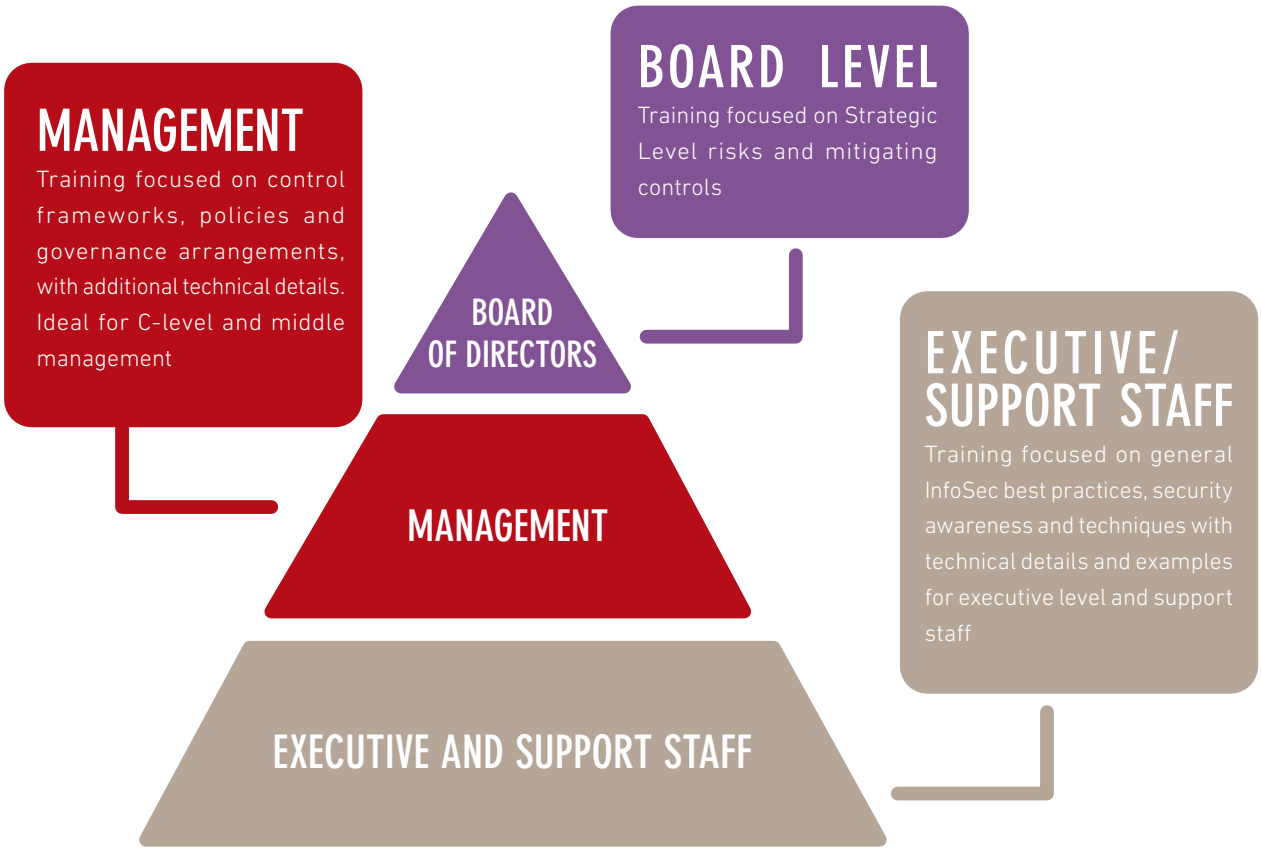
Training services are offered on both a bespoke and standard basis, depending on the nature of the client and target audience. The scope of the training include a specific set of InfoSec related topics, the details of which are listed below, based on the target audience.

Our training courses are aimed at and tailor-made to the following target audience profiles:

- Board Level
- Management Level (Including C-Level Management)
- Executive
- Support Staff (Admin / Customer Support etc.)

TRAINING COURSES

Our training is defined for each target audience profile. Certain overlaps in training items may arise as training items may be applied to more than one audience profile.



TRAINING ITEM	DETAILS	BOARD	MANAGEMENT	EXECUTIVE
Reputation Damage	Implications of IT risks on company reputation	✓		
Regulatory Compliance	Importance of regulatory for the purposes of IT risk mitigation	✓		
Sensitive Information Disclosure	Different types of risks inherent and caused by sensitive information disclosure	✓	✓	✓
Social Engineering Awareness	Risks and mitigating procedures to typical SE attacks	✓		
Data Classification	Categorisation of different levels of document sensitivity	✓		
Governance and control frameworks	High level overview of IT control frameworks	✓	✓	
Importance of InfoSec in relation to GDPR	High-Level overview of risks related to GDPR	✓	✓	
BCP/DR	Business Continuity and Disaster Recovery risks & best practices	✓	✓	
Incident Response Management	Media Handling Policies, Cyber Crimes	✓	✓	
Password Controls	Password best practices and controls		✓	✓
Role-Based Access Controls	Segregation of responsibilities and data access controls		✓	
Security Best Practices	General IT security best practices, risks and controls		✓	✓
Data Classification	Classification of document sensitivity		✓	
User Management Policies	Procedures and inherent risks of onboarding and employee termination policies		✓	
Mobile Device Management	Importance of MDM, inherent risks and controls		✓	
Loss of income through data theft / loss	Risks associated with data theft and data loss		✓	
Outsourcing	Risks, controls & best practices when adopting Cloud & outsourcing models		✓	
IT Security Awareness	Mobile security, ransomware threats			✓

SOCIAL ENGINEERING

Our service offering is unique in that, at the client's discretion and subject to strict agreed terms, we can conduct tailor-made social engineering scenarios to try and test for employee readiness and security awareness.

The Mazars InfoSec team may attempt to gain access to a company's systems by manipulating employees using a number of tactics in an attempt to coerce them into disclosing sensitive company information.

The actions carried out by Mazars will provide clients with an in-depth understanding of their employees' security awareness and identify real vulnerabilities that may impact the security and integrity of their IT system, as well as any resultant impact on reputation and revenue.

PHISHING ATTEMPTS	Employees will be subjected to random emails sent by the Mazars InfoSec team (masquerading as company employees) and will attempt to harvest employee credentials by appearing to be legitimate
TAILGATING (PIGGYBACKING)	Members of the Mazars InfoSec team will attempt to gain access to secured locations on company premises by following authorised employees into restricted areas within company premises
BAITING	The Mazars InfoSec team will attempt to acquire sensitive company information by luring employees with false adverts of free goods and services and tricking them into disclosing sensitive information
QUID PRO QUO	The Mazars InfoSec team will create a fabricated scenario (pretext) which will be used to obtain information from employees using the pretence of the fabricated scenario to trick employees into giving up sensitive information
INFORMATION EXCHANGE	Employees are prompted to disclose sensitive information by being promised an exchange of information or services by the Mazars InfoSec team to determine whether employees are vulnerable to "Quid Pro Quo" attacks
USB ATTACKS	The Mazars InfoSec team is able to gauge and demonstrate employees' awareness to the implications of plugging in untrusted devices to their computers by distributing custom built USB flash drives which are able to send out remote alerts when plugged in to an employee's computer

Get in touch

Mazars Malta
32, Sovereign Building
Zaghfran Road,
Attard ATD 9012
Tel: +356 21345 760
E-mail: contact@mazars.com.mt

Alan Craig
Partner
alan.craig@mazars.com.mt

Ramon Cutajar
Senior Manager
ramon.cutajar@mazars.com.mt

Detailed information available on on www.mazars.com.mt

MAZARS