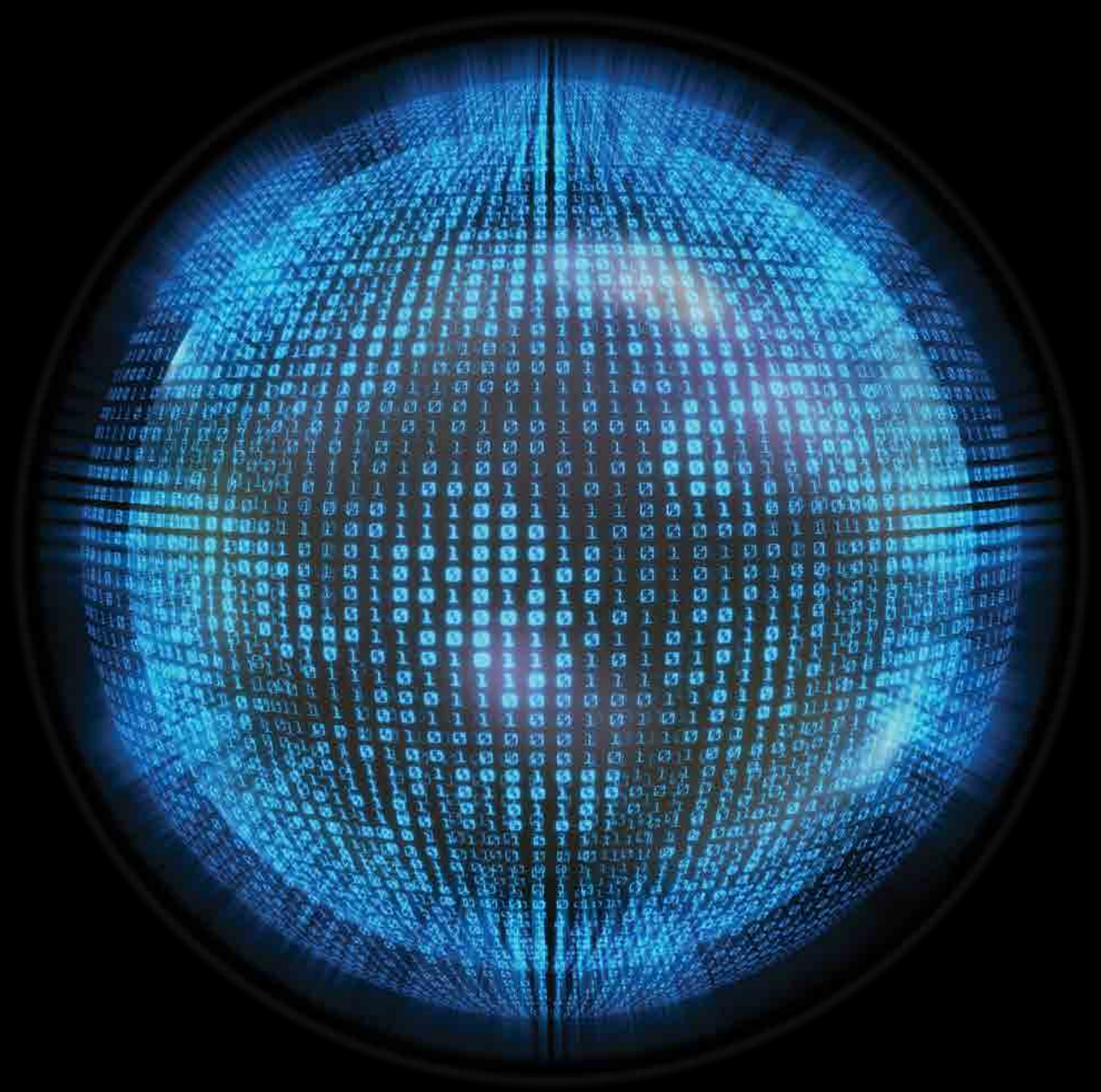
Deloitte.



Cyber Risk Services

Secure. Vigilant. Resilient.

Deloitte Malta, 2017

Cyber

Cyber operations
Secure. Vigilant. Resilient.

Secure
Establishing risk-prioritized controls to protect against known and emerging threats, and comply with standards and regulations. Establish a current security state to ensure that all devices are patched, updated and ready to handle potential attack.

Vigilant
Reducing detection time and developing the ability to detect the unknown. Establishing situational risk and threat awareness across the environment is a must to detect violations and anomalies.

Resilient
Strengthening your ability to recover when incidents occur. Establish the ability to handle critical incidents, quickly return to normal operations, and repair damage to the organization.

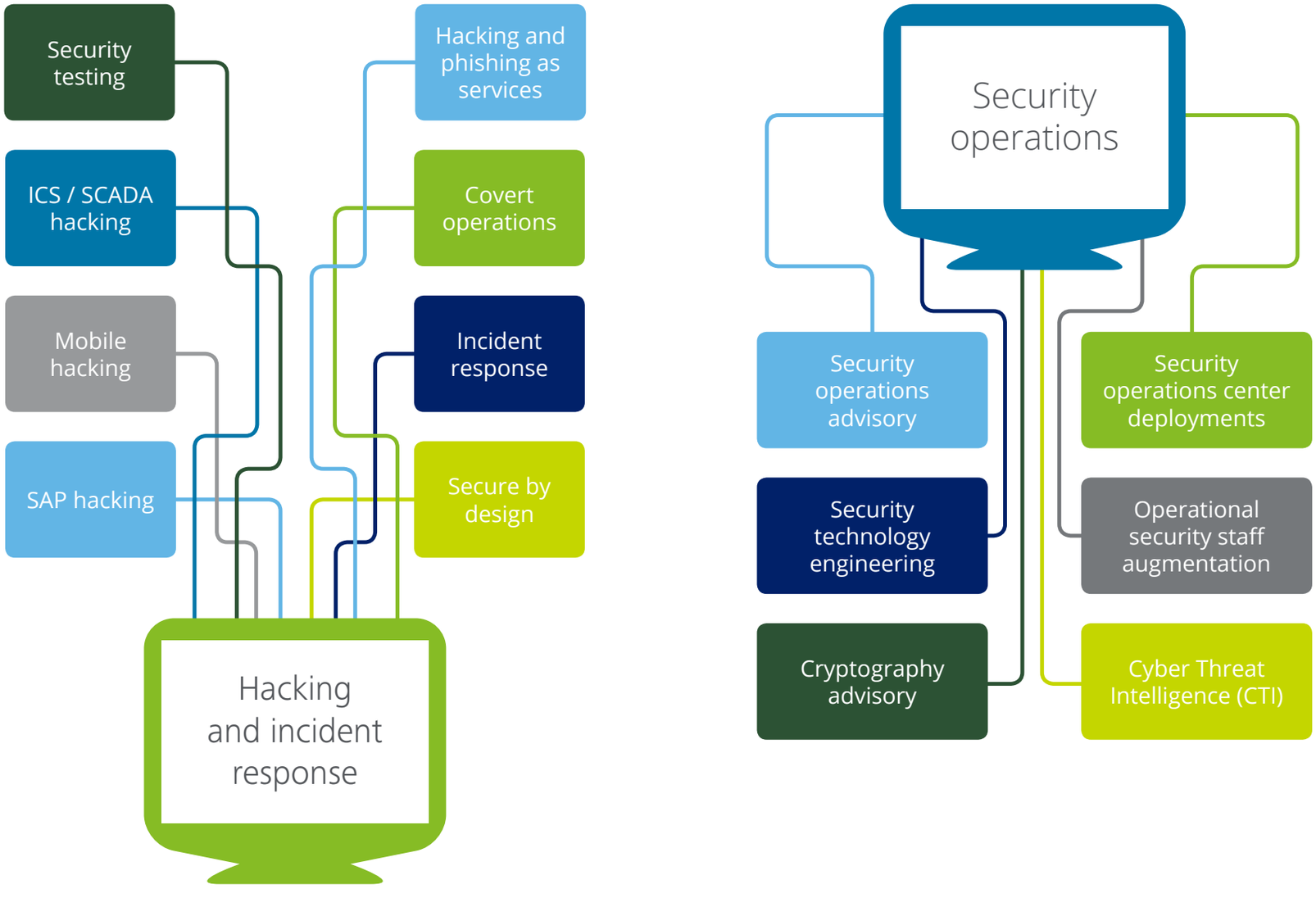
Cyber operations services

- Core services
- Security testing
- Mobile hacking
- SAP hacking
- Hacking as a service
- Covert operations
- Incident response
- Secure by design
- Security operations advisory services
- Security Operations Center (SOC) deployments
- Security technology engineering
- Cryptography advisory
- Cyber Threat Intelligence (CTI)
- Cyber simulation

Contents

Cyber operations services

Core services



Cyber simulation

Security testing

Description

Businesses are relying on IT infrastructure and (web) applications to provide their services to clients and run an efficient backoffice process. The information security of these environments (and the information in them) is very important to businesses. Deloitte provides services which perform a simulated hacker attack on selected IT infrastructure and (web) application environments. Aim is to:

- Identify vulnerabilities in these environments which may cause access to sensitive information or service interruption;
- Provide insight on business risk; and
- Provide recommendations for improvement of the security posture.

How can we help?

- Internet-facing IT infrastructure such as VPN solutions or platforms supporting applications;
- Selected internal IT systems such as file servers, workstations, application servers;
- Specific internet-facing web applications such as a webshop or internet banking application, or internal web applications such as a call centre application;
- Specific new application functions such as APIs or transaction-based functions; and
- Configuration of firewalls, routers, databases, or Linux/Windows OS.

Security testing/hacking as a service

Specific services:

- Infrastructure security test
- Application security test
- Source code security test
- Wi-Fi security test
- Configuration security test

Mobile hacking

Description

Businesses are offering mobile apps to clients to provide access to their services and the possibility for their staff to work from any device. The information security of these environments (and the information in them) is very important to businesses. Deloitte provides services such as performing simulated hacker attacks on selected mobile app environments and mobile devices. The aim is to:

- Identify vulnerabilities in these environments which may cause access to sensitive information or service interruption;
- Provide insight on business risk; and
- Provide recommendations for improvement of the security posture.

How can we help?

- Configuration of phones and tablets running various mobile operating systems;
- Application security/source code of various mobile apps such as timesheets apps, news apps, or medical apps;
- Configuration of MDM platforms such as Good and MobileIron.

Mobile hacking
Specific services:

- Mobile device (management) security test
- Mobile app security test

SAP hacking

Description

SAP software supports critical processes of business, e.g. for finance or CRM. These SAP systems are critical for business operations and contain highly sensitive information. The information security of these SAP environments (and the information in them) is very important to businesses. In the past years the complex SAP software has been increasingly expanded with new functionality/technologies, and multiple security issues have been discovered in SAP software.

Deloitte can perform simulated hacker attacks on selected SAP systems and the supporting IT infrastructure. Aim is to:

- Identify vulnerabilities in SAP environments which may cause access to sensitive information or service interruption;
- Provide insight on business risk; and
- Provide recommendations for improvement of the security posture.

How can we help?

- Selected internal SAP core systems;
- IT infrastructure supporting SAP core systems;
- Configuration of firewalls, routers, databases, or Linux/Windows OS.

SAP hacking

Specific services:

- SAP hacking test

Hacking as a service

Bronze
Periodic security testing of Internet-facing infrastructure components for insecure software, services, and the presence of new systems. This test simulates an attack by a malicious attacker on the infrastructure that supports your online applications.

Silver
Same as Bronze. In addition, the Silver subscription includes security test websites on known vulnerabilities, such as SQL injection and Cross-Site Scription (XSS). This test simulates an attack by a malicious attacker on your websites.

Gold
Same as Silver. In addition, the Gold subscription includes thorough security testing of web applications, specifically on “privilege escalation” (the unauthorized access to information or functions as a normal user). This test simulates an attack by a malicious attacker who already has access to your online applications as an authorized user.

Hacking as a service
Specific services:

- Subscription based security test

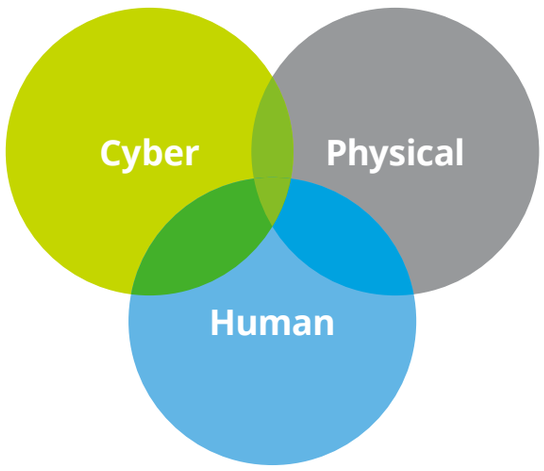
Hacking as a service	Bronze	Silver	Gold
Vulnerability reporting			
Insecure software (e.g. outdated versions of software)	●	●	●
Unknown systems and services	●	●	●
Insecure services (e.g. insecure management interfaces, inadequate encryption)	●	●	●
Weaknesses in websites (e.g. SQL injection, XSS)	○	●	●
Weaknesses in web applications (e.g. privilege escalation)	○	○	●
Trend reporting (annual)	●	●	●

Covert operations

Description

A covert operations team is a group of highly skilled ethical hackers who assess the security of an organization which is often unaware of the existence of the team or its exact assignment. Such teams provide a more realistic picture of the security readiness than exercises, staged role playing, or pre-announced assessments.

Covert operations teams are designed to both capture pre-agreed "flags" as well as trigger active controls and countermeasures within a given operational environment.



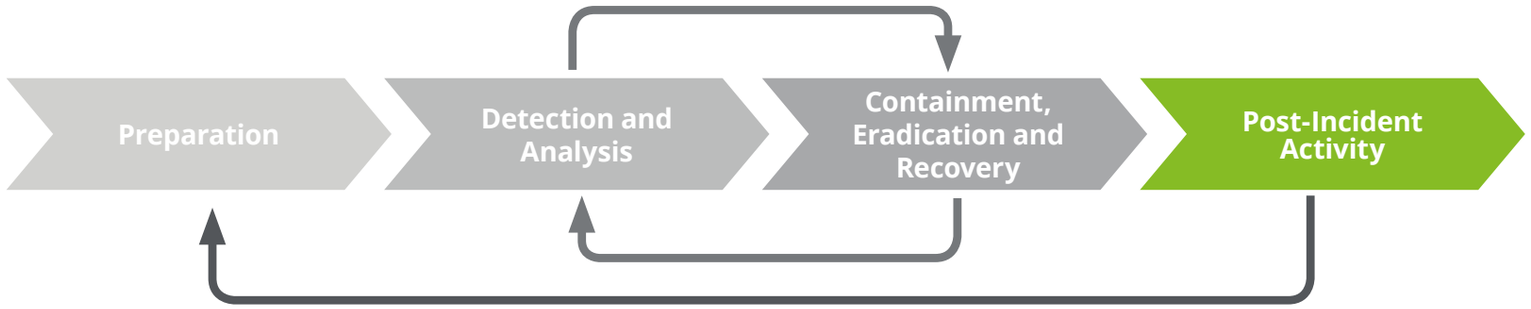
How can we help?

- Simulation of a cyber attack on an organization where attackers aim to capture the organization's "crown jewels" by using physical, human and technical weaknesses;
- Spear phishing campaign to identify selected employees' awareness and/or to show that network access can be obtained via custom malware;
- Use Open Source Intelligence (OSINT) to gather intelligence about a company or persons. The OSINT may aid in a cyber attack;
- Capture pre-defined "flags" (e.g. gain access to critical internal databases) via a tactical network exploitation exercise on the internal network.

Covert operations
Specific services:

- Spear phishing
- Social engineering
- Tactical network exploitation
- Physical penetration test
- Intelligence analysis (OSINT)
- Awareness sessions

Incident response



Description

Deloitte's incident response services focus on helping organizations prepare an adequate incident response and to provide support during a cyber security incident. Activities could include awareness sessions, mock incident training, and hands-on support such as malware analysis and recovery support.

How can we help?

- Support an organization during or after a hacker attack with hands-on technical analysis capabilities such as malware analysis. We can help with detection and analysis, containment, eradication and recovery, and support with post-incident activities such as improving existing capabilities;
- Enhance an organization's awareness and preparedness for an incident by providing mock incident training. These mock incidents may uncover issues in an organization's incident response process, governance or technical capabilities which may require improvement before a real incident takes place;
- Support during crisis management or forensic investigations through technical cyber security expertise.

Incident response
Specific services:

- Incident response support
- Mock incident training

Secure by design

Description

Support an organization to embed security throughout the Software Development Lifecycle (SDLC) in order for an organization to deliver a software product which is secure by design.

How can we help?

- Perform a maturity assessment of security in the SDLC to provide insight on the current maturity level;
- Support in improving the organization's SDLC process by embedding security aspects in all phases. This would entail tailoring the process by including practical checklists or adding steps such as security requirements, threat modelling or security tests;
- Provide security training to development teams, e.g. around Open Web Application Security Project (OWASP) top 10 security issues including source code examples;
- Support an organization with embedding regular security testing in the SLDC, e.g. by setting up a source code security review tool and supporting tracking/support process;
- Provide security expertise in ongoing development projects, e.g. by reviewing proposed architecture or discussing security requirements.

Secure by design
Specific services:

- SDLC maturity assessment
- Threat modelling
- Architecture review
- Automated source code reviews
- Remediation tracking and support
- Virtual patching support

Secure by design

Define → **Design** → **Develop** → **Test** → **Deploy**

Acquisition, discovery, analysis

- Maturity assessment
- Identify/create application security guidelines and standards
- Identify client security and privacy needs, contract check lists

Flow, prototype, refine

- Threat modelling of apps to create security requirements
- Architecture review
- Secure SDLC training

Build, test, iterate

- Automated and manual code review using static analysis tools
- Verify the security requirements

Test, accept

- Perform security tests (app and infrastrcture)
- Baseline configurations
- Remediation tracking and support

Operations, publish, launch

- Virtual patching support
- Continuous monitoring and scanning
- Managed security operations

Security operations advisory services

Description

- Security operations advisory services are a broad collection of services in which we help our clients create and augment management decision mechanisms in regards to operational security;
- These services are focused on advising businesses on how best to make use of security operations to meet their business objectives;
- These services are offered by professionals with a deep business, industry and technology understanding.

How can we help?

- Create a maturity assessment for your security operations capabilities;
- Evaluate or design a Target Operating Model (TOM) for security operations;
- Create a business case for security operations;
- Provide technology acquisition advice, including technical evaluations and Proof of Concept (PoC);
- Help to decide upon a sourcing model for your Security Operations Center (SOC).

Secure operations advisory services

Specific services:

- Make the right decisions and be fully supported to strategize, plan and organize your security operations capability

Security Operations Center (SOC) deployments

Description

- SOC deployment encompasses all services related to the design, build, operation and maintenance of SOCs for our clients;
- Deloitte offers multiple delivery methods: in-house, fully outsourced and hybrid. Outsourced and hybrid are considered managed services, whereas in-house is operated by the client;
- SOC services cover people, processes and technology.

How can we help?

- We can design, build and help you leverage your in-house capability;
- We can build a custom and dedicated SOC for you in which Deloitte takes care of absolutely everything;
- We can build your capability in a fully outsourced model in which Deloitte's Cyber Intelligence Centre (CIC) takes care of everything with a minimal footprint on the client side.

SOC deployments
Specific services:

- Existing or recently acquired security technology may need configuration, tuning and performance optimization

Security technology engineering

Description

- Security technology engineering services are designed to help companies make use of new or existing technology;
- Services range from performance management to content creation and maintenance;
- These services are completely executed by fully trained Deloitte professionals.

How can we help?

- Selecting and deploying security technology (see table overleaf for some examples);
- Executing performance improvements (reduction of false positives, network performance, poor user experience, latency, etc.) in new or existing technology;
- Creating and maintaining use cases for detection and response;
- Enabling centrally managed capabilities for distributed technology;
- Performing integration of different existing technologies.

SOC deployments

Specific services:

- Existing or recently acquired security technology may need configuration, tuning and performance optimization

Security technology engineering

Type	Technologies	
SIEM	ArcSight	IBM QRadar
Log Management	splunk	TIBCO loglogic
IDS/IPS	SOURCEfire	TippingPoint
Network Security	FireEye	palo alto NETWORKS
Endpoint APT protection	Bromium	Bit9 + CARBON BLACK
Analytics and big data	hadoop	SAS
Vulnerability assessment	RAPID7	Qualys
Risk management	skybox security	

Cryptography advisory

Description

- Cryptographic advsiory is a collection of services in which Deloitte helps its clients to increase the level of security, as well as offering other related expertise with regards to cryptography;
- These services range from advisory assignments to fully managed cryptographic solutions (e.g. as a key management provider). Training is also an important aspect;
- Services are offered by skilled professionals with a sound background in security and cryptography combined with industry experience.

How can we help?

- We can advise on the development of new and innovative crypto solutions for clients and their business partners;
- We can perform reviews of new and existing applications, protocols and solutions.

Cryptography advisory
Specific services:

- Providing end to end (managed) cryptographic services

Cyber Threat Intelligence (CTI)

Description

- Services focusing on assisting our clients to achieve operational security intelligence
- Can be provided in a fully managed way (via our CTI portal) or custom built for clients (on premise, or dedicated).

How can we help?

- Performance of social media scraping to identify security exposures;
- Design and deploy your own custom cyber threat intelligence solutions;
- Provide you with custom intelligence feeds;
- Addition of specific signatures and Indicators of Compromise (IOCs) which fit your environment.

Cyber Threat Intelligence (CTI)

Specific services:

- Cyber threat
- Security intelligence

Cyber simulation

- Hacking demos
- HackLAB training sessions
  - Hands-on
  - Demo edition
  - Malware
  - HackLab for kids
- Cyber simulation games
  - Hacking challenges
  - Capture the Flags (CTFs)
  - Red/Blue team exercises

For further information, please contact:

Ivan Spiteri
Senior Manager, IT Risk Advisory
ispiteri@deloitte.com.mt
T: +356 2343 2326

Bernard Farrugia
Manager, IT Risk Advisory
befarrugia@deloitte.com.mt
T: +356 2343 2325

www.deloitte.com/mt/riskadvisory

Deloitte.