COMPANY PROFILE

الخدمات المـدارة
MANAGED SERVICES

DEVELOPING A CULTURE OF CYBERSECURITY

BUSINESSES DEPENDS ON
TECHNOLOGY

1

IMPORTANCE OF CYBERSECURITY

In 2021, data breach costs have increased

TO USD **4.24** million

FROM USD **3.86** million

Cybercrimes cost organizations $ **2.9** / minute million

USD **1.07** million ↑ Due to COVID-19, the average cost of breaches caused by remote work was USD 1.07 million higher than those caused by no remote work.

USD **3.81** million ↓ With automation and security artificial intelligence (AI), organizations saved up to USD 3.81 million less than those without it.

BUSINESSES CHALLENGES

SHORTAGE OF CYBERSECURITY PROFESSIONALS.

EMPLOYEES' LACK OF CYBERSECURITY AWARENESS.

LACK OF EXPERIENCE IN CYBERSECURITY.

LACK OF RESOURCES DEDICATED TO CYBERSECURITY.

WHAT IS A MANAGED SERVICES PROVIDER?

Managed Services Provider (MSP) offer a combination of business services and technology to enable client businesses to:

Manage business activities efficiently and effectively.

Free up resources for other business needs.

WHY WORK WITH A MANAGED SERVICES PROVIDER (MSP)?

A short-handed Security Team

Limited Security Team Scalability and Readiness

Can't Justify Full-Time Employees For All Roles

MANAGED SERVICES COMPANY

When every business in the kingdom is **secure***, the kingdom itself is* **secure.**

MISSION

To serve the Kingdom with the best local, cutting-edge cybersecurity resources, putting the region on the map as the top cybersecurity hub.
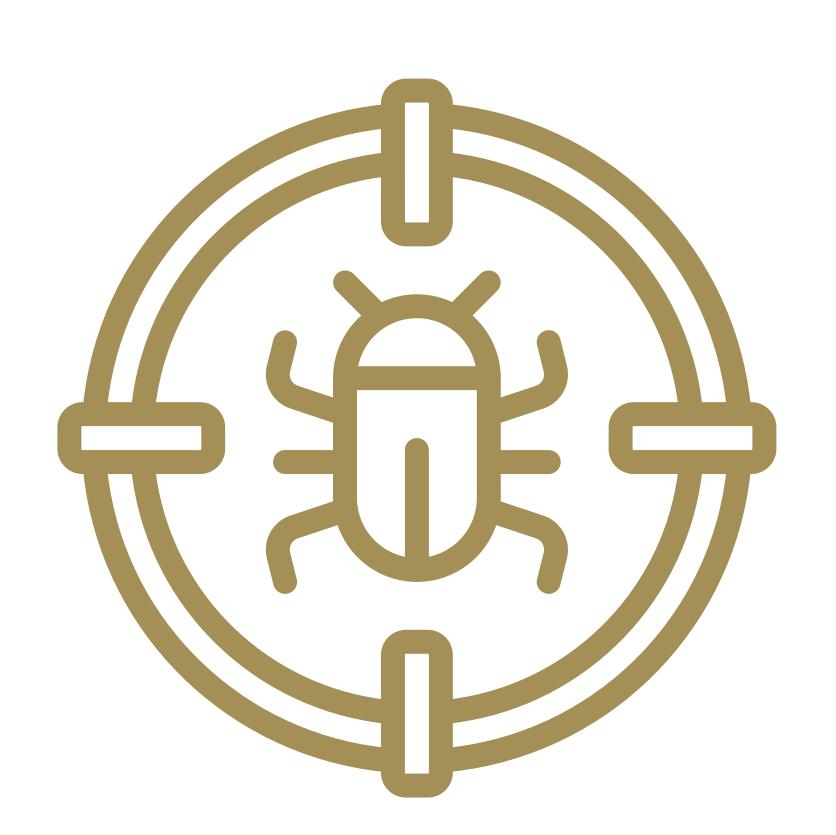
VISION

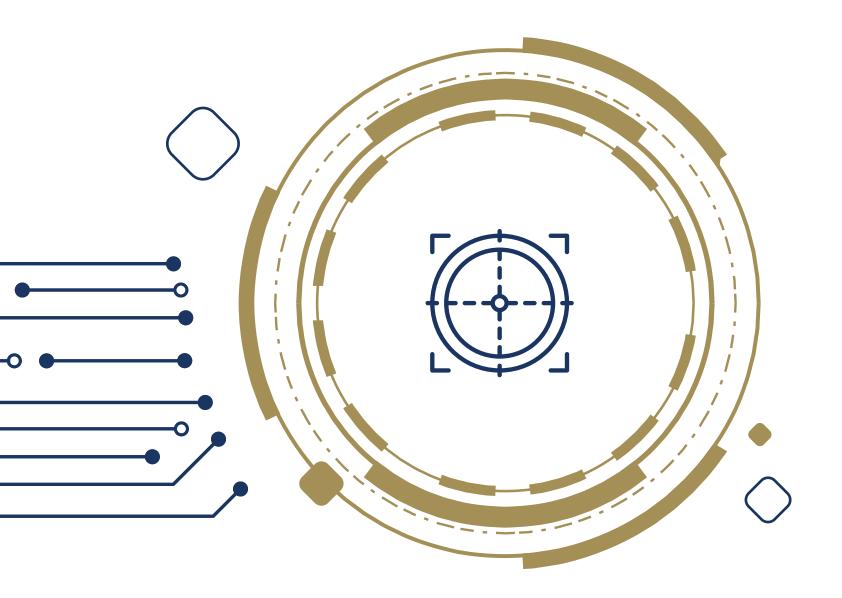We aim to be the most innovative and trusted cybersecurity leader in the Kingdom.

OUR SERVICES

SECURE

Managed Detection and Response

Human Threat Prevention

TRANSFORM

Compliance

Assurance

Digitalization

MANAGED DETECTION AND RESPONSE (MDR)

THE IMPORTANCE OF
MDR

A service that focuses on delivering a meaningful security outcome meant to ease both pre-breach and post-breach concerns and the ability to detect and respond to threats.

Providing 24/7 threat monitoring, detection and lightweight response services to customers leveraging a combination of technologies deployed at the host and network layers, advanced analytics, threat intelligence, and human expertise in incident investigation and response.

THREAT
HUNTING

MDR
SERVICES

THREAT
MANAGEMENT

THREAT HUNTING

A process of proactively searching through networks to detect and isolate advanced threats that evade existing security solutions.

KEY FEATURES AND BENEFITS:
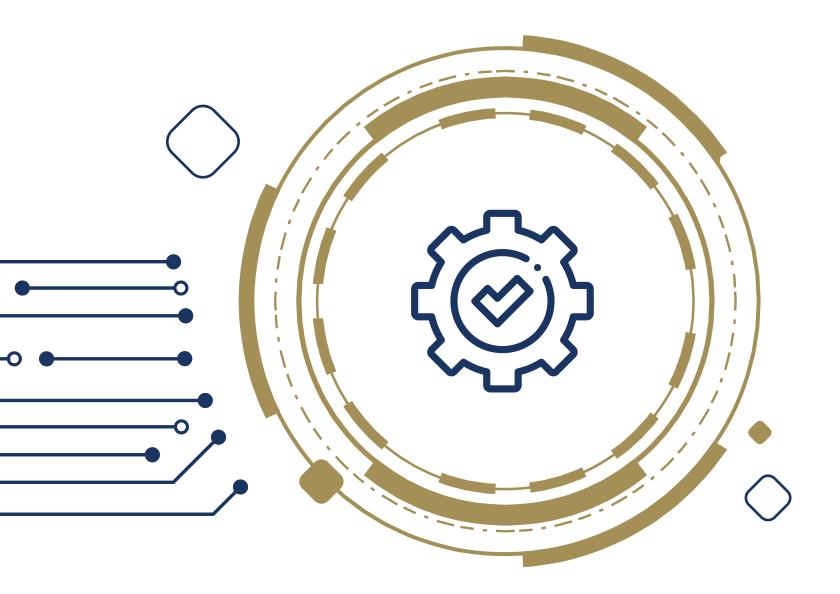
Focus efforts on unknown exploits by cyber-criminals.

Leverage deep knowledge and experience to identify attacks at early stage.

Combine the use of human talent and engineering to seek/hunt deficiencies.

ADDED-VALUE:

⊘ Feed the threat intelligence process with new threats and IOCs.

⊘ Identify threats faster and respond to them before damages occur.

⊘ Able to effectively filter out potential threats that need to be examined.

THREAT MANAGEMENT

A process used by cybersecurity professionals to prevent cyber attacks, detect cyber threats and respond to security incidents.
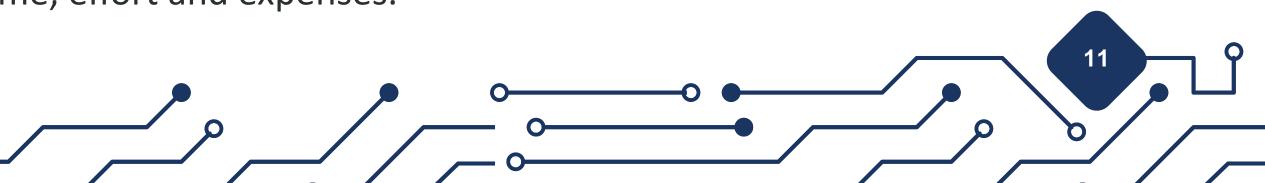
KEY FEATURES AND BENEFITS:

Identify and protect businesses most important assets and resources.

Detect and respond to cyber threats quickly and efficiently.

Correlate real-time threat detection results with global threat intelligence.

ADDED-VALUE:

⊘ Effectively prevent threats.

⊘ Rapidly detect breaches before damage occurs.

⊘ Respond comprehensively to incidents.

⊘ Proactively identify and respond to potential security issues.

⊘ Reduce time, effort and expenses.

HUMAN THREAT PREVENTION

THE IMPORTANCE OF
HUMAN THREAT PREVENTION

An awareness process to prevent intrusions, malwares and threats by enhancing the cybersecurity knowledge of employees.

- Complying with the local regulations.

- Improving overall cybersecurity awareness.

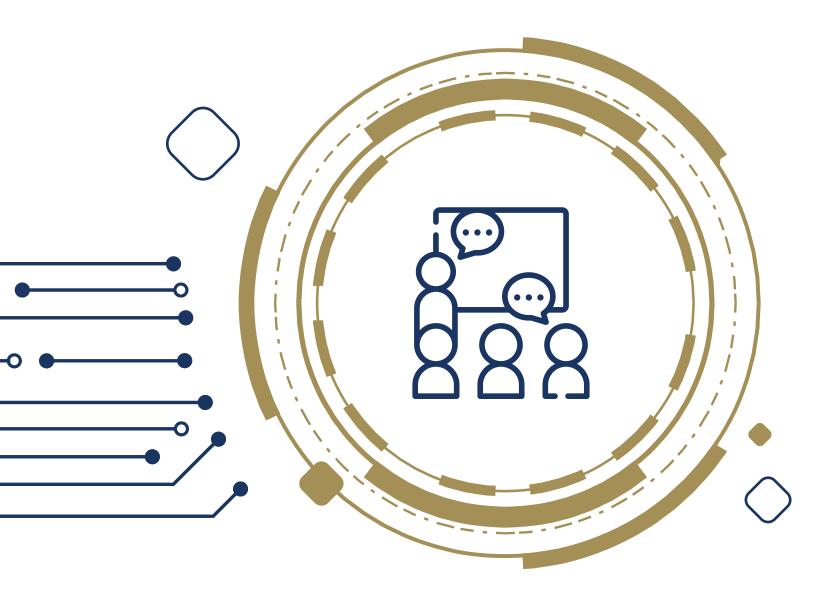- Protecting and defending your businesses' environment against cyber-threats.

THREAT PREVENTION
FOCUS-POINTS

The Privacy Act (Outline Responsibilities)

Document Handling and Classification Policies

Types of Threats

Phishing Attacks

The Dangers of Downloading Unofficial Files

Social Engineering

Best Practice Password Management

The Dangers of Installing Unofficial Apps and Programmes

Public Wi-Fi Hotspots (The Need for VPN Software)

Avoiding Insceure or Unverified Websites

Ongoing Vigilance

Social Media Posts (Do's and Don'ts)

HUMAN THREAT PREVENTION SERVICES

AWARENESS TRAINING

PHISHING SIMULATIONS

AWARENESS TRAINING

A strategy used by security professionals to improve cybersecurity awareness.

KEY FEATURES AND BENEFITS:

Mitigate the potential security risks caused by human errors.

Actively promote cybersecurity awareness programs amongst employees.
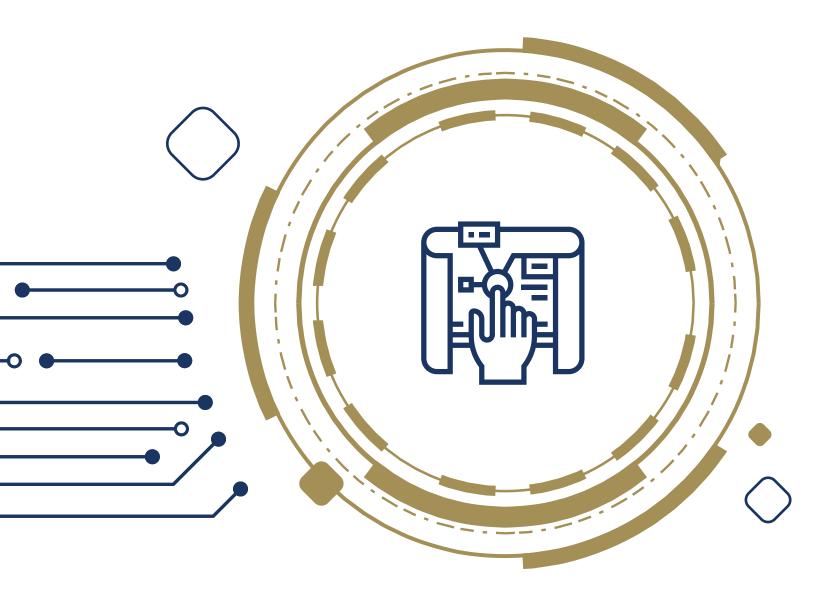
Validate organizations' cybersecurity policies and procedures.

Adapt employees' behaviors in relation to cyber-risks.

ADDED-VALUE:

- ⊘ Educate and empower employees against cyber-threats.

- ⊘ Protect reputation and secure overall business investments.

- ⊘ Ensure employees are up-to-date on the latest methods of various attacks.
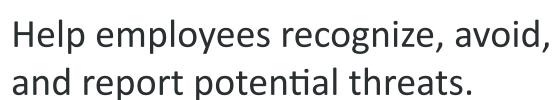
PHISHING SIMULATIONS

Apart of security awareness program that guards your business against social-engineering threats.

KEY FEATURES AND BENEFITS:

Help employees recognize, avoid, and report potential threats.

Test and measure employee vulnerability to the leading cause of data breaches.
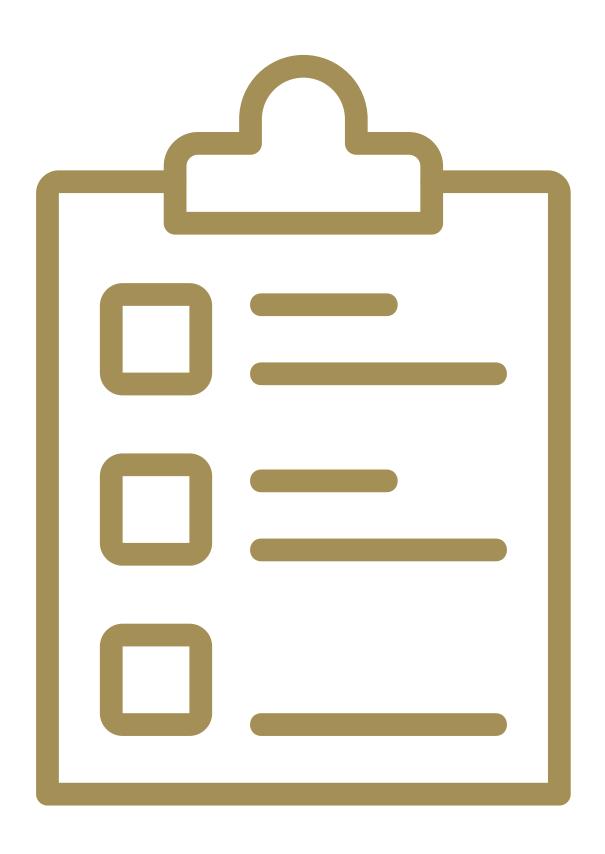
Deploy anti-phishing strategies and educate employees about cyber security.

ADDED-VALUE:

⊘ Ensure the resilience and alertness of employees against phishing risks.

⊘ Measure the vulnerability degrees of corporate and employees.

⊘ Decrease security risks of organizations due to social engineering attacks.

COMPLIANCE
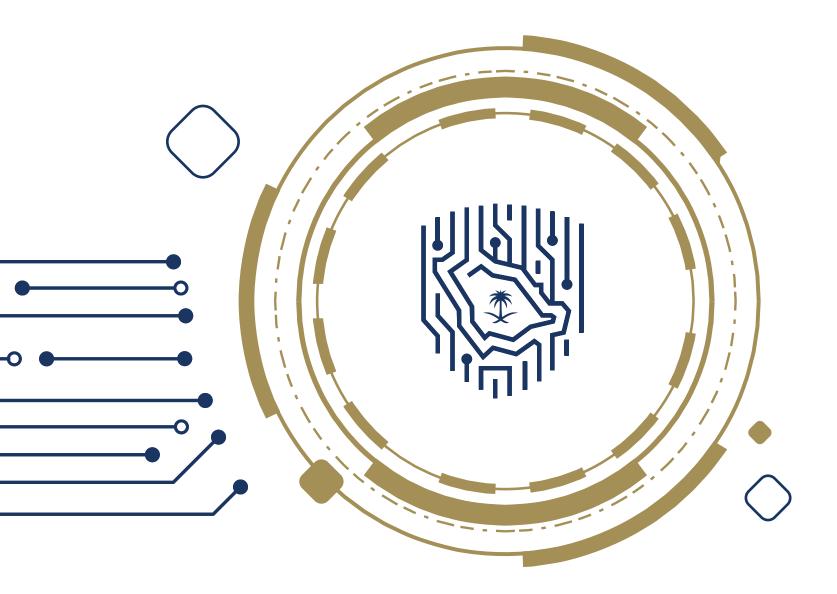
THE IMPORTANCE OF
COMPLIANCE

Ensure organization's security posture is aligned with regulators' standards by implementing compliance controls customized to your business environment.

- Comply with the standard regulations.

- Reduce legal issues.

- Reduce business risks.

- Maintain a solid reputation.

COMPLIANCE SERVICES

NCA COMPLIANCE

SAUDI ARAMCO COMPLIANCE

ISO27001

NCA COMPLIANCE

OFFERED SERVICES:

1.

Conduct gap Assessment against NCA Essential Cybersecurity Controls (ECC) regulatory framework.

2.

Design and Implement cyber security practice against NCA ECC framework.

3.

Review and Improve existing cyber security controls against the NCA ECC framework.

4.

Develop cybersecurity policy roadmap and procedures for the NCA ECC compliance requirements.

5.

Conduct independent audit of existing cybersecurity posture against NCA ECC regulatory framework.

ADDED-VALUE:

- ⊘ Determine the current security posture.
- ⊘ Comply with the NCA regulations.
- ⊘ Protect IT system and infrastructure against Attacks.
- ⊘ Establish a roadmap for compliance.

SAUDI ARAMCO COMPLIANCE

OFFERED SERVICES:

1.

Conduct CCC and CCC+ assessments to ensure compliance with the applicable controls under the client's classification.

2.

Provide guidance to the client prior to the assessment.

3.

Assist the client through the assessment process.

ADDED-VALUE:

⊘ Qualified to conduct business or register with Saudi Aramco.

⊘ Obtain Aramco Cybersecurity Compliance Certificate / Cybersecurity Compliance Certificate Plus.

⊘ Ensure company's adherence to the cybersecurity requirements in the Third-Party Cybersecurity Standard (SACS-002)

ISO27001

OFFERED SERVICES:

1.
Information Security
Management System (ISMS)

2.
Risk Assessment

3.
ISMS Gap Assessment

4.
Security Controls
Gap Assessment

5.
Security Metrics

6.
Gap Remediation
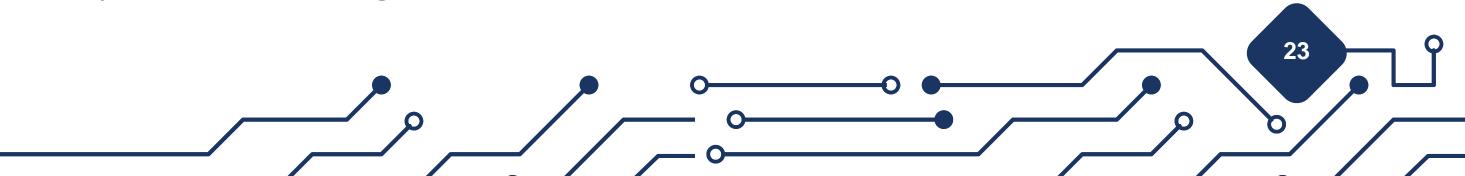Facilitation/Support

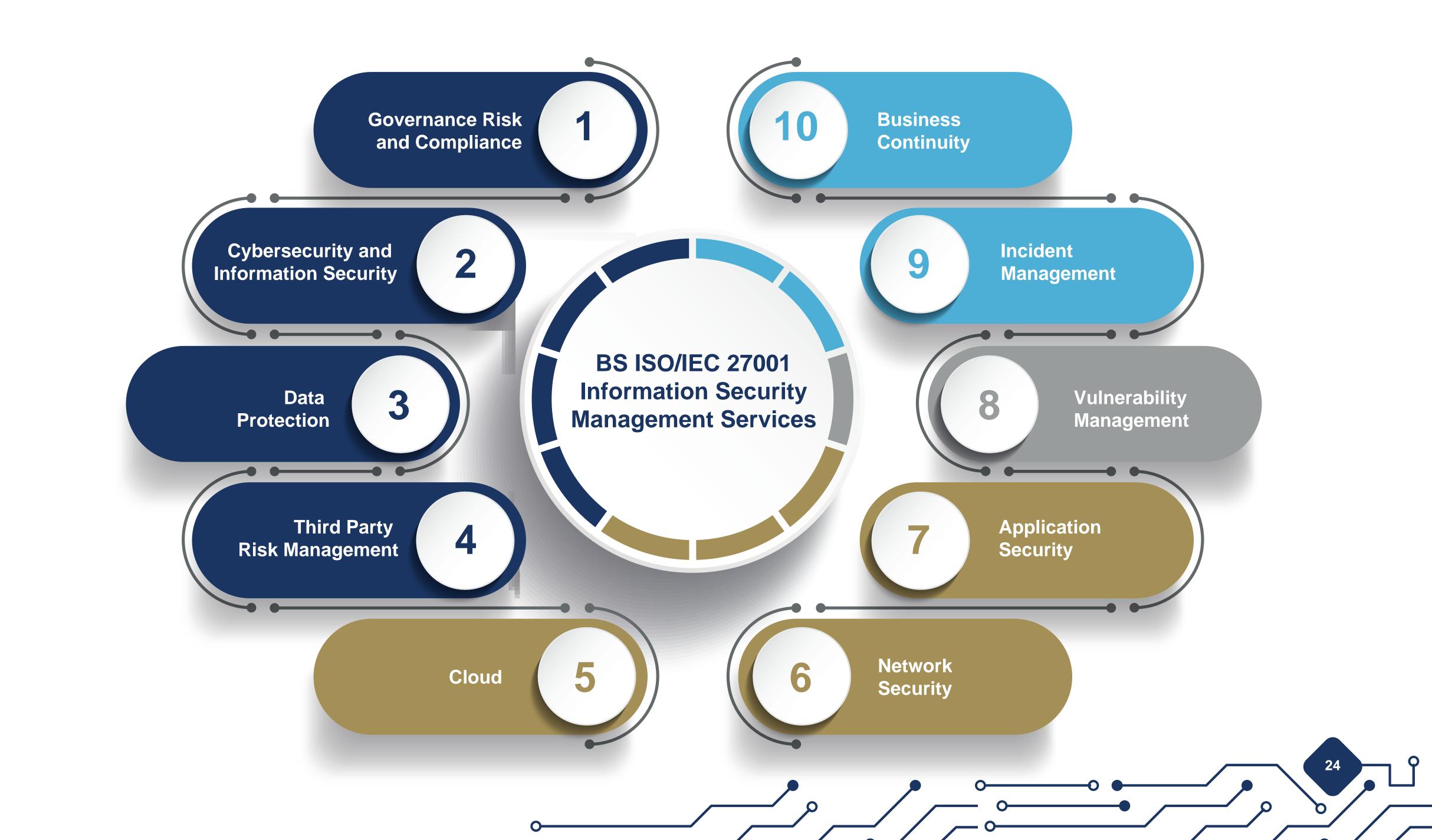**7.**
Prioritized Roadmap
Definition

8.
Policy, Standards, &
Procedure Support

ADDED-VALUE:

⊘ Increase reliability and security of systems and information

⊘ Improve customer and business partner confidence

⊘ Enhance management processes and integration with
corporate risk strategies

ASSURANCE

THE IMPORTANCE OF
ASSURANCE

A service with the goal of improving information so that decision makers can make more informed, and presumably better, decisions.

Assurance services assesses organization's cybersecurity posture and tests vulnerabilities, to point out improvements and create a comprehensive plan that helps you reduce potential breaches.

PENETRATION
TESTING

ASSURANCE
SERVICES

VULNERABILITY
ASSESSMENT

PENETRATION TESTING

A technique of ethical hacking where our team of experts interrogate your systems to identify the vulnerabilities that can cause cyber-attacks.

KEY FEATURES AND BENEFITS:

Complete view of vulnerabilities and remediation prioritization.

Secure your business against internal and external threats.

Independently validate your organization's security posture and processes against industry best practices.
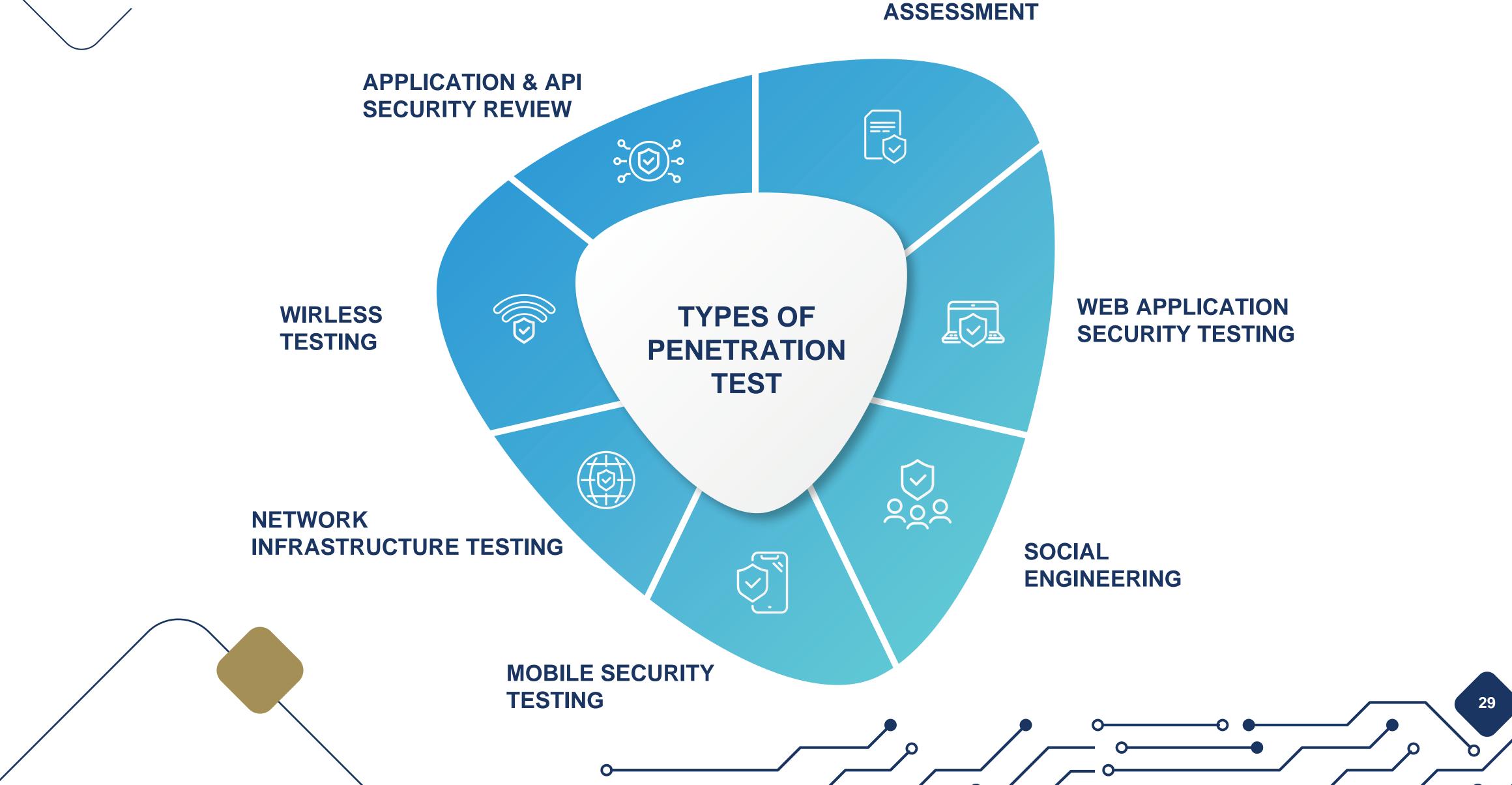
Provide feedback on vulnerabilities to development teams to drive improvements in secure coding practices.
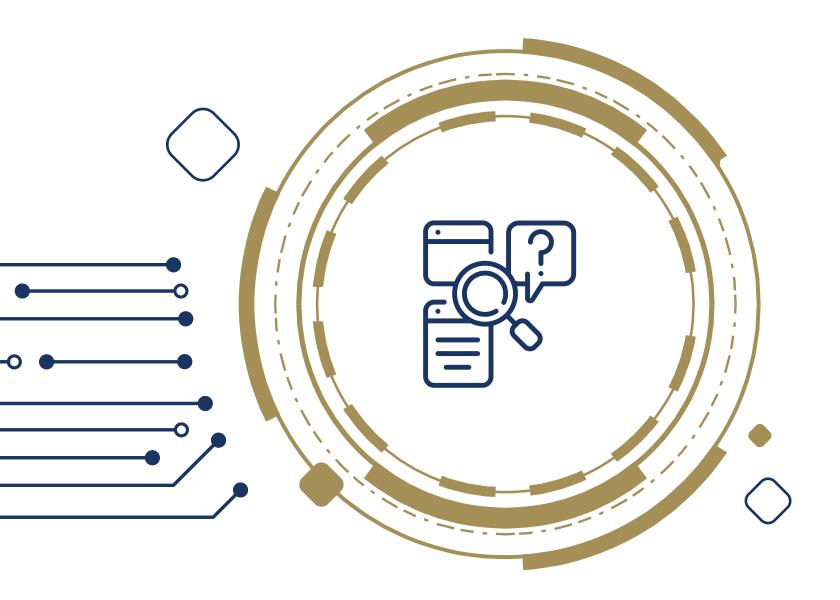
ADDED-VALUE:

⊘ Avoid business disruptions, escalating costs, legal ramifications, and reputational damages.

⊘ Comply with regulatory security controls requirements.

⊘ Build a solid trust with clients and partners.

VULNERABILITY ASSESSMENT

Manual evaluation and automated scanning of your IT infrastructure or its components to detect security vulnerabilities.

KEY FEATURES AND BENEFITS:

Identify, quantify, and analyze security vulnerabilities in the IT infrastructure and applications.

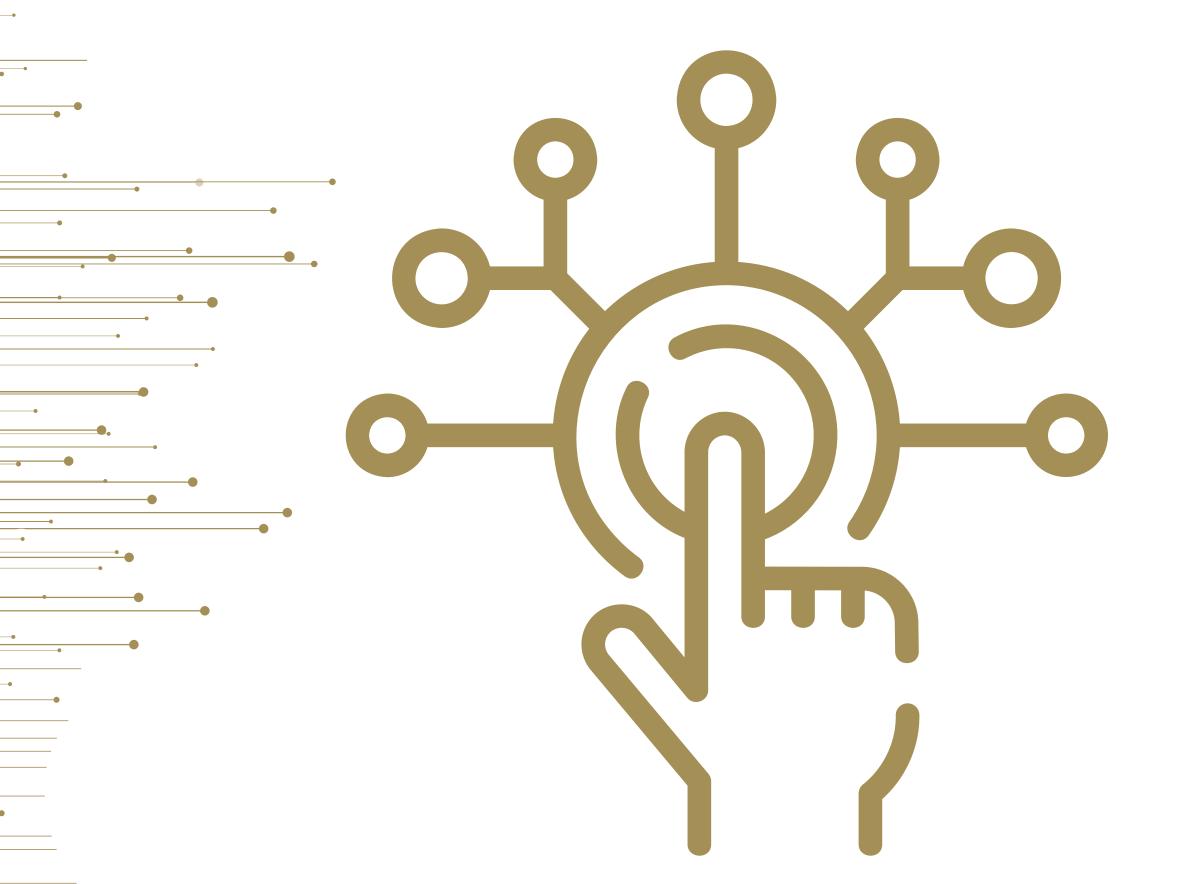Provide recommendations on how to mitigate the detected vulnerabilities.

Validate vulnerability management activities are in-line with the best practices

ADDED-VALUE:

⊘ Provide strategic advice through recommendations that will help you to secure your organization.

⊘ Secure sensitive and confidential data.

⊘ Define the level of risk that exits within IT posture.

DIGITALIZATION

THE IMPORTANCE OF
DIGITALIZATION

Digitalization offers opportunities to rebuild your business around the customer to create a truly connected and highly profitable enterprise.

The optimization of business process using latest cutting-edge technology by

- Improving the efficiency of business processes, consistency, and quality.

- Improving accessibility and facilitate better information exchange.

- Increasing response time and customer experience.

- Enhancing employee productivity and operational controls.

- Balanced investment in terms of costs and increased performance.
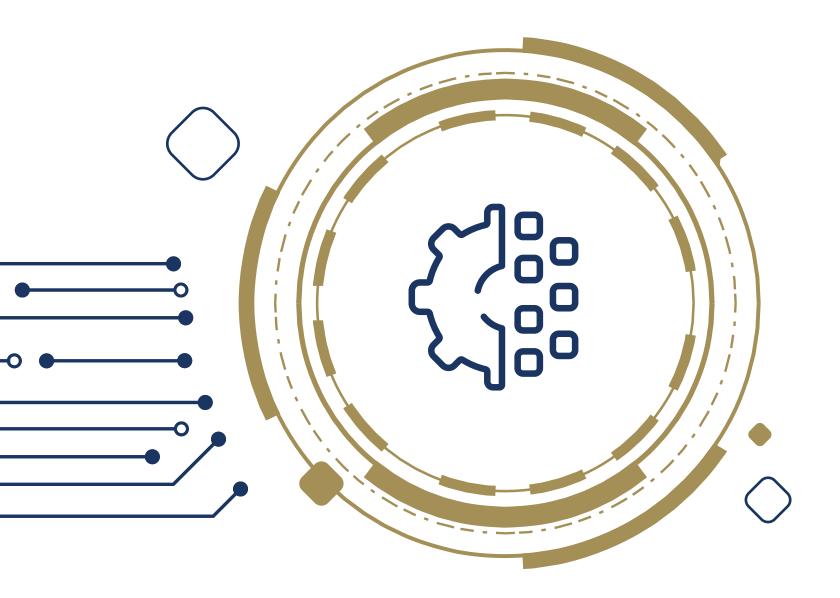
DIGITALIZATION SERVICES

DIGITAL TRANSFORMATION SERVICES

OFFICE AUTOMATION

BUSINESS INTELLIGENCE

DIGITAL TRANSFORMATION SERVICES

Services aim to develop and implement right strategy for successful digital transformation.

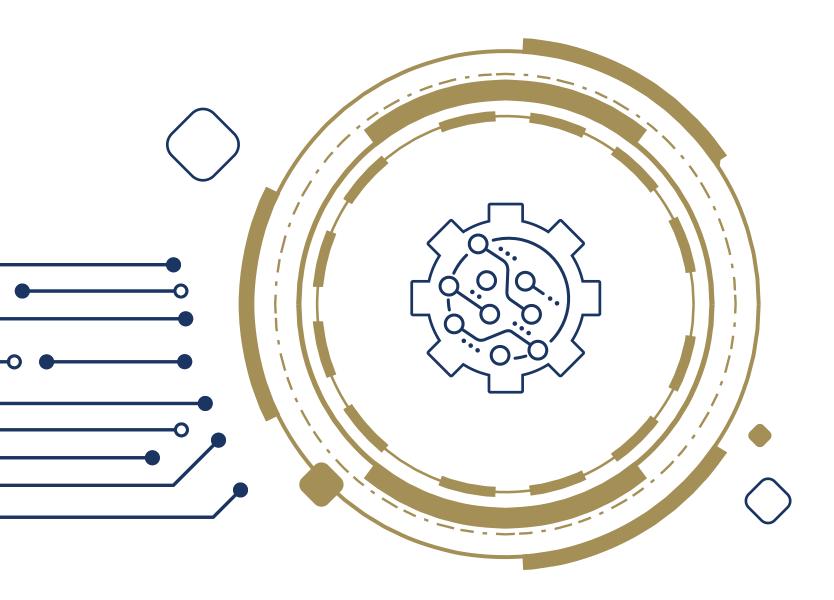## KEY FEATURES AND BENEFITS:

In-depth business discovery

Eliminate missed opportunities

Provide direction

ADDED-VALUE:

- ⊘ Selection of right technology
- ⊘ Successful implementation and execution
- ⊘ Clear path to strategic goals
- ⊘ Digital Differentiation

OFFICE AUTOMATION

An approach to increase the business efficiencies using digital channels.

KEY FEATURES AND BENEFITS:

Enhance customers' experience.

Ensure speedy recording, processing and presenting of information.

Take advantage of analytics & real user data.

Integrate records or files into a digitalized form and eliminating redundancies.

ADDED-VALUE:

⊘ Enhance business productivity.

⊘ Improve performance accuracy and efficiency.

⊘ Reduce operational cost.

⊘ Prevent human error.

Microsoft Automation Platforms

MICROSOFT OFFICE 365	DYNAMICS365	COLLABORATION SERVICES	POWERAPPS
Microsoft Office Products (Office, Email, Security Licenses, Directory Services, and Teams)	MS Dynamics Business Central (ERP Solution)	Collaboration Services (SharePoint)	Internal Organization Websites Model Driven Apps
Configuration & Migration	Customized ERP for Clients Requirements	Teams Meeting Rooms	Power BI Reports/Dashboards
		Office Project Management	Marketplace PowerApps

BUSINESS INTELLIGENCE (BI)

Business intelligence enable organization to see their raw data into actionable insights to drive their decisions.

KEY FEATURES AND BENEFITS:

Easily visualize and understand company data.

Encourage data-driven decision making for business optimization.

Discover new insights that can enhance the bottom line.

ADDED-VALUE:

⊘ Data-driven decision-making to optimize and achieve full potential of the business.

⊘ Measure and understand company performance.

⊘ Discover new actionable insights.

DIGITALIZATION STATISTICS

Companies that have higher digital maturity reported

40%

Digital technologies accelerate progress towards enterprise goals by

24%

Meeting Customer Expectations by

72%

45%

Revenue Growth

Improvement of Operational Efficiency

22%

of companies reach significant decisions and strategies through digital transformation.

35%

of businesses have reached very effective responses by adapting digital technologies during COVID-19.

OUR
PARTNERS

CONTACT US

MANAGED SERVICES

📍 3227 Anas Ibn Malik - Al Sahafah Dist.
Riyadh 13321 - 8347
Kingdom of Saudi Arabia

📱 +966 11 4185222

✉️ sales@managed.sa

🌐 www.Managed.sa

in 🐦 ManagedSA