myCloudDoor

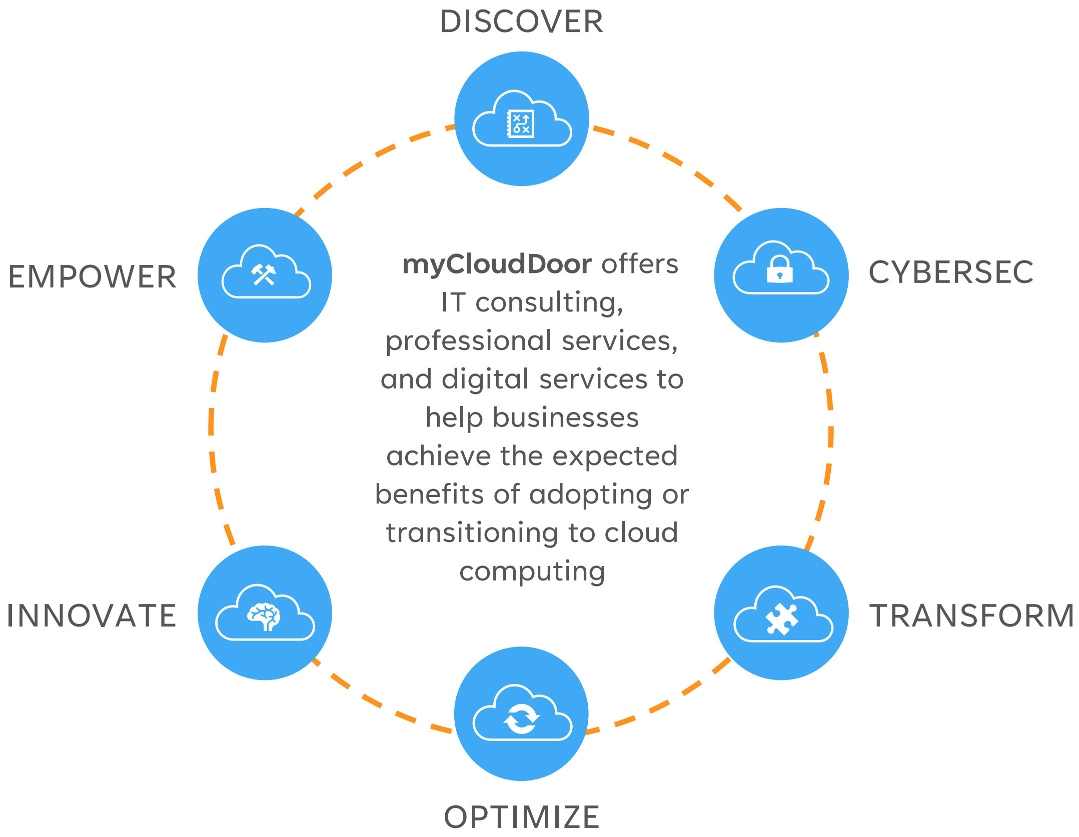
Cybersecurity & Innovation

- **myCloudDoor**
  - Value Proposal
  - Microsoft Alliance
  - Offices
  - Security Services Portfolio
- **Cloud Security Posture Assessment**
  - Current Situation
  - NIST Framework
  - Service Description
  - Key Points
  - Benefits
  - Methodology
  - Planning
  - Work Team
  - Deliverables

my
Cloud
Door

mycloudDoor

Value Proposal: The **most** cyber-secure journey to the cloud



DISCOVER

CYBERSEC

TRANSFORM

OPTIMIZE

INNOVATE

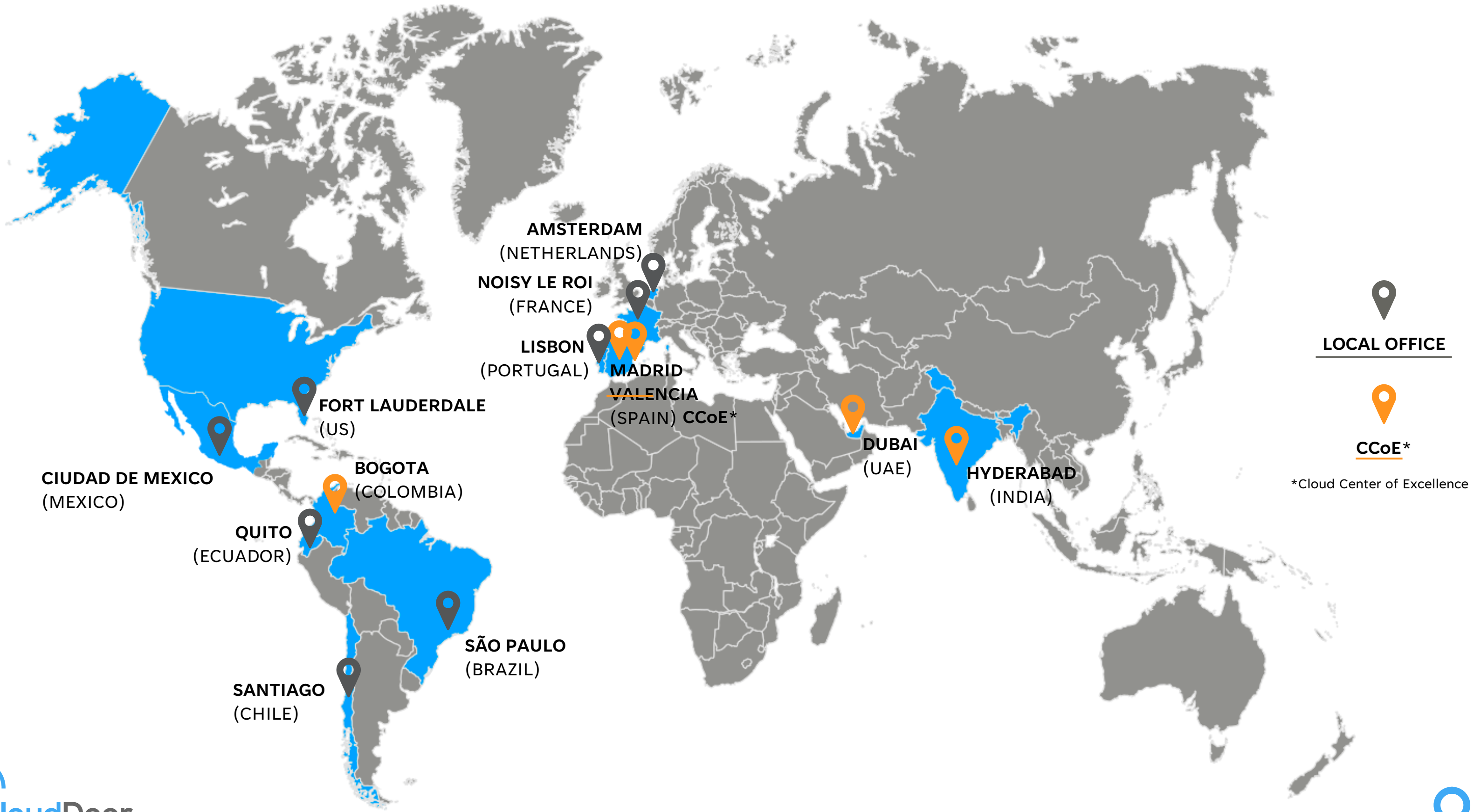
EMPOWER

myCloudDoor offers IT consulting, professional services, and digital services to help businesses achieve the expected benefits of adopting or transitioning to cloud computing

myCloudDoor Cloud Journey – **Our Services**

DISCOVER	CYBERSEC	TRANSFORM	OPTIMIZE	INNOVATE	EMPOWER
CLOUD ADOPTION ROADMAP	CYBER RISK & RESILIENCE ADVISORY	CLOUD MIGRATION	MANAGED CLOUD SERVICES	ARTIFICIAL INTELLIGENCE	BUSINESS APPS
CLOUD, DATA & CYBERSECURITY STRATEGY	SECURITY & PRIVACY COMPLIANCE	CLOUD SECDEVOPS	SOC & MANAGED XDR	DATA PLATFORM & DATA ENGINEERING	MODERN APPLICATIONS
CLOUD MODERNIZATION ASSESSMENT	PREVENTION AND PROTECTIVE TECHNOLOGIES	MULTICLOUD AND HYBRID ARCHITECTURES	MANAGED SAP BASIS SERVICES	ADVANCED DATA ANALYTICS	EXTENDED SAP ON CLOUD
CLOUD, DATA & CYBERSECURITY GOVERNANCE	THREAT INTELLIGENCE & CYBEROPERATIONS	SAP ON CLOUD	FINOPS	SYSTEMS 4.0	AUTOMATION & RPA

myCloudDoor Offices

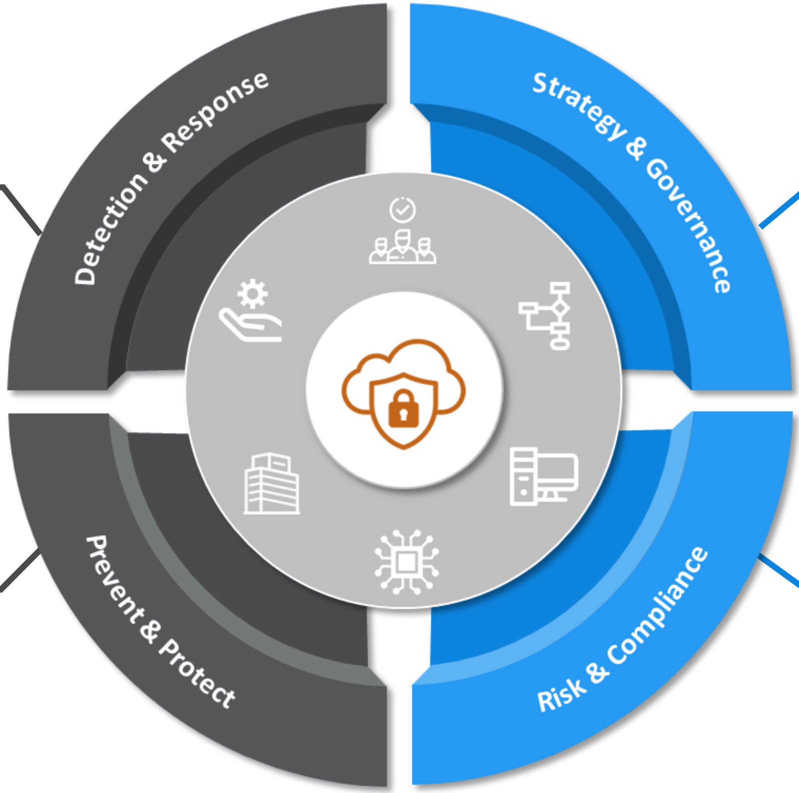


myCloudDoor: Global Portfolio of Cybersecurity Services

Cybersecurity strategy, a pillar of digital transformation

myCloudDoor SOC 24x7x365

- MANAGED DETECTION & RESPONSE
- DIGITAL FORENSICS
- DIGITAL SURVEILLANCE
- THREAT HUNTING
- SECURITY OPERATIONS



- DASHBOARD CYBERSECURITY RATING
- CYBERSECURITY MASTER PROGRAM
- CISO & DPO AS A SERVICE
- INFORMATION SECURITY OFFICE
- CYBERSECURITY CULTURE

- VULNERABILITY MANAGEMENT (AVM)
- PENTESTING & RED TEAM
- DIGITAL IDENTITY & ACCESS
- PROTECTIVE TECHNOLOGIES
- DATA PROTECTION

- NIST, SOC II, ISO 27001, DORA, ENS
- RISK MITIGATION SERVICES
- CLOUD SECURITY ASSESSMENT (CSPM)
- CYBER RESILIENCE (BCP, DRP)
- PRIVACY CONSULTING (GDPR)

my
Cloud
Door

Cloud Security Posture Assessment

Cybersecurity: Current situation

What is happening?

Threat Detection

200 days to detect a security incident.

Cloud Access Vector

Use of stolen credentials is the initial access vector in **36%** of cloud incidents but, email and the human factor are used in almost 100% of cases.

Response

77% of companies do not have a response plan for disruptive incidents affecting business processes.

Ransomware

66% of companies report having suffered a ransomware attack. The triple extortion technique is increasingly used.

Source: Verizon Data Breach Investigations Report

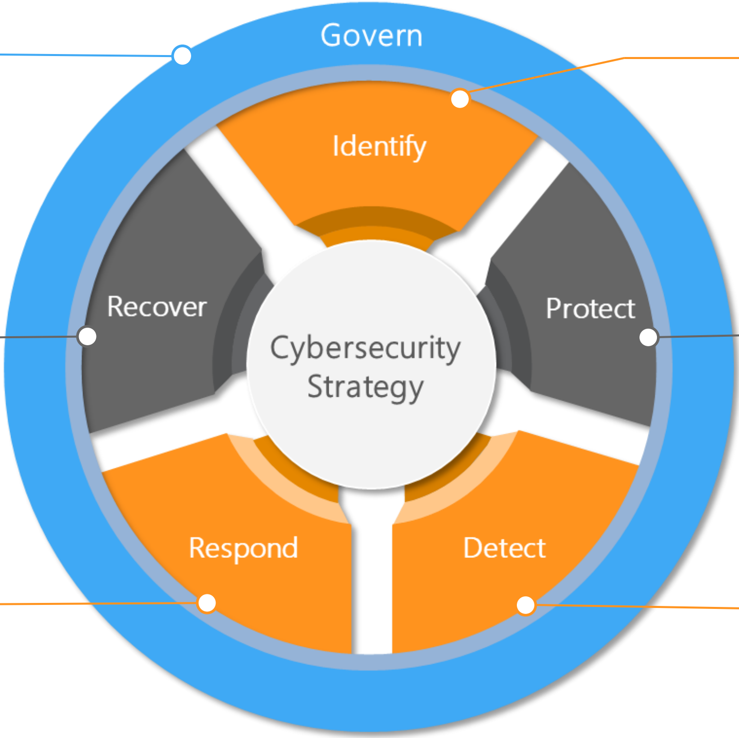
myCloudDoor: Journey to Cyber Resiliency

CyberRisk Management: the key to protecting business processes

Governance must establish cybersecurity policies, procedures and standards.

Improve organizational resilience and recover business processes in the event of an attack.

Responding to cybersecurity incidents to **minimize business impact.**



The starting point is to **identify the critical assets** that need to be protected.

Protect critical assets and their dependencies **based on the risk** to which they are exposed to.

Detect possible cybersecurity intrusions in a **24x7 model**.

myCloudDoor

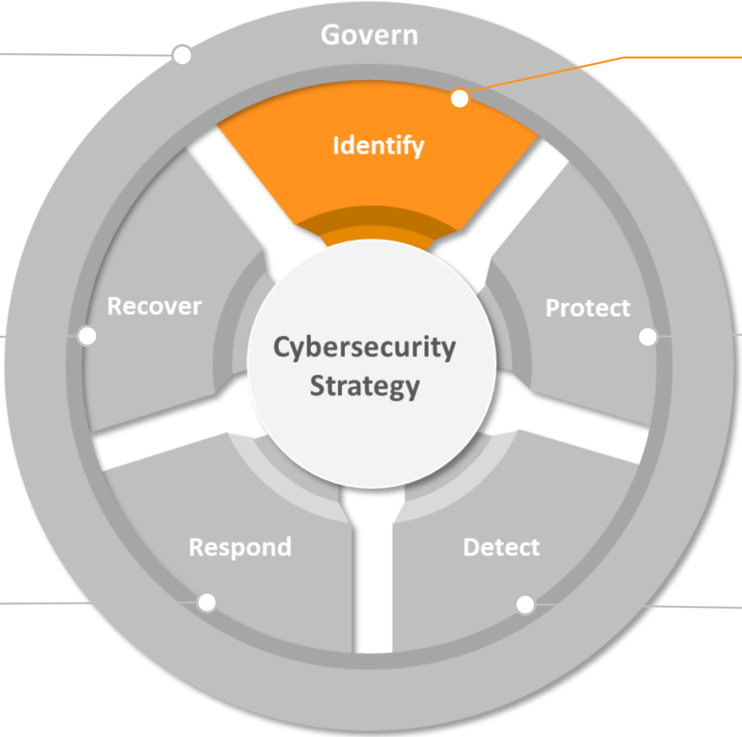
Journey to Cyber Resiliency

CyberRisk Management: The Key to Securing Business Processes

Governance must establish cybersecurity policies, procedures and standards.

Improve organizational resilience and recover business processes in the event of an attack.

Responding to cybersecurity incidents to minimize business impact.



Cloud Security Posture Assessment

The starting point is to identify the critical assets that need to be protected.

Protect critical assets and their dependencies based on the risk to which they are exposed to.

Detect possible cybersecurity incidents in a 24x7 model.

Service Description

What is the Cloud Security Posture Assessment service?

The cloud security posture assessment service in Azure is a set of practices and tools used to analyze and assess the security of a cloud infrastructure that utilizes Microsoft Azure services and resources. The purpose of this service is to identify and mitigate security risks, weaknesses, vulnerabilities, and misconfigurations that could compromise the security of data and applications hosted in Azure.

Key Points

The main key aspects of the Cloud Security Posture Assessment

1

Microsoft Defender CSPM

Configuration and deploy Microsoft Defender CSPM on Azure Tenant.

2

Microsoft Defender for Servers

Configuration and deploy Microsoft Defender for Servers on servers. This includes the installation of agents and configuration of security policies.

3

Security Policy Creation

Define security policies that specify the required configurations and behaviours for the servers and cloud. These policies should comply with security best practices and regulations.

4

Vulnerability Scanning

Using the capabilities of Microsoft Defender for Servers and Microsoft Defender CSPM, perform vulnerability scans on servers and cloud environment and Identify security weaknesses

5

Cloud and Server Configuration Analysis

Monitor and evaluate the security configuration of the cloud and servers, verifying that the defined policies are being complied with and that there are no insecure configurations.

6

Access Controls Assessment

Analyse server access controls to ensure that they are properly configured. This includes authentication, authorization and password policies.

7

Reporting

Creating periodic reports summarizing the security posture of servers, including details on vulnerabilities, detected threats and policy compliance.

8

Results Report

Creation and presentation of a final report outlining the threats and findings presented that may pose a cybersecurity risk to the organization.

myCloudDoor

Benefits

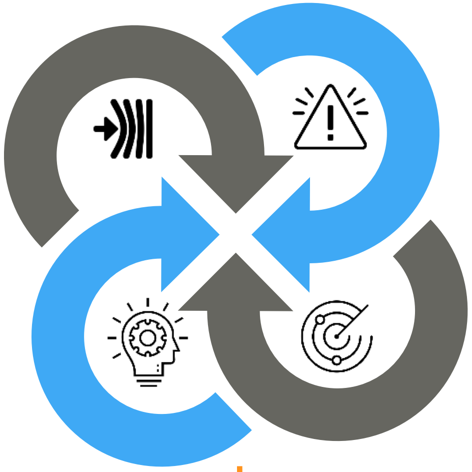
The main benefits of security assessment for Azure Cloud environments

Vulnerabilities and Weaknesses

Detect and document potential vulnerabilities and weaknesses in the security configuration of cloud resources. This includes identifying misconfigurations or insecure configurations that could expose the organization to security risks.

Compliance

Verify that the cloud resources complies with applicable security and privacy regulations and standards.



Security Posture Enhancement

Implement enhancements and fixes to strengthen the cloud security posture and ensure it is aligned with security best practices.

Risk Reduction

Minimizing security risks associated with misconfiguration of cloud resources, including mitigating potential threats.

Business Resilience: Increase the organization's resilience by assessing and improving its ability to withstand and recover from security incidents and disasters.

Methodology

Frameworks and standards used for the methodology of the assessment

NIST

The National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity is a widely recognized security framework used to improve cybersecurity within organizations.

CIS

Center for Internet Security (CIS) is the standard of best practices for the security of most operating systems and applications used in the market and can therefore offer the best recommendations for vulnerability mitigation.

ISO 27001

The international standard ISO/IEC 27001 establishes a framework for information security management.

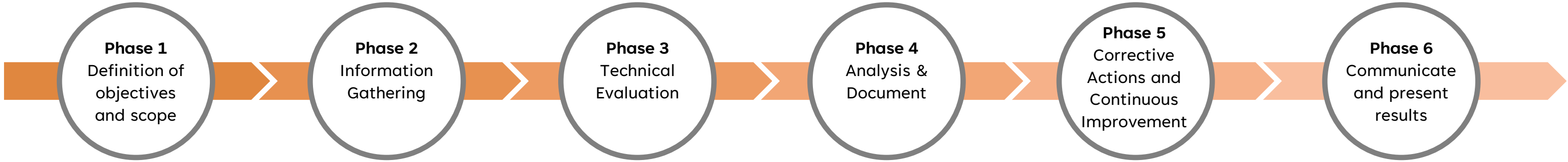
C. CRITERIA

The Common Criteria are an international standard for the security assessment of information technology products and systems. Microsoft Security Benchmark incorporates elements of Common Criteria to ensure the security of Microsoft products and services.

Cloud Security Posture Assessment Planning

Phases and activities

Week 1	Week 2	Week 3	Last Day
Kick-off meeting	Assessment Tools. Deploy and configure Microsoft Defender CSPM and Microsoft Defender for Servers	Analyze the results of the technical assessment to identify weaknesses and threats	Communicate the results of the evaluation to stakeholders
Preparation of documentation for the start	Vulnerability Scanning	Classify and prioritize the identified issues	Make a detailed presentation of the results and recommendations
Review and compile documentation	Configuration Analysis	Create detailed reports summarizing the assessment results, recommendations, and necessary corrective actions.	
Validate tool access	Threat Detection	Document a continuous improvement plan	
Staff Interviews			



Phase 1 Definition of objectives and scope

Phase 2 Information Gathering

Phase 3 Technical Evaluation

Phase 4 Analysis & Document

Phase 5 Corrective Actions and Continuous Improvement

Phase 6 Communicate and present results

Work Team

Proposed working team for the audit exercise

Cybersecurity Project Manager

Computer Systems Engineering

- Prince2 Practicioner
- ITIL Expert 2011
- SC-200 / SC-400
- ISACA CDPSE
- AZ-500 / MS-500

+15 years of experience managing cybersecurity services and projects:

- Sothis
- HP
- Americas Cup Mgmt

Cybersecurity projects in:

- Mercadona
- Cajamar
- Allianz
- Cosentino
- RTVE
- Europastry

Auditor Senior

Bachelor's Degree in Computer Engineering

- EC-Council CEH
- SC-200 / AZ-500
- CPHE_2022
- LISA Cyberintel.

+5 years of experience as an auditor:

- Sothis
- Nunsys
- Grupo Palacios

Audit cybersecurity projects in:

- Mercadona
- CESCE
- RTVE
- Ayto. Zaragoza
- Port de Barcelona
- IMED
- B2B Salud
- Vintegris

Deliverables

Crucial deliverables for communicating findings and recommendations to stakeholders

Executive Report

Executive summary intended for the leaders of the organization. Provides an overview of the audit results, highlighting key findings and critical areas of focus.

Detailed White Paper

A whitepaper that provides specific details about the current configuration, test results, and analysis of audit logs. Include detailed information about each area assessed. In addition, a detailed list of the audit findings

Risk Matrix

A matrix that classifies identified risks according to their impact and likelihood. This helps prioritize corrective actions and allocate resources effectively.

Corrective Action Plan

A detailed plan that outlines the specific actions the organization should take to address the audit findings. Include timelines, responsibilities, and follow-up actions. Clear and specific recommendations to address each of the identified findings

Q&A

my
Cloud
Door

myCloudDoor

Creating future

THANK YOU

info@myclouddoor.com

FORT LAUDERDALE (US) · MADRID (SE) · VALENCIA (SE) · AMSTERDAM (WE) · SANTIAGO DE CHILE (LATAM) · DUBAI (MEA)