myCloudDoor

Cybersecurity & Innovation

+500 IT

YEARS ACUMULATED IN CONSULTING

10

OFFICES

AMERICAS-EMEA

12

STRATEGIC ALLIANCES / PARTNERS

7 IP

SOLUTIONS

Cloud instant

my Cloud MAS+

smart Cloud Migrations

my Cloud DBM

40%

more AGILE & deployment cost reduction

my Cloud Door

300 %

YOY

4

CLOUD AREAS

CONSULTING

MANAGED

ANALYTICS

PROJECTS

+ 100

CLIENTS

+10 MM €

IN CLOUD BUSINESS

COMPETENCIES

12

GOLD CLOUD PLATFORM

GOLD DATACENTER

GOLD DATA PLATFORM

GOLD DATA ANALYTICS

GOLD DEVOPS

GOLD APPLICATION DEVELOPMENT

GOLD APPLICATION INTEGRATION

GOLD CLOUD PRODUCTIVITY

SILVER MESSAGING

SILVER COLLABORATION AND CONTENT

SILVER SECURITY

SILVER SMALL AND MIDMARKET CLOUD SOLUTIONS

80%

CERTIFIED CONSULTANTS

TOP 3

COMPANIES

★★★★★

SAP on Azure LeaderShip

my
Cloud
Door

Microsoft 365 Security Assessment

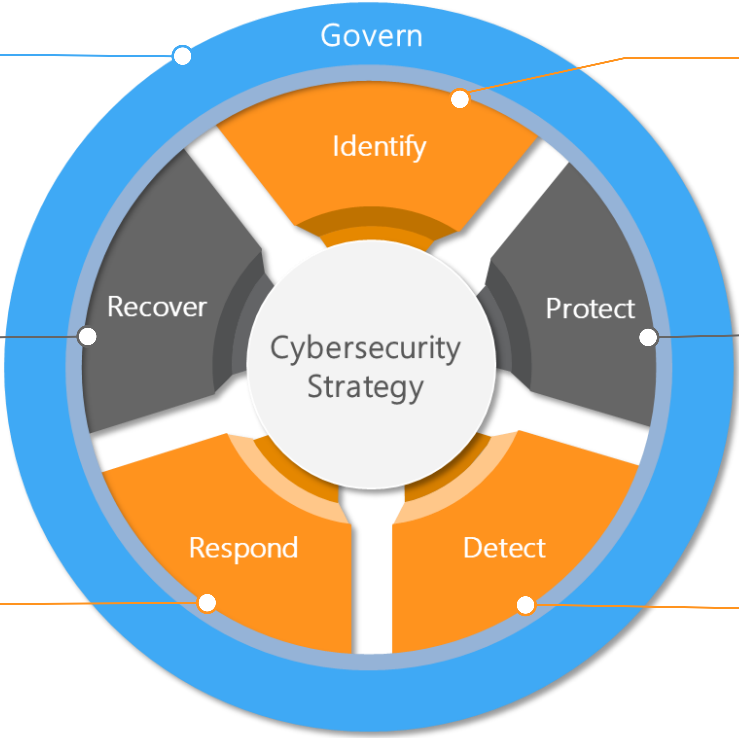
myCloudDoor: Journey to Cyber Resiliency

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** to be protected.

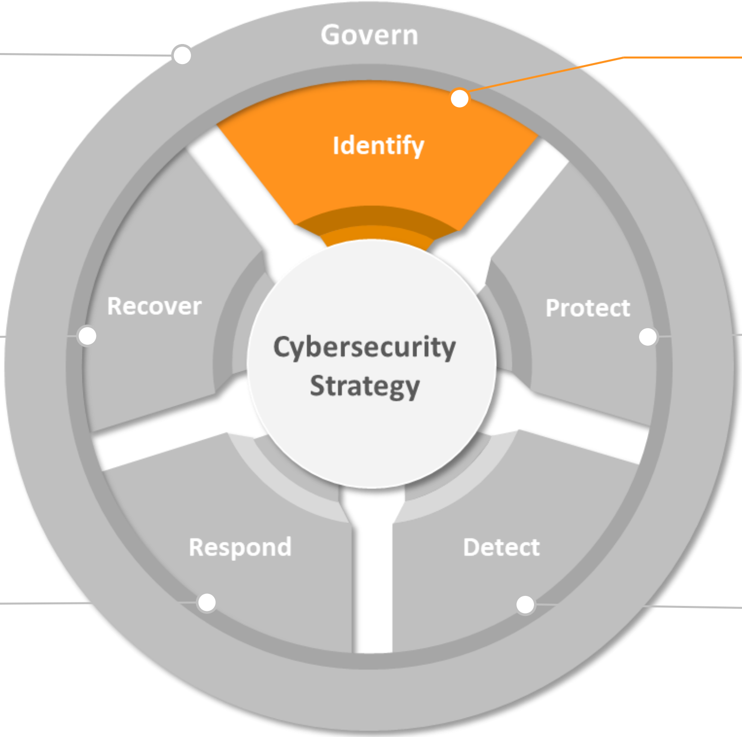
Protect critical assets **based on the risk** they are exposed to

Detect possible cybersecurity intrusions on a **24x7 basis**.

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.

Respond to potential security incidents while minimizing the potential impact.

M365 Security 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

Detect possible cybersecurity incidents in a 24x7 model.

Service Description

What is the Microsoft 365 security assessment service?

The Microsoft 365 environment security assessment service, offered by **myCloudDoor's** team of cybersecurity auditors and consultants, aims to assess risks and improve security in a Microsoft 365-based environment. This service focuses on reviewing security settings, policies, and practices across the suite of services and apps that are part of Microsoft 365.

myCloudDoor

Key Points

The main key aspects of the Microsoft 365 security assessment

1 Configuration and Policies

Security auditors review security settings in Microsoft 365, including security policies, identity settings, user permissions, and configurations for individual services such as Exchange Online, SharePoint, OneDrive, Teams, and more.

2 Audit Log Analysis

A detailed analysis of the audit logs of the different Microsoft 365 services is carried out. This involves identifying relevant security events, tracking user activities, and detecting potential threats.

3 Threat Protection Assessment

The security measures implemented to protect the environment against threats such as malware, phishing, brute force attacks, etc. are evaluated. This includes reviewing solutions such as Microsoft Defender for Endpoint, Microsoft Defender for Office 365, among others.

4 Identity and Access Auditing

An audit of identity management is performed, reviewing password synchronization, role and permissions management, and multi-factor authentication (MFA) settings.

5 Regulatory Compliance Practices

It verifies that the configuration complies with the regulatory and legal requirements applicable to the organization, ensuring that compliance with specific regulations is maintained.

6 Device Management & Remote Access

Device management and remote access policies are evaluated to ensure that devices are secure and access to resources is done securely.

7 Trainning & Awareness

We include evaluating security trainning and awareness programs for end users, identifying opportunities to improve security awareness.

8 Report and Recommendations

The organization is provided with a detailed report that summarizes the audit findings, highlights areas for improvement, and offers specific recommendations to strengthen the security posture.

myCloudDoor

Benefits

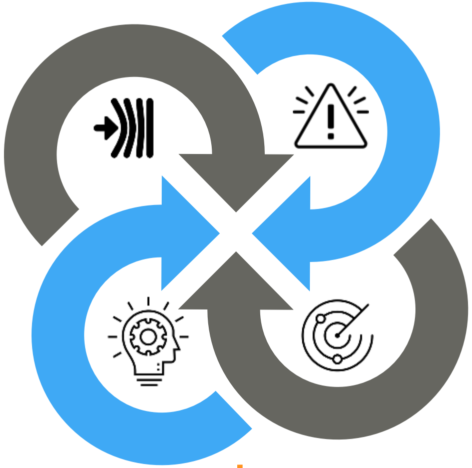
The main benefits of security assessment for Microsoft 365 environments

Vulnerabilities and Weaknesses

Detect and document potential vulnerabilities and weaknesses in Microsoft 365 security settings. This includes identifying misconfigurations or insecure configurations that could expose the organization to security risks.

Compliance

Verify that the organization complies with applicable security and privacy regulations and standards. This is especially important in regulated industries, such as healthcare (HIPAA) and personal data protection (GDPR).



Security Posture Assessment

Assess the current security posture of Microsoft 365, including security settings, permissions, roles, and security policies. This allows you to understand the level of protection and compliance of the platform.

Improved Security

Propose corrective actions and recommendations to improve security in Microsoft 365. These improvements may include configuration adjustments, implementing stronger security policies, and adopting security best practices.

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.

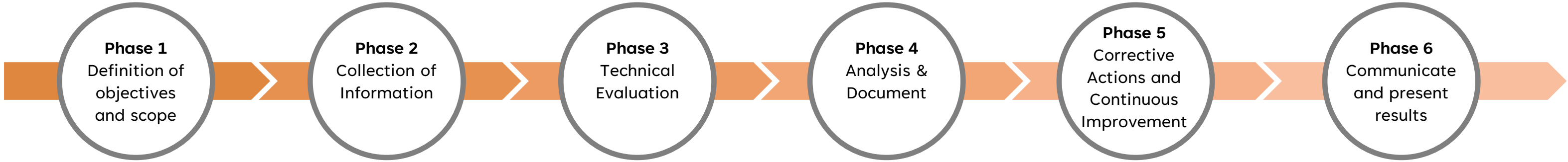
C. CRITERIA

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.

Microsoft 365 Security Assessment Planning

Phases and activities

Week 1	Week 2	Week 3	Last Day
Kick-off meeting	Configuration Review	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	User Auditing	Create detailed reports summarizing assessment results, recommendations, and necessary corrective actions	Make a detailed presentation of the results and recommendations
Review and compile documentation	Access Auditing	Document a continuous improvement plan	
Validate tool access	Audit Log Analysis		
Staff Interviews	Threat Protection Assessment		
	Identity Management		
	Compliance		
	Education & Awareness		



Phase 1 Definition of objectives and scope

Phase 2 Collection of Information

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
- 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

myCloudDoor

myCloudDoor

Creating future

THANK YOU

info@myclouddoor.com

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