Compliance Concepts in the Microsoft Cloud

Vlad Catrinescu

Microsoft MVP | Independent Consultant

@vladcatrinescu | VladTalksTech.com | YouTube.com/@VladTalksTech

Overview

Introduction to regulatory compliance

Governance, Risk, and Compliance (GRC) framework

Introduction to Regulatory Compliance

Regulatory Compliance for IT Professionals

GDPR

Set of digital security requirements and practices

Ensure that a company's business processes are secure

Usually done to satisfy a third party

- Government
- Security framework
- Client

Popular IT Compliance Standards and Regulations

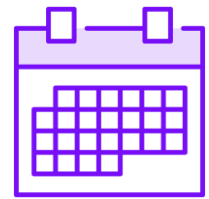|	
GDPR	**HIPAA**
The National Institute of Standards and Technology (NIST) *EX: NIST SP 800-171*	**PCI-DSS**

Example Compliance Needs

Granting individuals the right to access their data at any time

Granting individuals the right to correct or delete data about them if needed

Introducing retention periods that dictate a minimum or maximum amount of time data should be stored

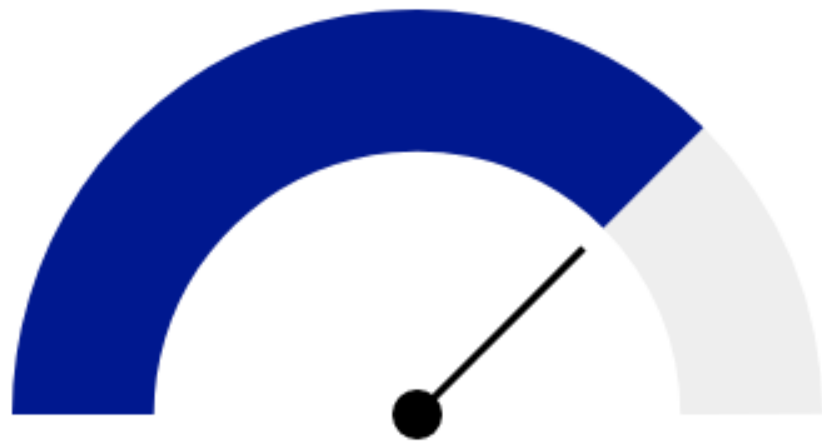Enabling governments and regulatory agencies the right to access and examine data when necessary

Defining rules for what data can be processed and how that should be done

Compliance in the Cloud

Overall compliance score

Your compliance score: 75%

12159/16167 points achieved

Your points achieved ⓘ
0/ 4008

Microsoft managed points achieved ⓘ
12159/ 12159

Compliance score measures your progress towards completing recommended actions that help reduce risks around data protection and regulatory standards.

Security in the cloud is a partnership
- So is compliance!

Part of the requirements will be done by Microsoft
- Microsoft will provide the documentation / proof of it for you

A lot of it depends on you

Governance, Risk, and Compliance (GRC)

GRC

Governance, Risk, and Compliance (GRC) is a structured way to align IT with business goals while managing risks and meeting all industry and government regulations. It includes tools and processes to unify an organization's governance and risk management with its technological innovation and adoption. Companies use GRC to achieve organizational goals reliably, remove uncertainty, and meet compliance requirements.

Governance, Risk, and Compliance

Governance

Governance is the set of policies, procedures, rules, and frameworks that a company uses to achieve its business goals

Risk management

Risk management is the process of identifying, assessing, and responding to threats or events that can impact company or customer objectives

Compliance

Compliance refers to the country/region, state or federal laws or even multi-national regulations that an organization must follow

Helps organizations establish policies and practices to minimize compliance risk

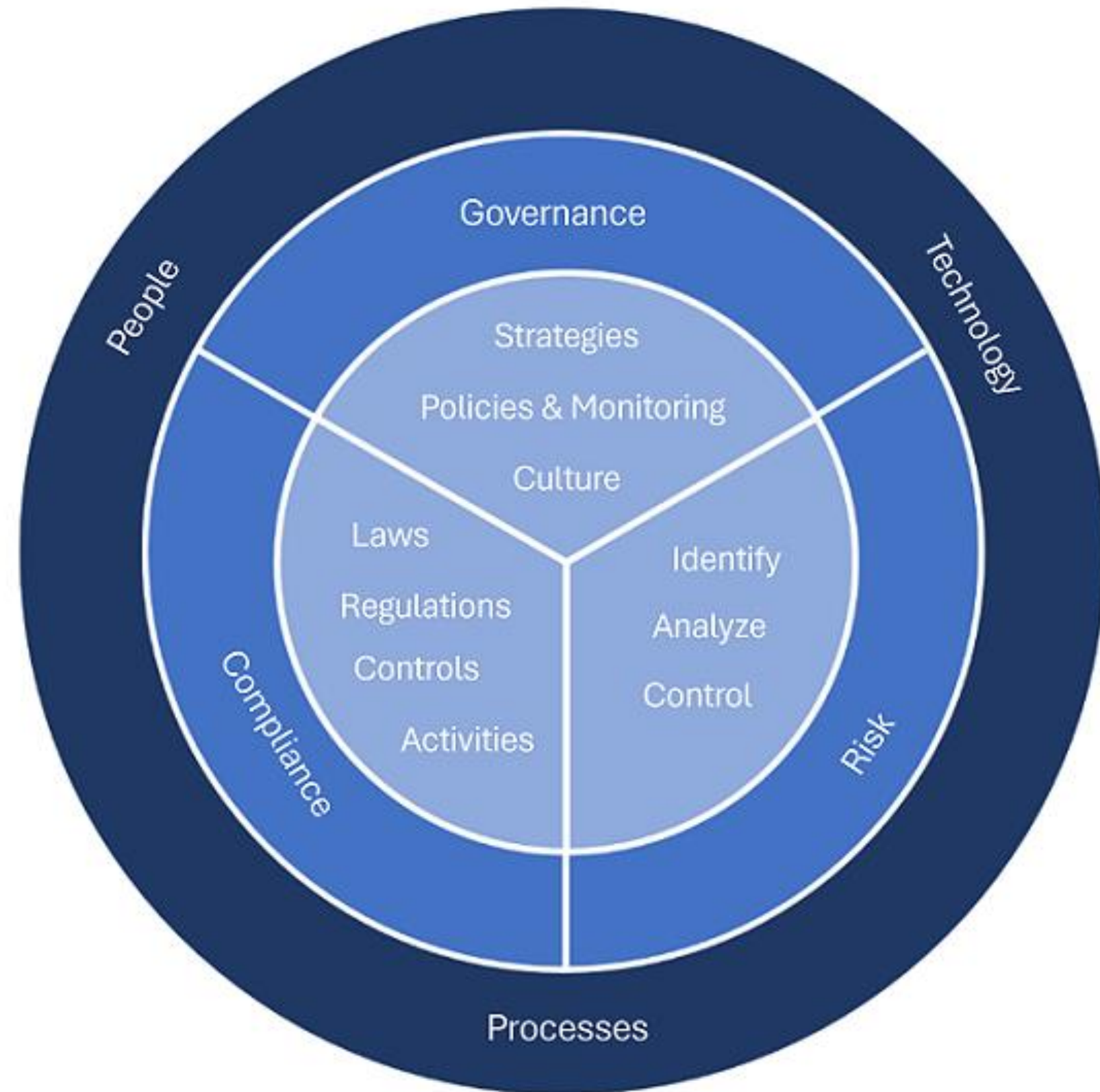**It's a way to get everyone aligned on business objectives**

Senior executives

Legal teams

Finance and HR managers

IT departments

Microsoft has many tools that can be part of your GRC policies

Governance

Strategies
Policies & Monitoring
Culture

People

Technology

Compliance

Laws
Regulations
Controls
Activities

Identify
Analyze
Control

Risk

Processes

Image Source: Microsoft

Module Conclusion

Introduction to regulatory compliance

- Set of digital security requirements and practices
  - Usually done to satisfy a third party

Governance, Risk, and Compliance (GRC) framework

- Helps organizations establish policies and practices to minimize compliance risk

Up Next:

Course Conclusion