2020

TREASURYGO™

DATA SECURITY AND PRIVACY ASSESSMENT NOVEMBER 24, 2020

JENNIFER CHARTRAW

TREASURYGO

Table of Contents

TREASURYGO

Independent Audit report

Please see under Appendix of this document “Microsoft Corporation – Azure DevOps – System and Organization Controls (SOC) 2 Report July 1, 2019 to June 20, 2020 and “Microsoft Azure, Dynamics, and other Online Services - Information Security Management System - ISO/IEC 27001 8.13.2020”

This audit was conducted By Deloitte, an independent Service Auditor for the security, availability, processing integrity and confidential criteria for Microsoft Azure which is the Cloud Services Partner of TreasuryGo.

TreasuryGo uses and is supported at the highest levels by Microsoft Azure for all our environments (Dev, UAT, Prod). The Azure platform is a Shared Responsibility Model.

For purposes of data and privacy auditing – and any other regulatory compliance mandate such as SOC2 and GDPR compliance – it is important to note the following for Microsoft Azure as it relates to TreasuryGo:

Supporting physical infrastructure is primarily Azure’s responsibility, while host infrastructure (such as configuring and deploying virtual hosts) is the responsibility of TreasuryGo and is fully supported by Microsoft Azure DevOps

There are clear lines of responsibility, but often, there are also shared roles between Microsoft Azure and TreasuryGo when it comes to responsibility regarding security and compliance. How we ensure being compliant with Microsoft’s Treasury and IT Engineering team is by adhering to all Microsoft Azure required areas for:

Operations Management Suite Security and Audit Dashboard (SOC2/GDPR/etc.)

Azure Advisor

Azure Security Center – Data and Privacy coverage

Azure Monitor

Log Analytics

Application Insights

TREASURYGO

Information Security Program

TreasuryGo has an established information security program based in all the essential foundational components as defined by the ISO/IEC 27001.

For background and definition of this standard, the International Organization for Standardization (ISO) is an independent nongovernmental organization and the world's largest developer of voluntary international standards. The International Electrotechnical Commission (IEC) is the world's leading organization for the preparation and publication of international standards for electrical, electronic, and related technologies.

These standards published under the joint ISO/IEC subcommittee, the ISO/IEC 27000 family of standards outlines hundreds of controls and control mechanisms to keep information assets secure. These global standards provide a framework for policies and procedures that include all legal, physical, and technical controls involved in an organization's information risk management processes and are the bedrock foundation of TreasuryGo Information Security Program in partnership with Microsoft Azure.

For access to the latest TreasuryGo / Microsoft Azure ISO/IEC 27001 certification click on the following link.

Information Security Management System - ISO/IEC 27001:2013

Information Security Policies

TreasuryGo's Information Security Policies are guided and paired with Azure Policy Regulatory Compliance built-in initiatives.

Using Azure Policy TreasuryGo evaluates resources in Azure by comparing the properties of those TreasuryGo Azure resources to TreasuryGo tenants, regulatory rules and client requirements. These business rules, described in JSON format, are known as policy definitions. TreasuryGo has simplified management, grouping several business rules together to form a policy initiative (called a policySet) within its Azure platform. TreasuryGo policy definition or initiative is assigned to any scope of resources that Azure supports, such as management groups, subscriptions, resource groups, or individual resources. The assignment applies to all resources within the TreasuryGo Resource Manager scope of that assignment.

TreasuryGo and Azure Policy uses a JSON format to form the logic the evaluation uses to determine if a resource is compliant or not. Definitions include metadata and the policy rule. The defined rule can use functions, parameters, logical operators, conditions, and property aliases to match exactly the scenario you want. The policy rule determines which resources in the scope of the assignment get evaluated.

Azure Security Center's features cover the two broad pillars of cloud security:

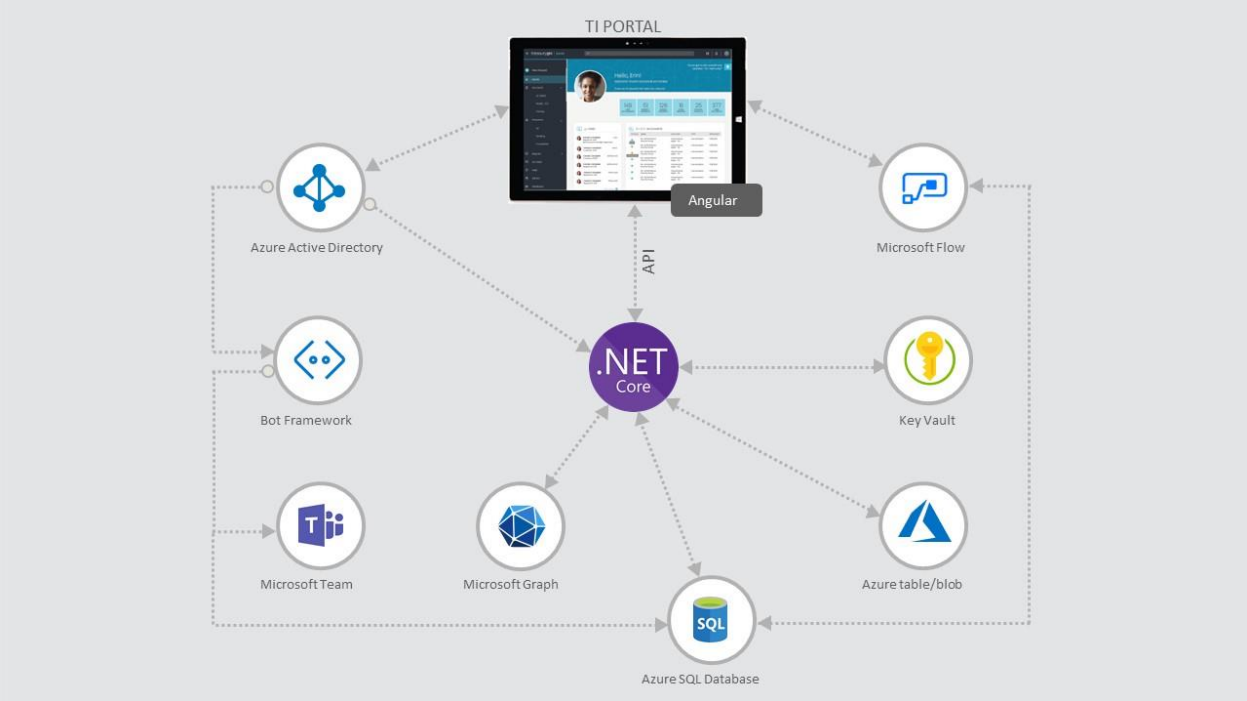
Using the Azure Cloud security posture management (CSPM) - Security Center TreasuryGo enables detection of security misconfigurations in our Azure machines, asset inventory, and other proprietary areas. Using these CSPM features to strengthen TreasuryGo's hybrid cloud posture and track compliance with ISO built-in policies.

Cloud workload protection (CWP) - Security Center's integrated cloud workload protection platform (CWPP), Azure Defender, brings advanced, intelligent, protection of TreasuryGo's Azure and hybrid resources (bank and other financial institutions) and workloads. Enabled by Azure Defender TreasuryGo uses a range of additional security features in addition to the built-in policies, we have enabled within our Azure Defender plan custom policies and initiatives. Adhering to regulatory standards - such as NIST and Azure CIS - as well as the Azure Security Benchmark for a truly customized view of our compliance.

Guided by the Microsoft Azure Security team and adherence to the Information Security Policy as described with the Azure platform.

Architecture Diagram

TreasuryGo architecture diagram November 2020



Clean Desk Policy

Overview

TreasuryGo stands committed to the development of secure policies and practices, and in doing so, has implemented this Clean Desk Policy to increase physical security at TreasuryGo locations worldwide. This policy ensures that confidential information and sensitive materials are stored away and out of sight when they are not in use or when the workspace is vacant.

This policy sets forth the basic requirements for keeping a clean workspace, where sensitive and confidential information about TreasuryGo] employees, clients, vendors, and intellectual property is secured.

The policy shall apply to all TreasuryGo employees, contractors, and affiliates.

Policy

Employees are required to secure all sensitive/confidential information in their workspace at the conclusion of the workday and when they are expected to be away from their workspace for an extended period of time. This includes both electronic and physical hardcopy information.

Computer workstations/laptops must be locked (logged out or shut down) when unattended and at the end of the workday. Portable devices like laptops and tablets that remain in the office overnight must be shut down and stored away.

Mass storage devices such as CD, DVD, USB drives, or external hard drives must be treated as sensitive material and locked away when not in use.

Printed materials must be immediately removed from printers or fax machines. Printing physical copies should be reserved for moments of absolute necessity. Documents should be viewed, shared, and managed electronically whenever possible.

All sensitive documents and restricted information must be placed in the designated shredder bins for destruction or placed in the locked confidential disposal bins. Please refer to the Records Retention Policy for additional information pertaining to document destruction.

File cabinets and drawers containing sensitive information must be kept closed and locked when unattended and not in use.

Passwords must not be written down or stored anywhere in the office.

Keys and physical access cards must not be left unattended anywhere in the office.

It is the responsibility of each Team Lead and Company Officer to ensure enforcement with the policies above. Repeated or serious violations of the clean desk policy can result in disciplinary actions in accordance with TreasuryGo’s Employee Handbook.

If you notice that any of your devices or documents have gone missing, or if you believe your workspace has been tampered with in any way, please notify Greg Morris or Jennifer Chartraw immediately.

Visitor Policy

Scope

This policy applies to all employees. “Workplace visitors” may refer to employees’ friends and family (referred to as personal visitors) contractors, external vendors, stakeholders and the public.

This policy does not refer to remote employees or employees from other company locations. To ensure safety at work, employees who are on parental leave may enter our premises with visitor passes.

Policy elements

The following rules apply for all kinds of visitors:

Visitors should sign in at the [reception/ gate/ front-office] and show some form of identification.

Visitors will receive passes and return them to [reception/ gate/ front-office] once the visit is over.

Employees must always tend to their visitors while they are inside our premises.

Our internet usage, data protection and confidentiality policies temporarily cover our visitors while they are on company premises. They must not misuse our internet connection, disclose confidential information, or take photographs of restricted areas. If they do not conform, they may be escorted out or face prosecution if appropriate.

Visitors are allowed during working hours. After-hours visitors must have written authorization from [HR/management.]

What is the policy for personal visitors in the workplace?

As a general rule, employees may not allow access to our buildings to unauthorized personal visitors. We can make exceptions on a case-by-case basis. Employees may bring visitors to company events or after obtaining authorization from [HR/ Security Officer/ Office manager.] To avoid confusion or misunderstanding, authorization should be in writing. [HR/ Security Officer/ Office manager] may also give verbal authorization, when appropriate, but must also inform reception and security guards.

Common areas, like lobbies, may be open to visitors. We advise our employees to only permit visitors in those areas for a short time and for specific reasons. Employees are responsible for accompanying any of their underage visitors at all times.

Contractors and service vendors

Contractors, suppliers and service vendors, like IT technicians and plumbers, can enter our premises only to complete their job duties. Front-desk employees are responsible for providing contractors and vendors with badges and for instructing them to wear those badges at all times on our premises.

Other kinds of visitors

Our company may occasionally accept the following types of visitors:

Students

Investors

Customers

Job candidates

Business partners

Those visitors should receive written authorization from HR or management before entering our premises. They should always be accompanied by an employee while on company property.

Solicitation

In accordance with our non-solicitation policy, visitors must not try to proselytize employees, gather donations or request participation in activities while on our premises. Any visitors who violate this policy may be escorted out.

Deliveries

Anyone who delivers orders, mail or packages for employees should remain at the building's reception or gate. [Front office employees/ security guards] are responsible for notifying the employee who expects the delivery. If that employee is unable to receive their order, front office employees may accept the order on the employee's behalf upon request.

Front-office personnel must sign for and disseminate all business orders and mail.

Dangerous or restricted areas

Employees may not bring or accept visitors in areas where there are dangerous machines or chemicals, confidential records or sensitive equipment.

Representatives of regulatory bodies and stakeholders (e.g. investors) may be exempted, if they have received official authorization from [HR/ Security Officer/ Office manager.] In these cases, employees should provide visitors with the necessary badges and protective equipment to enter premises when needed.

Unauthorized visitors

Security staff who spot unauthorized visitors may ask them to leave. Visitors who misbehave (e.g. engage in hate speech, cause disruption or steal property) will be asked to leave and prosecuted if appropriate.

Employees who spot unauthorized visitors may refer them to [security/office manager.]

Disciplinary Action

Employees who violate this policy may face disciplinary consequences in proportion to their violation. HR will determine how serious an employee's offense is and take the appropriate action:

For minor violations (e.g. bringing in personal visitors without authorization), employees may only receive verbal reprimands.

For more serious violations (e.g. bringing in unauthorized visitors who rob or damage company property), employees may face severe disciplinary actions up to and including termination. It is the responsibility of each Team Lead and Company Officer to ensure enforcement with the policies above. Repeated or serious violations of the clean desk policy can result in disciplinary actions in accordance with TreasuryGo's Employee Handbook.

If you notice that any of your devices or documents have gone missing, or if you believe your workspace has been tampered with in any way, please notify Greg Morris or Jennifer Chartraw immediately.

Employee Signature:

TREASURYGO

Privacy Policy

TreasuryGo and Azure Data Privacy Policy

TreasuryGo has implemented and adheres to Azure Data Subject Requests for the GDPR portal, which provides step-by-step guidance on how to comply with GDPR requirements to find and act on personal data that resides in Azure. This capability to execute data subject requests is available through the Azure portal on our public and sovereign clouds, as well as through pre-existing APIs and UIs across the breadth of our online services.

TreasuryGo's Policy, which is deeply integrated into Azure Resource Manager, helps your organization enforce policy across resources. Using Azure Policy we define policies at an organizational level to manage resources and prevent developers from accidentally allocating resources in violation of those policies. TreasuryGo uses Azure Policy in a wide range of compliance scenarios, such as ensuring that your data is encrypted or remains in a specific region to comply with the GDPR.

With Compliance Manager, which is a free workflow-based risk assessment tool, TreasuryGo manages regulatory compliance within the shared responsibility model of the cloud. It delivers a dashboard view of standards, regulations, and assessments that contain Microsoft control implementation details and test results as well as customer-managed controls. This enables you to track, assign, and verify your organization's regulatory compliance activities.

Azure Information Protection, and TreasuryGo offers file-share scanning for on-premises servers to discover sensitive data, can enable you to label, classify, and protect it thereby improving organizational data governance.

Azure Security Center, which provides unified security management and advanced threat protection. Integration with Azure Policy enables you to apply security policies across hybrid cloud workloads to enable encryption, limit organizational exposure to threats, and respond to attacks.

Azure Security and Compliance GDPR Blueprint has enabled TreasuryGo to meet GDPR requirements. Leveraging common reference architectures, deployment guidance, GDPR article implementation mappings, customer responsibility matrices, and threat models to simplify adoption of Azure for TreasuryGo's GDPR compliance initiatives.

Disaster Recovery/ Business Continuity Plan

TreasuryGo Business Continuity and Disaster Recovery Overview

TreasuryGo best practice for business continuity and disaster recovery is partnered with Azure Data Explorer as it enables TreasuryGo modules to continue operating in the face of a disruption. TreasuryGo is covered with uptime availability (intra-region) and disaster recovery. Azure's native capabilities and architectural considerations for a resilient Azure Data Explorer redeployment enables TreasuryGo to maintain active 99% uptime services. These Azure configurations depend on resiliency requirements such as Recovery Point Objective (RPO) and Recovery Time Objective (RTO), needed effort, and cross partnership with TreasuryGo's DevOps team.

See Appendix

For TreasuryGo's Azure Stack Considerations for business continuity and disaster recovery

Security Patching Policy

TreasuryGo and Azure Defender provide quick and secure patching to detected IT or code issues.

TreasuryGo uses Azure Defender, integrated with Azure Security Center, that protects TreasuryGo's hybrid cloud workloads including servers, data, storage. Using Microsoft Defender for Endpoint (servers) and protect Linux servers. Assess application vulnerabilities in virtual machines. Helps protect your data that's hosted in Azure Virtual Machines, on premises, or in other clouds, and detect unusual attempts to access Azure Storage accounts.

TreasuryGo uses Azure Arc to extend security coverage to workloads outside of Azure. Scanning for vulnerabilities in container images in Azure Container Registry and protect managed Azure Kubernetes Service instances.

Streamline security management, TreasuryGo deploys Security Center on large-scale environments, using policies and automation with Azure DevOps. Using AI and automation to quickly identify threats, streamline threat investigation, and help automate remediation.

TreasuryGo connects to existing tools and processes, such as Azure Sentinel security solutions to streamline threat mitigation. Creating safe workflow management automation with Azure Logic Apps implementing patches in real time for seamless uptime of TreasuryGo modules.

Single Sign on Policy

TreasuryGo has implemented Single sign-on (SSO) security using Azure Active Directory (Azure AD).

Many organizations rely on software as a service (SaaS) applications, such as Microsoft 365, Box, and Salesforce, for end user productivity. Historically, IT staff needed to individually create and update user accounts in each SaaS application, and users needed to remember a password for each.

easily integrate them in your tenant.

Licensing

Azure AD SSO for pre-integrated SaaS applications is free. However, the number of objects in your directory and the features you wish to deploy may require additional licenses. For a full list of license requirements, see Azure Active Directory Pricing.

Application licensing - You'll need the appropriate licenses for your SaaS applications to meet your business needs. Work with the application owner to determine whether the users assigned to the application have the appropriate licenses for their roles within the application. If Azure AD manages the automatic provisioning based on roles, the roles assigned in Azure AD must align with the number of licenses owned within the application. Improper number of licenses owned in the application may lead to errors during the provisioning/updating of a user.

Microsoft Cloud App Security (MCAS) is a Cloud Access Security Broker (CASB) solution. It gives you visibility into your cloud apps and services, provides sophisticated analytics to identify and combat cyberthreats, and enables you to control how your data travels.

TreasuryGo and MCAS enables the product modules to control access by:

Use Cloud Discovery to map and identify your cloud environment and the cloud apps your organization is using.

Sanctioning and un-sanction apps in TreasuryGo tenent

TreasuryGo’s APIs, for visibility and governance of apps that you connect to Conditional Access App Control protection to get real-time visibility and control over access to each company access to modules within TreasuryGo.

AAD SSP enables TreasuryGo to have continuous control by setting, and continual fine-tuning, for each clients policies.

Microsoft Cloud Application Security (MCAS) Session control is available for any browser on any major platform on any operating system. Mobile apps and desktop apps can also be blocked or allowed. By natively integrating with Azure AD.

Account Maintenance Policy

TreasuryGo and Azure AD assigns group access to the TreasuryGo modules that are deployed in Azure TreasuryGo combines dynamic groups with individual assignment to modules, automated user app access assignments/ TreasuryGo uses Azure Active Directory Premium to assign access to it's product modules

Azure AD also gives TreasuryGo granular control of the data that flows between the app and the groups to whom each client assigns access. Within Enterprise Applications, TreasuryGo select Provisioning to:

Set up automatic provisioning for Bank and Loan modules

Provide credentials to connect to TreasuryGo management API

TreasuryGo maps control between user attributes flow between Azure AD and the app when user accounts are provisioned or updated

Start and stop the Azure AD provisioning service for an app, clear the provisioning cache, or restart the service

View the Provisioning activity report that provides a log of all users and groups created, updated, and removed between Azure AD and TreasuryGo, and the Provisioning error report informing the Account Maintenance Reporting.

Partnered with Azure AD and SSO TreasuryGo's account maintenance is uniform and up to date with each companies personnel changes.

Information Security Incident Response policy

TreasuryGo and Azure DevOps services responds to a potential data breach according to the security incident response process, which is a subset of the Microsoft Azure incident management plan. Azure's security incident response is implemented using a five-stage process: Detect, Assess, Diagnose, Stabilize, and Close. The Security Incident Response Team may alternate between the diagnose and stabilize stages as the investigation progresses. An overview of the security incident response process is below:

DETECTION OF POTENTIAL BREACHES

Stage

1 — Detect

First indication of a potential incident.

2 — Assess

An on-call incident response team member assesses the impact and severity of the event. Based on evidence, the assessment may or may not result in further escalation to the security response team.

3 — Diagnose

Security response experts conduct the technical or forensic investigation, identify containment, mitigation, and workaround strategies. If the security team believes that customer data may have become exposed to an unlawful or unauthorized individual, execution of the Customer Incident Notification process begins in parallel.

4 — Stabilize and Recover

The incident response team creates a recovery plan to mitigate the issue. Crisis containment steps such as quarantining impacted systems may occur immediately and in parallel with diagnosis. Longer term mitigations may be planned which occur after the immediate risk has passed.

5 — Close and Post-mortem

The incident response team creates a post-mortem that outlines the details of the incident, with the intention to revise policies, procedures, and processes to prevent a recurrence of the event. This post-mortem is shared with impacted clients.

Change Control Policy

TreasuryGo Change Control Policy, Procedure and Form

Purpose

TreasuryGo's Change Control is a very simple concept. It means providing an orderly way for making changes to our Microsoft Azure applications (i.e., Active Directory, Exchange, OS Patches, etc.).

Change Control Team

The Change Control Team manages the objectives of the request and is comprised of members representing the technical, client and management communities. This team will meet as needed to review, approve/reject all proposed changes, and schedule change actions.

Procedure

1. A request must be submitted to the Change Control Manager
2. If the initial request is approved by the Change Control Manager and is not an Emergency Change, an appropriate Change Control Team is formed.
3. An impact analysis is performed by a member of the Change Control Team to determine what applications are affected by the change, if an outage is required and to determine the approximate costs and risks associated with the request. A back-out plan is also developed and included in the impact analysis to ensure that unsuccessful changes or undesirable results do not adversely impact business processes.
4. The Change Control Team will meet as needed to review proposed changes. The Change Control Manager is the coordinator of the Change Control Team.
5. If a request is denied, the requestor is notified in writing.
6. Requests that are approved are categorized by priority (critical or normal), a Change Implementer is assigned, an implementation date is determined, and responsibility for end user communications is assigned.
7. Emergency changes and IT changes: In the event of an emergency requirement for a change, the Change Control Manager must approve a change prior to implementation

and document reason for change, implementation notes and appropriate testing. The Change Control Manager will review all approved emergency changes and IT changes periodically with the IT Manager.

8. The Change Control Team will develop test scripts as necessary and assign test responsibilities so that users can validate the changes in the production environment. User acceptance information (name, date, summarized results, etc., as applicable) is documented in a database.

9. Once completed and tested, the documentation and history of the project is retained. All user approvals that were captured by email will be also be saved. The Change Control Manager will maintain copies of approval emails in his/her email files to facilitate validation of the contents of emails.

RFC FORM

Change Proposal Title:

Requested By:

Planned Unplanned

Development Change Yes No Project Name:

Describe proposed change:

Risk(s) of implementing the proposed change:

Fallback or back-out plan:

If an outage or interruption of service to users is required, who will be affected and for how long?

Review

Date:

Implementer Assigned:

Date Implementation of Change is Due:

Approval: Approved Rejected Postponed

Priority: Critical Medium Low

Describe any testing that was performed after implementing the change:

User Acceptance (if necessary)

Appendix

CERTIFICATE OF REGISTRATION

Information Security Management System - ISO/IEC 27001:2013 – attached.

Azure DevOps SOC 2 Type2 Report

As a supplement to the above ISO Certification we have available to provide under NDA an additional ISO certification details document outlining the Microsoft Azure areas certified and used by TreasuryGo, details listed below.

Microsoft Azure (All-Up), Dynamics 365 and Other Online Services

ISO/IEC 27001:2013, 27018:2019, 27701:2019

Information Security and Privacy Management Systems - Statement of Applicability

This document is considered Microsoft TRADE SECRET. While it may be shared with current potential customers

under NDA, the information found within must remain confidential. The information contained in this document

describes the ISMS Statement of Applicability for Microsoft Azure, Dynamics 365 and Other Online Services as of the

revision date specified . The information contained in this document is subject to change at any time and does not

represent a commitment, contractual or otherwise, on the part of Microsoft. MICROSOFT MAKES NO WARRANTIES,

EXPRESSED, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.'

Statement of Applicability (Dated 2/29/2020) v2020.01