Technical Guide

DANAOS ProjectVIEW ERP | SaaS

Author/Signatory	Approver	Reference Nr.	Date	Release
Eng. Christos Emmanouilidis	Eng. Vassilios Sakorafas	**MC 23N/402**	29th July 2023	V1
Eng. Christos Emmanouilidis	Eng. Vassilios Sakorafas	**MC 24N/136**	10th October 2024	V2
Eng. Christos Emmanouilidis	Eng. Vassilios Sakorafas	**MC 24N/136**	25th May 2025	V3

Keep Private and Confidential

TABLE OF CONTENTS

1. DANAOS ProjectVIEW ERP - SaaS

DANAOS ProjectVIEW ERP (www.projectview.cloud) as a Service (SaaS) Guide outlines the principles and processes required for the successful technical deployment and support of **DANAOS ProjectVIEW ERP v.11** in the Microsoft Azure Cloud Computing Environment as a SaaS offering.

The DANAOS Web Enterprise Architecture is based on a 3-tier architecture model and fulfills the definition of an Information System by providing:

A.	Centralized access control module based on roles and tasks
B.	Interactive groupware features such approvals and workflows
C.	Information sharing and digital integration between business entities
D.	Various reports related to the core business
E.	Custom reporting by capitalizing any data structure within the system database
F.	Detailed user activity logging mechanism

1.1 Data Tier - Database server

- **Operating System version**: Microsoft Windows Server 2022 or later
- **RDBMS version**: SQL Server 2022 (Web, Standard or Enterprise Edition)

OR Azure SQL

1.2 Application Tier - Application Server

- **Operating System Version:** Microsoft Windows Server 2022
- **Web Server**: IIS 10.0

OR Azure App Service

- **DANAOS ProjectVIEW ERP:** Version 11.x

1.3 Presentation Tier - Web Browser

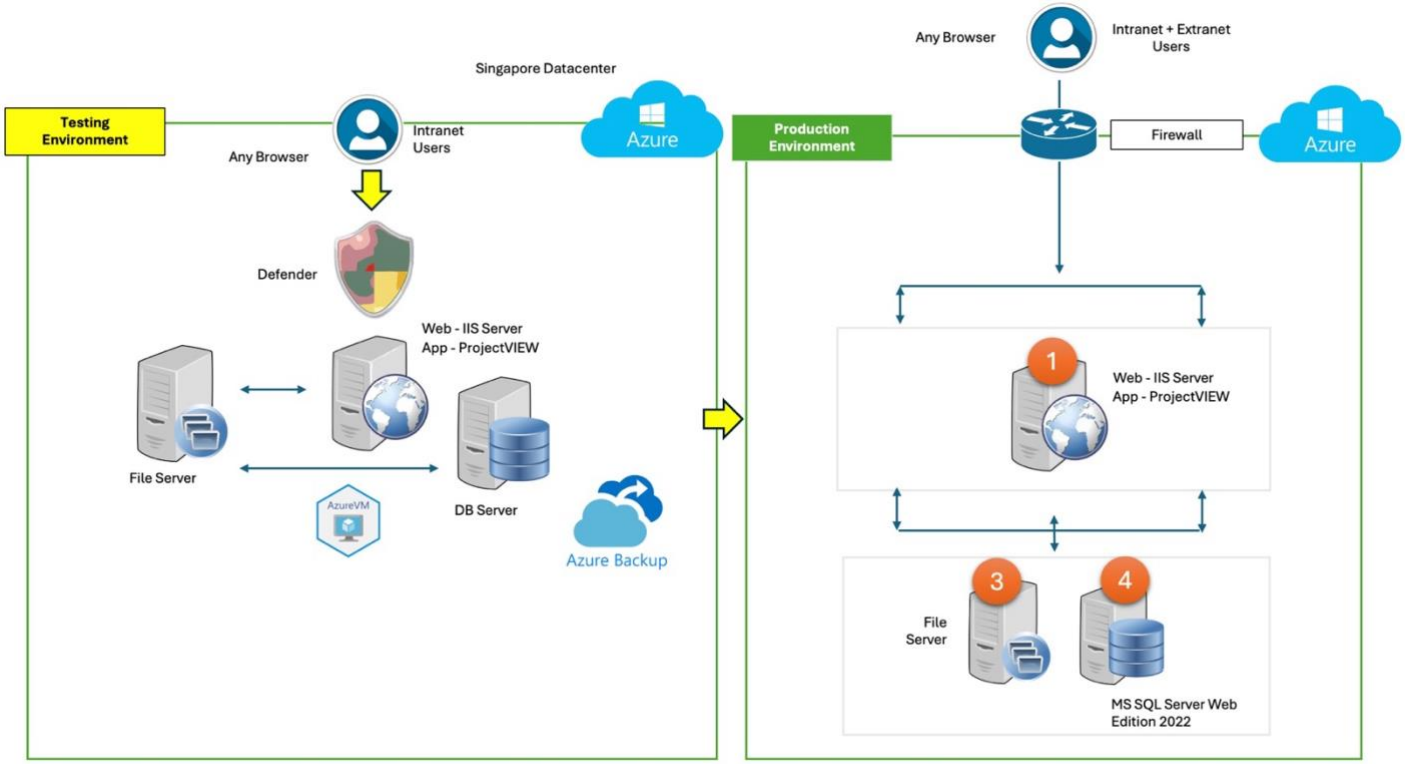
All common web browsers including but not limited to:

- Google Chrome
- Mozilla Firefox
- Safari
- Edge

DANAOS ProjectVIEW ERP deployment in Microsoft Azure is based on the following topology:

1.4 Cloud Topology

Each VM is supported via Network Security Groups that provide Firewall functionality with access rules. Azure Firewall (Web Application Firewall) will further protect the Web Applications workload. Below Server-based topology can be substituted with Service-based topology based on the aforementioned.



2. CONFIDENTIALITY & SECURITY PRINCIPLES

DANAOS ProjectVIEW EPR incorporates the following security mechanisms to ensure system confidentiality:

2.1 Password Policy

2.1.1 Password Complexity

As part of the System Admin console, ProjectVIEW ERP v. 11 provides functionalities for a Sysadmin (User as System Administrator) to define the password policy per category.

The **recommended/default setup** for Password complexity is as follows:

- Minimum Characters: 8
- Minimum Letters in Uppercase: 1
- Minimum Letters in Lowercase: 1
- Minimum Digits: 1
- Minimum Special Characters: 1
- Disallow the last password: Yes/No
- The administrator can manually reset the password: Yes

2.1.2 Password Expiration mechanism

DANAOS ProjectVIEW ERP v. 11 allows the system administrator to define a period after which users are mandated to alter their password values. **The default parameters are as follows**:

- Days before expiration is: 90 days
- Days before password expiry warning: 10 days
- Hours before password reset token expiration: 24 Hours

2.1.3 Failed authentication security mechanism

DANAOS ProjectVIEW ERP v. 11 allows the system administrator of each Data Controller to define the number of failed consecutive login attempts per account, after which the account will become “locked.” System administrator intervention will be needed to enable it again.

The **default parameters** are as follows:

- Allowed login attempts: 3 (will lock the user out of the system after three unsuccessful attempts with an option to tag if the Sysadmin user account will be included in the lockout
- Session timeout (default as per IIS): 20 minutes. The system will terminate the session and display an alert that the login session may have expired due to inactivity.

2.1.4 Password history checking

DANAOS ProjectVIEW ERP v. 11 allows system administrators to prevent users from using any password values they used in the past again. **The default value** is:

The password may not match any of the user's last password

2.1.5 Minimum Password length restriction

DANAOS ProjectVIEW ERP v. 11 allows system administrators to define the minimum length of the password value users are allowed to utilize.

The default minimum number of characters is: 8

2.1.6 Away from keyboard lock screen mechanism

DANAOS ProjectVIEW ERP v. 11 allows system administrators to define the number of minutes the application will require users to submit their passwords again after being idle.

The default session timeout is: 20 minutes

2.1.7 Second factor authentication

DANAOS ProjectVIEW ERP v. 11 has incorporated the “Google Authenticator” or “Microsoft Authenticator” 2FA authentication when login requests are derived outside the intranet.

System administrators are allowed to define network and IP ranges, which are considered as “external” and mandate users to submit, apart from username/password credentials, the 6-digit value generated by Google or Microsoft authenticator either from a mobile device or browser extension.

2.1.8 End to end Data Transmission Encryption on Client-Server Communication

DANAOS ProjectVIEW ERP v.11suite supports SSL protocol end to end enforcing and assuring encryption on any communication between the server and client nodes

2.1.9 Single Sign On (SSO)

DANAOS ProjectVIEW ERP v.11supports single sign via Azure Active Directory

2.2 Access Control

DANAOS ProjectVIEW ERP v. 11 offers a detailed access control mechanism built on “Roles” and “Users Rights.”

The approach is based on the following principles:

1. Each DANAOS ProjectVIEW ERP v. 11 module is segmented into users and roles, which have access to functions and features.
2. Roles are mostly aligned to the actual business purpose of each job description.
3. Roles are assigned to users according to the intended goal
4. The Users and Roles maintenance are controlled by the system administrator

2.3 Source Code

DANAOS provides a lifetime warranty, which is assured with the deposit of our software source code to a third-party escrow account. This ensures the software's maintenance and alleviates the possibility of orphaning.

3. DANAOS CLOUD-FIRST STRATEGY

3.1 DANAOS Web-based ProjectVIEW v.11

DANAOS ProjectVIEW ERP v.11 is the technological bedrock on which purpose-specific modules representing business processes and corporate structure are integrated as one centralized enterprise application. **DANAOS ProjectVIEW ERP v.11** is developed and customized to the needs and specifications of each Client. **This constitutes our Modifiable-of-The-Shelf Software (MOTS) plateau.**

Our Modifiable-of-the-Shelf (MOTS) applications are pioneering within our industry due to:

1. the agile delivery time-to-market
2. the high ROI (Value for Money) and
3. the broad user acceptance

3.1.1 The New Era of DANAOS ProjectVIEW ERP v.11

DANAOS ProjectVIEW ERP v.11 is designed, developed and supported in-house by DANAOS-only engineers, consultants and subject-matter experts further enhanced with integration features (web services, web APIs) to support interoperability with 3rd party systems.

DANAOS ProjectVIEW ERP v.11 encapsulates construction software knowledge earned for over the past thirty years while launched as an enterprise-grade construction solution, syncing securely data; onsite and office.

DANAOS ProjectVIEW ERP v.11 makes it easier to customize business-specific operations and structure projects so IT managers, CIOs, and CTOs can easily maintain each application and assure business continuity software that is aligned with each company's Digital Transformation Strategy. This ensures service availability by eliminating hidden resiliency risks.

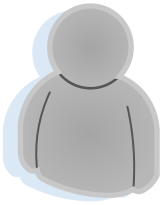
DANAOS ProjectVIEW ERP v.11 is conceptualized and developed on a lightweight, stateless, web-friendly architecture with a responsive UI. It provides predictable and minimal resource consumption (CPU, memory, threads) for highly scalable applications and advanced security.

More specifically, DANAOS ProjectVIEW ERP v.11 is architected and designed using the latest programming methodologies and technologies, encouraging flexible customization and clean, pragmatic design.

- Based on a multitier architecture (n-tier architecture) operational functions are physically separated into:
    - presentation,
    - application (business logic) and
    - data layers.

- Secure access to the system(s) applications and services is provided in real-time, anywhere (Intranet/Extranet/Internet).
- Personalized dashboards display meaningful insights for each user's role within the Company.

3.1.2 Architecture/Systems Topology



client

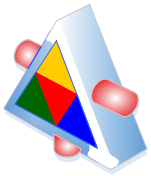
Secure access to the system(s) applications and services real-time, anywhere (Intranet/Extranet/Internet).

UI/UX

Responsive UI/UX providing aggregated information rendered to each user's role within the Company.

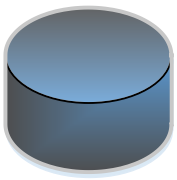
DANAOS Application(s)

DANAOS ProjectVIEW ERP v.11 Application, Components and Modules that simulate and facilitate Construction Business Logic.



development framework

The framework for developing/customizing DANAOS applications and integrating 3rd party systems.



database

MS SQL Server. A relational database that is used to store persistent structured data as a Single-Source-Of-Truth.

3.2 DANAOS Sovereign Cloud

Towards the digital transformation strategy, DANAOS Cloud-first policy includes a Software-as-a-Service (**SaaS)** delivery model in which DANAOS applications stack -for each Client- is hosted in Microsoft Azure Cloud

within a dedicated, private, secure Cloud Instance in the form of **Enterprise Application-as-a-Service** capturing the full benefits of DANAOS Construction purpose-specific modules, configured and customized to each Client's specs, along with Microsoft Cloud Azure advanced services and tools.

3.2.1 DANAOS SaaS Cloud

Providing a total peace of mind, DANAOS SaaS offering incorporates the benefits of DANAOS ProjectVIEW ERP v.11 industry-specific features, short time-to-market (short implementation period) as well as DANAOS superior Microsoft Azure Cloud Services, setting in place all necessary means and processes to optimize all business operations, centrally, assuring resilience, prevention and recovery of client's data assets, offered as Managed Services:

- Security Management
- Backup Management
- Resource Management
- Guaranteed Performance and Support

DANAOS SaaS offering is based on a high availability architecture with optional redundant resources. In any case, the sole ownership of data belongs to the Client.

3.2.2 Hybrid Cloud

Hybrid Cloud is a combination of an on-premises data center with another private cloud bundled with a set of DANAOS Hybrid Cloud services enhancing security and performance:

- Disaster Recovery (DR): replication of data and business continuity based in an off-premises location of DANAOS Azure Datacenter facilitating asynchronous backup.
- File Storage: a remote corporate on-cloud document vault that operates centrally, synchronizing and storing documents from diverse corporate locations, making them available to any device on-demand.

3.3 Cloud Security Process and Tools in place

The follow security controls and processes are in place:

1) Azure Defender (centralized security mechanism for MSFT Azure Cloud) used regularly for network vulnerability scanning
2) Firewall (each for VM)
3) Virtual Networks
4) VPN
5) Cloud Access Control (IAM)
6) Role-based access control (RBAC) for Azure Portal

7) Disaster Recovery (DR) in different geographic region (GRS) via daily backups (increased backup frequency on-demand)
8) Additional Antivirus and Antimalware software (eg. Bitdefender, Qualys)
9) Data Encryption in-transit (SSL, TLS) for all web applications
10) 2-Factor authentication
11) Automatic software updates for VMs
12) Secured Management Ports
13) Encryption at rest
14) Network watcher is used to monitor and diagnose problems in a network level with equivalent alerts and warnings
15) Mail notification for high severity alerts
16) Limited and dedicated access to authorized personnel only for administration purposes in Azure
17) Use of Locks to prevent accidental or malicious deletion or modification of resources
18) DDOS Protection is available

Moreover, extra controls are in place such as:

- Encryption at rest
- Credential encryption in configuration files
- Non-standard, high-complexity credentials used for DB access

3.3.1 Database Security Measures

1) Row-level security
2) Always Encrypted
3) Dynamic data masking
4) Server audit
5) Database Audit
6) Transparent database encryption
7) Data classification and auditing

3.3.2 Database Encryption

A first level of cryptography exists as Encryption-At-Rest in Virtual Machines and Hard Drives using Azure Managed Keys or Customer Managed Keys. Azure Managed Keys lifecycle is maintained by Azure.

AES Encryption with 256 Bit is used storage service encryption. DB is secured with:

1) Always Encrypted,
2) Dynamic Data Masking
3) Transparent Database Encryption (for MS SQL Enterprise Edition only) using AES and 3DES Encryption Algorithm.

3.3.3 Data Destruction

When customers delete data or leave Azure, Microsoft follows strict standards for overwriting storage resources before their reuse, as well as the physical destruction of decommissioned hardware. Microsoft executes a complete deletion of data on customer request and on contract termination.

3.3.4 Change Tracking and Inventory overview

This feature tracks changes in virtual machines hosted in Azure, on-premises, and other cloud environments to help you pinpoint operational and environmental issues with software managed by the Distribution Package Manager. Items that are tracked by Change Tracking and Inventory include:

- Windows software
- Windows files
- Windows registry keys
- Windows services

Change Tracking and Inventory makes use of Azure Security Center File Integrity Monitoring (FIM) to examine operating system and application files, and Windows Registry. While FIM monitors those entities, Change Tracking and Inventory natively tracks:

- Software changes
- Windows services

  The follow security controls and processes are in place:

3.3.5 Security Control for Cloud Administrators

1) Cloud Access Control (IAM)
2) Role-based access control (RBAC) for Azure Portal
3) 2-Factor authentication
4) Mail notification for high-severity alerts
5) Limited and dedicated access to authorized personnel only for administration purposes in Azure
6) Use of Locks to prevent accidental or malicious deletion or modification of resources

3.4 Development Tools and Processes

In terms of front-end DANAOS utilizes a stack of modern languages, frameworks and libraries such as:

- **HTML5,**
- **CSS,**
- **JavaScript,**
- **DevExpress Library,**

That, in association with APIs and Cross-platform add-ons, facilitates integration with other 3rd party systems.

DANAOS Web applications are developed on **Microsoft C# .NET (Server-side)** and utilize the above modern frameworks in the front-end, assuring a homogeneous technological approach with the hosting environment (**Microsoft Azure**) and a simplified, integrated User Experience among the different modules whilst maintaining a high performance, multi-platform and secure database approach by utilizing Microsoft MS SQL Server.

DANAOS hosts within Microsoft Azure Cloud two distinct environments:

1) QA and Testing (Pilot) that facilitates implementation prior to GO LIVE and testing of new features upon GO LIVE and onward
2) Production (per Client), a private Microsoft Azure environment with dedicated resources to each Client, in a data center closer to the Client's main workload

Business logic is maintained with the system's middleware, providing a secure orchestration of operations between all tiers: front-middleware and database and allowing advanced configuration, integrations and customizations as appropriate.

3.4.1 Secure Development

Part of DANAOS Agile development techniques and software development methodologies is an enhanced mechanism of Secure SDLC that involves integrating security testing and other activities into the existing development process on the framework level and for each module separately.

More specifically, Support and RnD Teams write security requirements alongside functional requirements and perform an architecture risk analysis during the design phase of the SDLC process. Above security principles also adhere to the cloud security principles of the Microsoft Azure, further reinforcing the security posture as a whole.

3.4.2 Versioning

DANAOS software development process includes a version-control mechanism (Git) that incorporates a "Master" (Standard DANAOS Application – Vanilla Version). Upon executing "Commit" and "Push" and after any "Pull" Request, application versions (instances) are fully justified by the relative programmer (or Agile Team) with semantic and contextual comments and allow the Reviewer to accept (or reject) changes based on DANAOS Programming Guidelines that include: Code Quality, Business Logic and Security Best Standards.

3.4.3 Quality Testing

For applications quality testing DANAOS utilizes an AI-based platform that uses Smart Locators to automate testing—slow authoring and unstable tests. More specifically, DANAOS is using Testim (https://www.testim.io/), a commercial end-to-end software testing tool powered by AI that provides developers and testers with a fast way to automate functional tests.

Furthermore, each application's business logic is exhaustively checked by DANAOS Support Engineers that are subject-matter experts within their domain and have full understanding on each Client's requirements and de facto operations. Per case, and based on specific functional operations, Unit Testing is performed validating that each unit of the software code performs as expected together with associated control data, usage procedures, and operating procedures.

3.4.4 Procedural and Transactional Compliance

In order to achieve auditability, traceability and compliance in all DANAOS applications processes, DANAOS attains a transparent mechanism, visible only to system admins, that records input information, inspects changes and controls data integrity between operators and processes, all documented into a detailed history log where every event is timestamped along with username. Compliance is achieved cross-modularly by inspecting data accuracy and consistency between each application's process.

Detailed History Log is stored and automatically updated into database. Based on the aforementioned, each AAA process adheres to all procedural and transactional requirements. Further to the standard logging processes, other logging registration, storing and management alternatives are also available via customization of the logging mechanism.

3.4.5 Change Management Auditability

Changes to the solution/service configuration are logged. A change management audit can be executed using these logs.

3.4.6 Users and Roles Management

Users and Roles Management Module is one of the foundation modules, of a set of DANAOS Framework Core Modules that allows assigning of user roles, controls the access rights to all applications levels and provides relative credentials to users. Standard Roles include: Application administrator, System (Global) administrator, Authentication Admin, Module (eg. Accounting, Tendering, Procurement, Finance, HR etc) Manager.

3.4.7 Obsolete Technologies

No obsolete, end of life or unsupported technologies are utilized by DANAOS. Considering the state-of-the-art development practices of DANAOS ProjectVIEW ERP v. 11, continuous integration with new technologies is fully assured.

3.4.8 Thin-Client Applications and Plugins

Considering the development of the front-end on the latest web standards (HTML5, CSS and JavaScript) and in order to assure compatibility with all modern browsers (Chrome, Safari, Mozilla, Edge etc.) DANAOS

Applications do not require client-side plugins. This light (thin-client) architecture assures faster loading time, higher security and any browser compatibility.

3.4.9 Manuals and Online Help

DANAOS User Manuals, DANAOS Technical Manuals, Installation Manual, Troubleshooting Manual along with onboarding and familiarization videos are provided online within the embedded Wiki (https://www.docs.projectview.wiki), easily accessible within the application. As part of overall customer experience, online documentation in retrieved based on easy/fuzzy search technique. DANAOS Support Engineers update relevant Customer-centric content.

3.4.10 Third-Party Services

2-factor authentication, Third-party services rendered within purpose-specific DANAOS Applications utilizing associated APIs. Beyond these purpose-specific addons, DANAOS Applications utilize per case, generic Cloud (Microsoft Azure Cloud) storage solutions that may extend to addons like: Intelligent Character Recognition (ICR).

3.4.11 Releases and Updates

DANAOS Web Applications enables users to update to the latest releases by automatically checking for updates while the device is connected to the internet.

Minor Releases and Updates: Maintenance releases and bug fixes mainly due to COTS (such as: OS and database) upgrades and updates. Releases are available to download on-demand subject to user (admin) acceptance 7-8 times per year.

Software Upgrades: New functional enhancements and extensions, major improvements in terms of UI/UX and new APIs/SKDs that constitute a new software version number. New versions are released approximately once a year.

DANAOS update process is facilitated by logging to ProjectVIEW ERP Wiki Portal (https://www.docs.projectview.wiki). Based on specific credentials and access rights, logged user is able to see all the latest (stable) update releases for each application. Each application's release is characterized by the release date and accompanied with comments on the latest features and functionalities.

Released updates may incorporate new features based on the latest customizations as requested by the Client along with resolution on compatibility issues with standard commercial off-the-shelf software, including O/S and the database. DANAOS Applications Portal is based on the **Gitbook** workflow (versioning workflow) where a "Branch" is cloned out of the "Master" of each application module. Each Application's "Master" is DANAOS "Standard" Application (aka Vanilla-version) that consolidates the updated general/horizontal features and functionalities and is further cloned based on each Client's configuration to

a separate “Branch”. This “Branch” is merged upon further consolidation from each customization – development “Sprint” and upon thorough quality testing.

System Administrator can select and download the desired applications and rollout latest release – updates to all users, automatically

3.4.12 End-Of-Life Policy

Succeeding the End of Life Announcement, End of Engineering Date occurs 30 days after, of which, Application Support ceases. Technical Support continues bug fixing without accepting new Change Requests. 12-Months after, End of Life occurs.

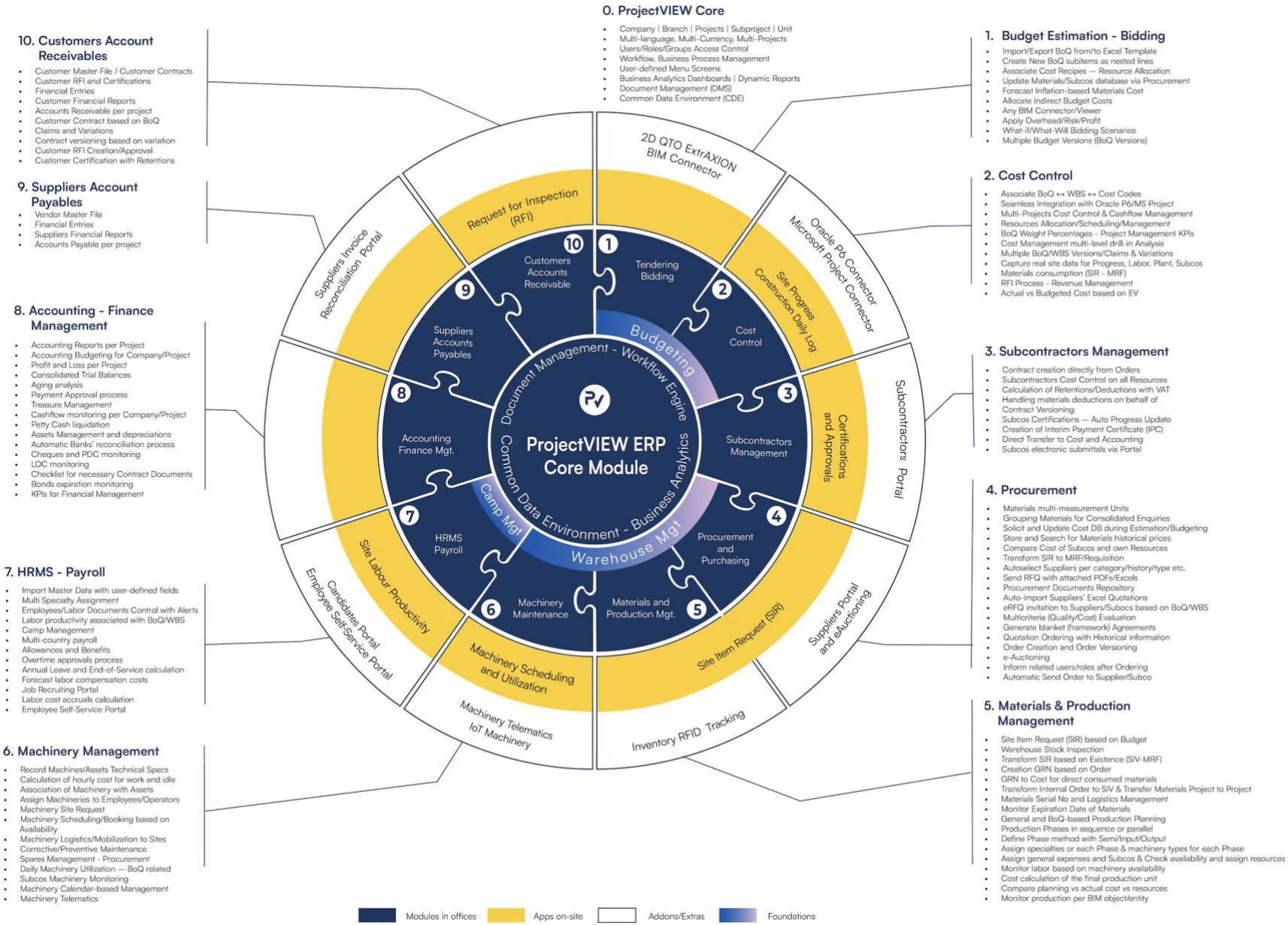
The representation of each DANAOS’s Application, the mapping of interconnectivity and the means of the accessibility from the users (intranet/extranet/internet) indicates a holistic (360 degrees) approach both broad and deep. DANAOS Solutions address all industry’s key challenges (listed above) whilst maintain an unparalleled modularity, scalability and extensibility.

3.4.13 DANAOS Business Strategy Overview

1. Applications, Components and Modules that simulate and facilitate Construction Business Logic.
2. The framework for developing/customizing DANAOS applications and integrating 3rd party systems.
3. Any relational database. A permanent repository that business applications use to store persistent structured data.

DANAOS ProjectVIEW ERP architecture is composed of a presentation tier (UI), an application layer (business logic tier - Middleware), and a data storage tier (MS SQL Server). Consequently, it complies with all standard scalability, agility, security, interoperability, and accessibility standards as it facilitates data flow and integrity between layers and tiers and holds a logical structuring mechanism for the elements that make up the software solution.

Combining comprehensive construction domain knowledge with advanced technology expertise, DANAOS provides construction software for the modern contractor, engineer, and consultant. **DANAOS ProjectVIEW ERP v.11 bundled with our Services** encompass the full spectrum of the shipping industry processes, addressing all daily challenges, either as stand-alone Applications or as a scalable, agile, secure and fully integrated Suites of Modules, accessed from everywhere, anytime.


0. ProjectVIEW Core
Company | Branch | Projects | Subproject | Unit
Multi-language, Multi-Currency, Multi-Projects
Users/Roles/Groups Access Control
Workflow, Business Process Management
User-defined Menu Screens
Business Analytics Dashboards | Dynamic Reports
Document Management (DMS)
Common Data Environment (CDE)
1. Budget Estimation - Bidding
Import/Export BoQ from/to Excel Template
Create New BoQ subitems as nested lines
Associate Cost Recipes — Resource Allocation
Update Materials/Subcos database via Procurement
Forecast Inflation-based Materials Cost
Allocate Indirect Budget Costs
Any BIM Connector/Viewer
Apply Overhead/Risk/Profit
What-if/What-Will Bidding Scenarios
Multiple Budget Versions (BoQ Versions)
2. Cost Control
Associate BoQ ↔ WBS ↔ Cost Codes
Seamless Integration with Oracle P6/MS Project
Multi-Projects Cost Control & Cashflow Management
Resources Allocation/Scheduling/Management
BoQ Weight Percentages - Project Management KPIs
Cost Management multi-level drill-in Analysis
Multiple BoQ/WBS Versions/Claims & Variations
Capture real site data for Progress, Labor, Plant, Subcos
Materials consumption (SIR - MRF)
RFI Process - Revenue Management
Actual vs Budgeted Cost based on EV
3. Subcontractors Management
Contract creation directly from Orders
Subcontractors Cost Control on all Resources
Calculation of Retentions/Deductions with VAT
Handling materials deductions on behalf of
Contract Versioning
Subcos Certifications — Auto Progress Update
Creation of Interim Payment Certificate (IPC)
Direct Transfer to Cost and Accounting
Subcos electronic submittals via Portal
4. Procurement
Materials multi-measurement Units
Grouping Materials for Consolidated Enquiries
Solicit and Update Cost DB during Estimation/Budgeting
Store and Search for Materials historical prices
Compare Cost of Subcos and own Resources
Transform SIR to MRF/Requisition
Autoselect Suppliers per category/history/type etc.
Send RFQ with attached PDFs/Excels
Procurement Documents Repository
Auto-import Suppliers' Excel Quotations
eRFQ invitation to Suppliers/Subocs based on BoQ/WBS
Multicriteria (Quality/Cost) Evaluation
Generate blanket (framework) Agreements
Quotation Ordering with Historical information
Order Creation and Order Versioning
e-Auctioning
Inform related users/roles after Ordering
Automatic Send Order to Supplier/Subco
5. Materials & Production Management
Site Item Request (SIR) based on Budget
Warehouse Stock Inspection
Transform SIR based on Existence (SIV-MRF)
Creation GRN based on Order
GRN to Cost for direct consumed materials
Transform Internal Order to SIV & Transfer Materials Project to Project
Materials Serial No and Logistics Management
Monitor Expiration Date of Materials
General and BoQ-based Production Planning
Production Phases in sequence or parallel
Define Phase method with Semi/Input/Output
Assign specialties or each Phase & machinery types for each Phase
Assign general expenses and Subcos & Check availability and assign resources
Monitor labor based on machinery availability
Cost calculation of the final production unit
Compare planning vs actual cost vs resources
Monitor production per BIM object/entity
6. Machinery Management
Record Machines/Assets Technical Specs
Calculation of hourly cost for work and idle
Association of Machinery with Assets
Assign Machineries to Employees/Operators
Machinery Site Request
Machinery Scheduling/Booking based on Availability
Machinery Logistics/Mobilization to Sites
Corrective/Preventive Maintenance
Spares Management - Procurement
Daily Machinery Utilization — BoQ related
Subcos Machinery Monitoring
Machinery Calendar-based Management
Machinery Telematics
7. HRMS - Payroll
Import Master Data with user-defined fields
Multi Specialty Assignment
Employees/Labor Documents Control with Alerts
Labor productivity associated with BoQ/WBS
Camp Management
Multi-country payroll
Allowances and Benefits
Overtime approvals process
Annual Leave and End-of-Service calculation
Forecast labor compensation costs
Job Recruiting Portal
Labor cost accruals calculation
Employee Self-Service Portal
8. Accounting - Finance Management
Accounting Reports per Project
Accounting Budgeting for Company/Project
Profit and Loss per Project
Consolidated Trial Balances
Aging analysis
Payment Approval process
Treasure Management
Cashflow monitoring per Company/Project
Petty Cash liquidation
Assets Management and depreciations
Automatic Banks' reconciliation process
Cheques and PDC monitoring
LOC monitoring
Checklist for necessary Contract Documents
Bonds expiration monitoring
KPIs for Financial Management
9. Suppliers Account Payables
Vendor Master File
Financial Entries
Suppliers Financial Reports
Accounts Payable per project
10. Customers Account Receivables
Customer Master File / Customer Contracts
Customer RFI and Certifications
Financial Entries
Customer Financial Reports
Accounts Receivable per project
Customer Contract based on BoQ
Claims and Variations
Contract versioning based on variation
Customer RFI Creation/Approval
Customer Certification with Retentions
2D QTO ExtrAXION BIM Connector
Oracle P6 Connector Microsoft Project Connector
Subcontractors Portal
Suppliers Portal and eAuctioning
Inventory RFID Tracking
Machinery Telematics IoT Machinery
Candidates Portal Employee Self-Service Portal
Suppliers Invoice Reconciliation Portal
Request for Inspection (RFI)
Site Progress Construction Daily Log
Certifications and Approvals
Site Item Request (SIR)
Site Labour Productivity
Machinery Scheduling and Utilization
Budgeting
Camp Mgt
Warehouse Mgt
Document Management - Workflow Engine
Common Data Environment - Business Analytics
ProjectVIEW ERP Core Module
Tendering Bidding
Cost Control
Subcontractors Management
Procurement and Purchasing
Materials and Production Mgt.
Machinery Maintenance
HRMS Payroll
Accounting Finance Mgt.
Suppliers Accounts Payables
Customers Accounts Receivable
Modules in offices
Apps on-site
Addons/Extras
Foundations

All modules have been designed under the same concept and they offer the same user interface. Modules process information from one department to another, if that is required. The linkage between the modules can be progressive to support initial stages. This structure offers your company the potential to activate the system progressively, according to its requirements. With the selection of any Suite's Module installation, **foundation (Core) modules** are a prerequisite.

Foundation modules create part of the administration panel providing low-level interconnectivity and functionality:

3.4.14 DANAOS ProjectVIEW ERP Modules

DANAOS ProjectVIEW ERP requires a set of Core Modules that facilitate system initialization and operations and maintain the consistency of processes and security of access. Furthermore, Core Modules meet the IEEE security requirements in respect of functional permissions and information access permissions. All functional permissions are maintained from the fleet management system while the information access permissions are maintained in the database level. This way the user can access only the information based on the database rights no matter what tool he/she may use. Regarding the functions within the applications, they are restricted to specific roles. Every user may be assigned one or more roles.

This way security requirements are maintained consistently in a quality and user-friendly manner.

User/Roles Management	Identity and access management for users and groups creation and setup. Users register, log in, and log out based in permissions that extend to enterprise Single Sign-On Manager based on organizational roles and policies via Windows Active Directory/LDAP
Workflows – Business Process Management	An easy-to-use application that allows digitalization of approval workflows with multiple checkpoints, users alerts and warnings facilitating interdepartmental collaboration and securing document circulation
Company's Projects Organizational and Operational Structure	Setup multiple levels of Company, Projects, Sub-Projects, Areas, Units, Departments etc. to facilitate Project Portfolio Management.

Templates and Print outs	Setup company standard templates and correspondence documentation. Associate templates with processes and users' signatures/rights.
Menu Selections and Parameterization	Arranged in a Menu hierarchical structure with visible and hidden control buttons, selections and items to administer access-control functionality. Toggle on/off system parameters in order to restrict flows and integrity checks between processes, data and users.
KPI	Create Alerts, Setup Warnings and Design Standard Reports/Dashboards for each entity and attribute.
Business Analytics	Insert the data warehouse file foundations for DANAOS Business Analytics. Activate on-demand.

3.4.15 Organizational Information Security – Security Assessment

DANAOS Secure development lifecycle system is safeguarded based on the above principles and processes. Considering the nature of the data handled, all DANAOS employees have signed and honored a strict confidentiality agreement. As part of DANAOS HR policies, all employees go through relevant to their academic, professional and civil background checks

Closely working both remotely and in person with several Clients over the years, DANAOS employees are fully aware of the required security processes of each Client, prior of engaging into any operations.

3.4.16 Applications Specifics and Blueprints

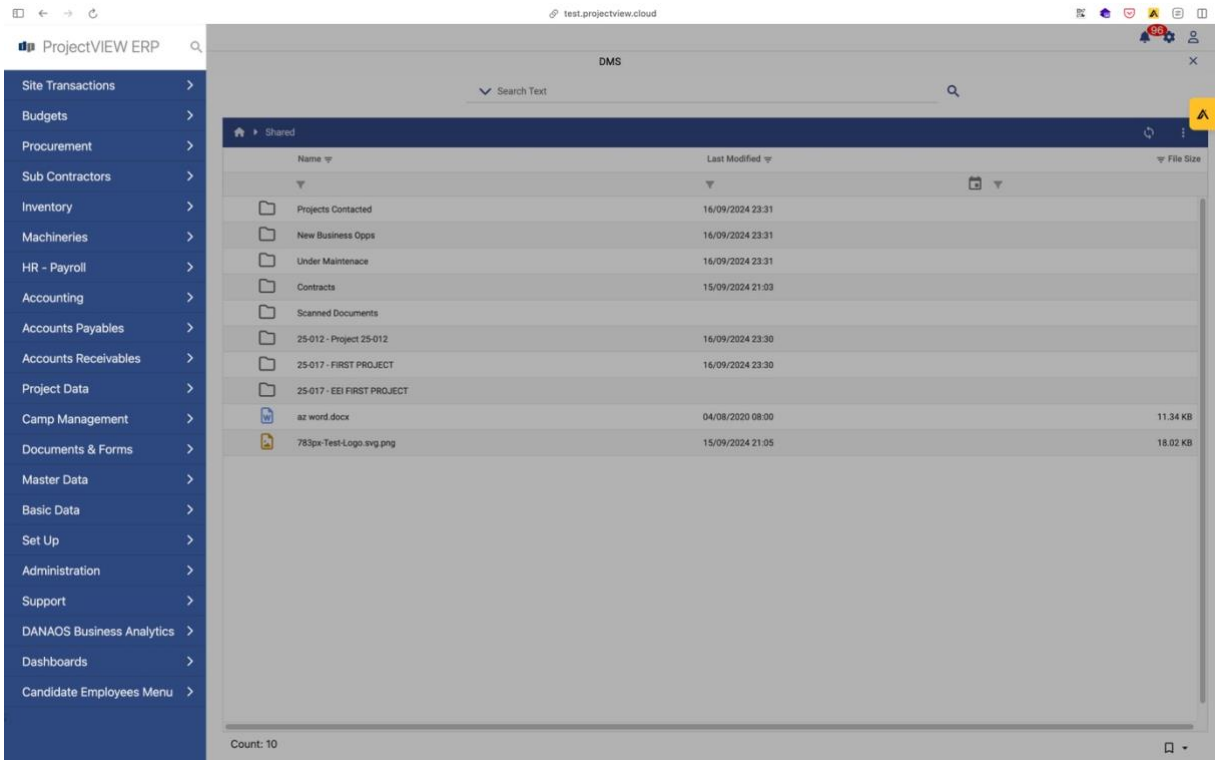
- The operating system for the Application Server is Microsoft Windows 64bit using the latest version (after 2022) since http2 is supported, which improves performance on multiple server requests.
- DANAOS Business Analytics also runs on QLIK Cloud
- Several support utilities and applications like synchronization run as Windows desktop applications and run on Windows Servers or Windows PC's
- Operating system for SQL Server 2022 (Web, Standard or Enterprise Edition) Database is Microsoft Windows

Server Side:

- .NET 8 C# MVC architecture
- Windows Server IIS for hosting the app
- Connection to database using .net System.Data.SqlClient . Entity Framework - ORMs for accessing the database
- JWT Authentication tokens or Session-based Authentication
- Single access to database: application user access, groups and rules proprietary handled by our DANAOS Web Enterprise framework
- SignalR for websocket communications

Client Experience:

- Authenticator for external (public) login
- Several JS frameworks including but not limited to DevExtreme, jQuery, Bootstrap
- All DANAOS Web Enterprise modules are hosted in a Single Page Application with each module having its own tab, as in the below picture.



Business Analytics:

DANAOS Management Consultants has a strategic partnership with QLIK that is powering our DANAOS Business Analytics module (optional). QlikSense Server from QLIK is hosted on Qlik Cloud

3.4.17 Interfacing with SAP/Oracle

Our current cases with interfacing with SAP:

- DANAOS Daemon runs and sends data from these tables to SAP through web services (wsdls)
- SAP returns a success msg with SAP document No. created or error msg with error indication
- Oracle Integration with Oracle P6 is succeeded via a custom app via P6 integration API

Upon request, DANAOS can develop any other interface or API with internal or external systems

3.4.18 Active Directory and SSO solutions

Microsoft Active Directory is read by our ProjectVIEW ERP to validate the user can login. We do not read or set credentials (passwords) in AD.

3.4.19 High Availability or redundancy within the Solution.

We do not provide our own solutions for high availability but rather utilize solutions via the Microsoft partnership. Database redundancy is also provided via our DATABASE and Microsoft partnership.

3.4.1 Password Composition

In the Production environment, the system is configured to require complex passwords (alpha and numeric characters, uppercase, and special characters) to reduce the likelihood of compromised passwords. In addition, users should be instructed not to use easily guessed passwords (e.g., words found in a dictionary, a variation on the user name, personal interests, etc.). Please refer to Password Complexity for more details.

3.4.2 Database data is available in the event of hardware failure

Backup execution can be georedundant if required by the Client.

3.4.3 Connections to the databases are controlled and monitored

Public access to the database is disabled by default. Only resources within the same Virtual Network can access the database.

Private endpoints to further restrict access to the database.

3.4.4 Access levels within the Database

User access is granted at the lower levels of the database (schema or table level). While access to the higher levels (instances) should be limited to database administrators.

Access is granted at individual database levels through roles, not individual IDs.

For databases that rely on application-level security, users and database administrators do not have direct update/write access to the production tables; production tables are only updateable via applications.

3.4.5 Default system accounts are properly secured by the DBA

Since leaving default accounts active and with default passwords provides an easy entry point for unauthorized access, it is highly likely that authorized users and attackers will attempt to log in to the database using the vendor-supplied default accounts. For this reason, the DBA should disable all default accounts and/or change default passwords.

3.4.6 Password Parameters

Passwords for Database Administration Accounts – Passwords associated with each database administration account should be different for each database instance.

3.4.7 Database control files

A database creates a number of files that are of paramount importance in the operation of a database and contain sensitive information. If unauthorized parties can modify these files, the database's security can be adversely affected.

3.4.8 Application Passwords

Third-party applications do not store weakly encrypted and clear- text passwords in the Database database. Verify that Third party applications do not store weakly encrypted and clear-text passwords in the database.

3.4.9 Database password authentication

Passwords are not sent in clear text during the login and transmission from client to server. Verify with the DBA whether any of the Database Advanced Security authentication methods have been implemented, e.g., KERBEROS-RADIUS (Remote Authentication Dial-In User Service) or DCE (Distributed Computing Environment) - Secure Sockets Layer (with digital certificates)

3.4.10 Remove all "system' privileges

The PUBLIC role is a built-in role that includes all users in the database. When a system privilege is granted to the PUBLIC role, the privilege is effectively granted to all users in the database. If inappropriate, these privileges can be used to gather sensitive information about the system, such as database and usernames. This in turn can assist in compromising the systems security.

3.4.11 Minimum permissions and roles

The correct definition and assignment of roles is essential to preserve the security principles of least privilege and segregation of duties. If users belong to roles and inappropriate privileges are assigned, users may be able to execute unauthorized transactions and compromise the integrity of the database.

3.4.12 DBA Remote Access

Knowledgeable users could make use of SQL*Plus or TOAD utilities to gain access to the database at a lower level and view tables and queries, which they would otherwise not have permission to view or modify when they access the database through an application server

3.4.13 Users unique ID's

All users including database administrators, end- users requiring ad-hoc reporting access, developers, and production support are assigned individual user logins. Obtain a list of all people who require access to the database and verify that each person has their own login and that no shared accounts are used to connect to the database.

User IDs should conform to a standard enterprise-wide naming convention: Review the listing of accounts with the System Administrator. Determine if account names comply with organizational naming standards and confirm the existence of policies and procedures to ensure all accounts are created to conform to the organization's naming standards

3.4.14 Account Lockout

Database user accounts are configured to lock users out after a certain number of failed login (specify this number) attempts within a set time frame (specify time frame).

3.4.15 Privilege Management

Appropriate privileges are set for all database users and administrators.

3.4.16 Auditing

Database auditing is configured to track key system and user activity, including actions performed by administrators and vendors, and all failed login attempts captured are reviewed in a timely manner (specify how this is being done).

- Logging Application Account Activity: The "auditing" control is configured so that all sensitive system actions and object modifications performed by application accounts are written to the audit trail.
- Log Failed Attempts to Access Objects: All failed attempts to access objects are logged and followed up
- Log File Retention: Log files are retained for an adequate time period

3.4.17 Transparent Data Encryption

Database Advanced Security Transparent Data Encryption (TDE) stops would-be attackers from bypassing the database and reading sensitive information from storage by enforcing data-at-rest encryption in the database layer. Applications and users authenticated to the database continue to have access to application data transparently (no application code or configuration changes are

required), while attacks from OS users attempting to read sensitive data from tablespace files and attacks from thieves attempting to read information from acquired disks or backups are denied access to the clear text data.

Out of the box, TDE provides industry-standard strong encryption for the database, full key lifecycle management, and integrated support for Database tools and technologies. TDE enables encryption of database columns or entire application tablespaces. Its high-speed cryptographic operations make performance overhead negligible in most applications. The two-tier encryption key architecture provides easy administration of keys, enforces clear separation of keys from encrypted data, and provides assisted key rotation – without having to re-encrypt data. The keystore can be managed using a convenient web console in Database Enterprise Manager or using a command-line.

3.5 Notifications for breaching

DANAOS notifies the client immediately, providing full transparency on the breaching process and the extent of the data leakage

Both procedures below assure that DANAOS has the required controls to restrict access to systems and data.

3.6 Systems Access Removal Policy

Access to the network and IT services is revoked by the DANAOS Global Admin upon receiving approval from the DANAOS Project Manager. This control provides a degree of protection for all DANAOS corporate applications as Access is limited to the network. This Policy safeguards that prior to any action by the Global Admin both DANAOS and Client are well notified in advance

3.7 Application Access Removal Policy

This Policy is used to delete any existing user access rights and is used to make sure the resultant user's structure is properly configured for a given app and will produce the desired outcome when applied to a module. Access to the Applications Core Modules (User/Roles Management) is the responsibility of the Applications' Admin. Access Rights modifications are all recorded in the Applications Log History

3.8 Deployment Procedure

1	DANAOS cloud environment administrators will create the two (2) aforementioned virtual	Up to Client to choose the remote connectivity platform	

	machines and provide remote access to DANAOS DevOps team.		
2	DANAOS DevOps team installs and configure SQLSERVER RDBMS	Activation of common language runtime (CLR) , which provides the execution environment for .NET Create needful databases Create needful database users	
3	DANAOS DevOps team installs and configures the IIS server	Enable the needful IIS Roles and features	FeatureName:IIS-ApplicationDevelopment FeatureName:IIS-ASP FeatureName:IIS-ASPNET FeatureName:IIS-BasicAuthentication FeatureName:IIS-CGI FeatureName:IIS-ClientCertificateMappingAuthentication FeatureName:IIS-CommonHttpFeatures FeatureName:IIS-CustomLogging FeatureName:IIS-DefaultDocument FeatureName:IIS-DigestAuthentication FeatureName:IIS-DirectoryBrowsing FeatureName:IIS-FTPExtensibility FeatureName:IIS-FTPServer

			FeatureName:IIS-FTPSvc FeatureName:IIS-HealthAndDiagnostics FeatureName:IIS-HostableWebCore FeatureName:IIS-HttpCompressionDynamic FeatureName:IIS-HttpCompressionStatic FeatureName:IIS-HttpErrors FeatureName:IIS-HttpLogging FeatureName:IIS-HttpRedirect FeatureName:IIS-HttpTracing FeatureName:IIS-IIS6ManagementCompatibility FeatureName:IIS-IISCertificateMappingAuthentication FeatureName:IIS-IPSecurity FeatureName:IIS-ISAPIExtensions FeatureName:IIS-ISAPIFilter FeatureName:IIS-LegacyScripts FeatureName:IIS-LegacySnapIn FeatureName:IIS-LoggingLibraries FeatureName:IIS-ManagementConsole FeatureName:IIS-ManagementScriptingTools FeatureName:IIS-ManagementService

			FeatureName:IIS-Metabase FeatureName:IIS-NetFxExtensibility FeatureName:IIS-ODBCLogging FeatureName:IIS-Performance FeatureName:IIS-RequestFiltering FeatureName:IIS-RequestMonitor FeatureName:IIS-Security FeatureName:IIS-ServerSideIncludes FeatureName:IIS-StaticContent FeatureName:IIS-URLAuthorization FeatureName:IIS-WebDAV FeatureName:IIS-WebServer FeatureName:IIS-WebServerManagementTools FeatureName:IIS-WebServerRole FeatureName:IIS-WindowsAuthentication FeatureName:IIS-WMICompatibility FeatureName:WAS-ConfigurationAPI FeatureName:WAS-NetFxEnvironment FeatureName:WAS-ProcessModel FeatureName:WAS-WindowsActivationService FeatureName:NetFx3 FeatureName:IIS-ASPNET45 FeatureName:WCF-HTTP-Activation

			FeatureName:WCF-HTTP-Activation45 FeatureName:IIS-WebSockets FeatureName:IIS-ApplicationInit FeatureName:IIS-CertProvider
4	DANAOS DevOps team installs and configures the SaaS	Copy the web application files Setup connection with the database Create dedicated Application Pool Create Web Site Modify the global web site preferences	
5	DevOps team overall testing		

4. DANAOS AGILE METHODOLOGY

Developed in 2009, DANAOS Agile software development is an integral part of DANAOS methodologies based on the most revered agile manifesto that laid down the principles and core practices.

DANAOS Agile is a set of techniques followed by a team to administer a project or plan by dividing it into various stages with continuous collaboration with customers. There is constant monitoring at every phase of the software development of the project. The agile methodology advantages are that both the development plus testing actions are parallel and synchronized, unlike the conventional waterfall methodology.

More specifically, DANAOS Agile Methodology is based on the Agile Scrum development methodology, which is depicted by various cycles of development. Similar to Kanban, Scrum breaks down the development phases into stages or cycles called ‘sprints’. The development time for each sprint is maximized and dedicated, thereby managing only one sprint at a time.

Scrum and agile methodologies focus on continuous deliverables, and thus this method lets designers adjust priorities to ensure that any incomplete or overdue sprints get more attention. Scrum Team has exclusive project roles such as a scrum master and a product owner with constant communications on the daily scrum where the activities are harmonized to devise the best way to implement the sprint

4.1 SDLC (Software Development Lifecycle)

1. Planning and requirements
2. Architecture and design
3. Test planning
4. Coding
5. Testing and results
6. Release and maintenance

In alignment with Microsoft development frameworks and Microsoft Azure Cloud, DANAOS follows:

4.1.1 Practice #1 - Provide Training

Security is everyone's job. Developers, service engineers, and program and product managers must understand security basics and know how to build security into software and services to make products more secure while still addressing business needs and delivering user value.

Effective training will complement and re-enforce security policies, SDL practices, standards, and requirements of software security, and be guided by insights derived through data or newly available technical capabilities.

Although security is everyone's job, it's important to remember that not everyone needs to be a security expert nor strive to become a proficient penetration tester. However, ensuring everyone understands the attacker's perspective, their goals, and the art of the possible will help capture the attention of everyone and raise the collective knowledge bar.

4.1.2 Practice #2 - Define Security Requirements

The need to consider security and privacy is a fundamental aspect of developing highly secure applications and systems and regardless of development methodology being used, security requirements must be continually updated to reflect changes in required functionality and changes to the threat landscape. Obviously, the optimal time to define the security requirements is during the initial design and planning stages as this allows development teams to integrate security in ways that minimize disruption. Factors that influence security requirements include (but are not limited to) the

legal and industry requirements, internal standards and coding practices, review of previous incidents, and known threats. These requirements should be tracked through either a work-tracking system or through telemetry derived from the engineering pipeline.

4.1.3 Practice #3 - Define Metrics and Compliance Reporting

It is essential to define the minimum acceptable levels of security quality and to hold engineering teams accountable to meeting that criteria. Defining these early helps a team understand risks associated with security issues, identify and fix security defects during development, and apply the standards throughout the entire project. Setting a meaningful bug bar involves clearly defining the severity thresholds of security vulnerabilities (for example, all known vulnerabilities discovered with a “critical” or “important” severity rating must be fixed with a specified time frame) and never relaxing it once it's been set.

In order to track key performance indicators (KPIs) and ensure security tasks are completed, the bug tracking and/or work tracking mechanisms used by an organization (such as Azure DevOps) should allow for security defects and security work items to be clearly labeled as security and marked with their appropriate security severity. This allows for accurate tracking and reporting of security work.

4.1.4 Practice #4 - Perform Threat Modeling

Threat modeling should be used in environments where there is meaningful security risk. Threat modeling can be applied at the component, application, or system level. It is a practice that allows development teams to consider, document, and (importantly) discuss the security implications of designs in the context of their planned operational environment and in a structured fashion.

Applying a structured approach to threat scenarios helps a team more effectively and less expensively identify security vulnerabilities, determine risks from those threats, and then make security feature selections and establish appropriate mitigations.

4.1.5 Practice #5 - Establish Design Requirements

The SDL is typically thought of as assurance activities that help engineers implement “secure features”, in that the features are well engineered with respect to security. To achieve this, engineers will typically rely on security features, such as cryptography, authentication, logging, and others. In many cases, the selection or implementation of security features has proven to be so complicated that design or implementation choices are likely to result in vulnerabilities. Therefore, it’s crucially important that these are applied consistently and with a consistent understanding of the protection they provide.

4.1.6 Practice #6 - Define and Use Cryptography Standards

With the rise of mobile and cloud computing, it's critically important to ensure all data, including security-sensitive information and management and control data, is protected from unintended disclosure or alteration when it's being transmitted or stored. Encryption is typically used to achieve this. Making an incorrect choice in the use of any aspect of cryptography can be catastrophic, and it's best to develop clear encryption standards that provide specifics on every element of the encryption implementation. This should be left to experts. A good general rule is to only use industry-vetted encryption libraries and ensure they're implemented in a way that allows them to be easily replaced if needed.

4.1.7 Practice #7 - Manage the Security Risk of Using Third-Party Components

Today, the vast majority of software projects are built using third-party components (both commercial and open source). When selecting third-party components to use, it's important to understand the impact that a security vulnerability in them could have to the security of the larger system into which they are integrated. Having an accurate inventory of third-party components and a plan to respond when new vulnerabilities are discovered will go a long way toward mitigating this risk, but additional validation should be considered, depending on your organization's risk appetite, the type of component used, and potential impact of a security vulnerability. Learn more about managing security risks of using third-party components such as open source software.

4.1.8 Practice #8 - Use Approved Tools

Define and publish a list of approved tools and their associated security checks, such as compiler/linker options and warnings. Engineers should strive to use the latest version of approved tools, such as compiler versions, and to take advantage of new security analysis functionality and protections.

4.1.9 Practice #9 - Perform Static Analysis Security Testing (SAST)

Analyzing the source code prior to compilation provides a highly scalable method of security code review and helps ensure that secure coding policies are being followed. SAST is typically integrated into the commit pipeline to identify vulnerabilities each time the software is built or packaged. However, some offerings integrate into the developer environment to spot certain flaws such as the existence of unsafe or other banned functions and replace those with safer alternatives as the developer is actively coding. There is no one size fits all solution and development teams should decide

the optimal frequency for performing SAST and maybe deploy multiple tactics—to balance productivity with adequate security coverage.

4.1.10 Practice #10 - Perform Dynamic Analysis Security Testing (DAST)

Performing run-time verification of your fully compiled or packaged software checks functionality that is only apparent when all components are integrated and running. This is typically achieved using a tool or suite of prebuilt attacks or tools that specifically monitor application behavior for memory corruption, user privilege issues, and other critical security problems. Similar to SAST, there is no one-size-fits-all solution and while some tools, such as web app scanning tools, can be more readily integrated into the continuous integration / continuous delivery pipeline, other DAST testing such as fuzzing requires a different approach.

4.1.11 Practice #11 - Perform Penetration Testing

Penetration testing is a security analysis of a software system performed by skilled security professionals simulating the actions of a hacker. The objective of a penetration test is to uncover potential vulnerabilities resulting from coding errors, system configuration faults, or other operational deployment weaknesses, and as such the test typically finds the broadest variety of vulnerabilities. Penetration tests are often performed in conjunction with automated and manual code reviews to provide a greater level of analysis than would ordinarily be possible.

4.1.12 Practice #12 - Establish a Standard Incident Response Process

Preparing an Incident Response Plan is crucial for helping to address new threats that can emerge over time. It should be created in coordination with your organization's dedicated Product Security Incident Response Team (PSIRT). The plan should include who to contact in case of a security emergency, and establish the protocol for security servicing, including plans for code inherited from other groups within the organization and for third-party code. The incident response plan should be tested before it is needed!

4.2 IT Change Management

DANAOS Customization services aim in building a high-quality product aligned with the Client's specifications, dealing with the dynamic work environment. In the Agile development world, change is constant. New non-functional and functional requirements can appear unexpectedly, while established requirements can shift multiple times. Failing to manage those new requirements can lead to project failure.

A good change management process ensures the following in your organization:

- Prevention of accidents
- Increase in asset reliability
- Traceability of changes
- Evaluation of alternative

Change management involves coordinating resources, applying tools, and managing a project plan to effectively execute the “transformation” of each DANAOS Systems (Software + IT Infrastructure) to the Client’s Solution.

DANAOS Change management practices are designed to reduce incidents and meet regulatory standards. The practices ensure efficient and prompt handling of changes to IT infrastructure and code. Whether rolling out new services, managing existing ones, or resolving problems in code, modern change management approaches break down silos, provide context and transparency, avoid bottlenecks, and minimize risk.

4.3 Backups and database exports

DANAOS recommends that database backups are made *regularly* and tested for quality:

- The DB every 12 hours.
- The application every 1 hour.
- The file storage daily.

5. AZURE SECURITY AND BUSINESS CONTINUITY

The following standard practices are used to achieve security and business continuity in Azure cloud services.

5.1 Security

1. Access to cloud resources
    a. Access to Azure online administration services is performed by authorized personnel, using two-factor authentication.
    b. Role-based access security is used to determine the access level of the resources.
2. Virtual Machines
    a. Remote Desktop is primarily disallowed.
    b. Access to VMs (RDP) is allowed for limited time slots, specific users and IPs, specified dynamically per access request, using Just In Time Administration protocols, or VPN.
    c. Disk Encryption is used to protect data at rest.
    d. Basic firewall functionality is provided by inbound at outbound port rules, using network security groups.
    e. Azure Security Center is used for Security alerts, log incidents and to provide security recommendations.
    f. All applications are kept up to date.
    g. Microsoft Defender or BitDefender can be used as the antivirus of choice for the VM's OS.
    h. Resource Health monitors the VMs and checks if they are running as expected, and if there exist any known Azure platform problems that affect the existing resources.
3. SQL Server
    a. Non standard ports and user names are used.
    b. Each database has it's own user.
    c. Data is encrypted at rest and in transit.
    d. SQL Advanced Threat Protection is used to detect and respond to potential threats as they occur by providing security alerts on anomalous activities. It provides alerts upon suspicious database activities, potential vulnerabilities, and SQL injection attacks, as well as anomalous database access and queries patterns.

e. SQL Vulnerability Assessment is used to employ a knowledge base of rules that flag security vulnerabilities. It highlights deviations from best practices, such as misconfigurations, excessive permissions, and unprotected sensitive data.

4. Networking
    a. SSL/TLS can be used to encrypt data in transit for all web applications
    b. SSL/TLS can be used to encrypt data in transit for SQL Server access
    c. Point to Site VPN is used to provide secure connectivity between mobile apps and the cloud Servers.
    d. Azure Network Watcher is used to monitor, diagnose and repair the network health of (Infrastructure-as-a-Service) products which includes Virtual Machines, Virtual Networks, Application Gateways etc.

5.2 Disaster Recovery and Business Continuity (Backup)

5.2.1 Virtual Machines

Daily VM backup is performed. Backups can be restored to the same VM, or to new VM instances.

5.2.2 SQL Server

Daily Database Backups are performed with a 7-day retention period. Extra features:

1. Customized, higher frequency, or longer retention backups can be set up after request.
2. A secondary server with read-only replicas of the databases can be setup, with high frequency backups (up to 15-minute intervals). In case of a disaster in the primary VM, this secondary VM takes over as the primary VM and database access is continued with minimal potential data and time loss.

5.2.3 Azure Backup

Azure backup-as-a-service is used to perform automated backups for system/apps and data using specified/customizable policies.

5.3 Customer Data Protection

Access to customer data by Microsoft operations and support personnel is denied by default. When access to data related to a support case is granted, it is only granted using a just-in-time (JIT) model using policies that are audited and vetted against our compliance and privacy policies. The access-control requirements are established by the following Azure Security Policy:

- No access to customer data, by default.
- No user or administrator accounts on customer virtual machines (VMs).
- Grant the least privilege that's required to complete task; audit and log access requests.

5.3.1 Data protection

Azure provides customers with strong data security, both by default and as customer options.

- At-rest data protection: Customers are responsible for ensuring that data stored in Azure is encrypted in accordance with their standards. Azure offers a wide range of encryption capabilities, giving customers the flexibility to choose the solution that best meets their needs. Azure Key Vault helps customers easily maintain control of keys that are used by cloud applications and services to encrypt data. Azure Disk Encryption enables customers to encrypt VMs. Azure Storage Service Encryption makes it possible to encrypt all data placed into a customer's storage account.

- In-transit data protection: Microsoft provides a number of options that can be utilized by customers for securing data in transit internally within the Azure network and externally across the Internet to the end user. These include communication through Virtual Private Networks (utilizing IPsec/IKE encryption), Transport Layer Security (TLS) 1.2 or later (via Azure components such as Application Gateway or Azure Front Door), protocols directly on the Azure virtual machines (such as Windows IPsec or SMB), and more.

Additionally, "encryption by default" using MACsec (an IEEE standard at the data-link layer) is enabled for all Azure traffic traveling between Azure data centers to ensure confidentiality and integrity of customer data.

Data redundancy: Microsoft helps ensure that data is protected if there is a cyberattack or physical damage to a datacenter. Customers may opt for:

- In-country/in-region storage for compliance or latency considerations.
- Out-of-country/out-of-region storage for security or disaster recovery purposes.

When you create your storage account, select one of the following replication options:

- Locally redundant storage (LRS): Locally redundant storage maintains three copies of your data. LRS is replicated three times within a single facility in a single region. LRS protects your data from normal hardware failures, but not from a failure of a single facility.

- Zone-redundant storage (ZRS): Zone-redundant storage maintains three copies of your data. ZRS is replicated three times across two to three facilities to provide higher durability than LRS. Replication occurs within a single region or across two regions. ZRS helps ensure that your data is durable within a single region.
- Geo-redundant storage (GRS): Geo-redundant storage is enabled for your storage account by default when you create it. GRS maintains six copies of your data. With GRS, your data is replicated three times within the primary region. Your data is also replicated three times in a secondary region hundreds of miles away from the primary region, providing the highest level of durability. In the event of a failure at the primary region, Azure Storage fails over to the secondary region. GRS helps ensure that your data is durable in two separate regions.

Data destruction: When customers delete data or leave Azure, Microsoft follows strict standards for overwriting storage resources before their reuse, as well as the physical destruction of decommissioned hardware. Microsoft executes a complete deletion of data on customer request and on contract termination.

5.3.2 Customer data ownership

Microsoft does not inspect, approve, or monitor applications that customers deploy to Azure. Moreover, Microsoft does not know what kind of data customers choose to store in Azure. Microsoft does not claim data ownership over the customer information that's entered into Azure.

5.3.3 Records management

Azure has established internal records-retention requirements for back-end data. Customers are responsible for identifying their own record retention requirements. For records that are stored in Azure, customers are responsible for extracting their data and retaining their content outside of Azure for a customer-specified retention period.

Azure allows customers to export data and audit reports from the product. The exports are saved locally to retain the information for a customer-defined retention time period.

5.3.4 Electronic discovery (e-discovery)

Azure customers are responsible for complying with e-discovery requirements in their use of Azure services. If Azure customers must preserve their customer data, they may export and save the data locally. Additionally, customers can request exports of their data from the Azure Customer Support

department. In addition to allowing customers to export their data, Azure conducts extensive logging and monitoring internally.

5.4 Security Key Points

Key Points	DANAOS
Application Security: (Tools & Processes) (WAF, Secure Code Review, VA/PT)	DANAOS ProjectVIEW ERP enables native WAF connectivity (WAF Agnostic) where all applications are securely rendered via Web Application Firewall Providers (eg. Cloudflare) in order to shield against cybercriminals. As a standard process, vulnerability analysis/penetration testing (VA/PT) is an ongoing active process of identifying existing vulnerabilities and available exploits in our security implementation and hosting (OpenVAS).
Master Data Management (Integration and interface with centrally governed MDG solution has been defined. MDM at individual application level must be strictly avoided.)	DANAOS Applications integrations' policies in B2G interconnectivity differ from region to region and country to country. Our MDM policies require a middleware process bridging business and Information Technology data assuring uniformity, accuracy, stewardship, semantic consistency and accountability bilaterally in all master data assets.
Data duplication to be avoided – the application is not creating duplicate data (Master data or Transaction data)	DANAOS ProjectVIEW ERP is based on the concept of the Single Source of Truth. Data is entered once. System facilitates automation and securing of data input. A business-specific controlled environment governs user roles and access rights whilst assuring process integrity
Data Sharing - Application supports API for data sharing with other applications in the organization's landscape	Based on their purpose-specific process, DANAOS applications have a native Web API, which can be used in various scenarios and is configurable at will. It provides access to needed data, and can also implement actions at DANAOS database. It includes token-based authentication – authorization. DANAOS API is used in several common integrations processes (SAP, Database ERP, Government Agencies, Banks, Other construction software) to access or input data.

Periodic Assessment & Testing (Internal assessment, external audits etc.)	DANAOS ProjectVIEW ERP is frequently assessed from Independent cybersecurity organizations with Vulnerability Tests and Penetrations Tests. Based on the needs of each Client, DANAOS can allow independent testing and take specific actions when required.
Third party components usage: (Process to validate and review usage of open source and third-party components as part of security requirements definition, scan source code using security tools and remediate identified Vulnerabilities)	Under the master general VA and PT (vulnerability assessment and penetration testing) process, DANAOS embedded third-party applications and add-ons are treated in the same manner as native DANAOS programming objects assuring consistency and interdependency and the overall integrity of the system –as one.
Change control procedures followed?	Upon system initialization, GAP Analysis indicates and prioritizes the necessary backlog requirements. MoSCoW techniques is used to setup the planning and the implementation splints (SCRUM – Agile methodology). Change Requests and Issue Log is tracked, monitored, managed and rectified based on continuous (iterative and incremental) ISO-approved processes and deliverables.
Audit Trail availability: (User, user actions & Critical Transaction)	DANAOS ProjectVIEW ERP is equipped and maintain a record of system activity both by system and application processes and by user activity of systems and applications. DANAOS ProjectVIEW ERP maintains a transaction log where upon login, all uses are timestamped, and all actions are recorded and monitored by the system. Rollback is available based on each business process and only from Admins.

6. APPENDIX

- Azure + Dynamics 365 (Public Government) Soc Bridge Letter April - June 2021.Pdf (1).pdf
- Microsoft Azure, Dynamics 365 and Online Services - Iso27001 and 27701 Certificate 12.18.2020 (2).pdf
- Microsoft Azure, Dynamics 365 and Online Services - Iso 27018 Certificate 12.18.2020 (3).pdf
- Professional Services Iso27001 Statement of Applicability (4).pdf
- Professional Services - 2020 Iso 27001 Assessment Certificate.Pdf (5).pdf
- Professional Services - 2020 Iso 27001 and 27018 Assessment Report.Pdf (6).pdf
- Professional Services - 2020 Iso 27018 Assessment Certificate.Pdf (7).pdf
- Microsoft Azure, Dynamics and Online Services Cyber Essential Plus 2021 - Report and Certificate.Pdf (8).pdf
- Microsoft Azure Commercial System Security Plan (Ssp) V3.6 20201124 (9).pdf
- Dynamics 365 Ens 2020-7-30.Pdf (10).pdf
- Azure Ens Certificate 2020-7-30.Pdf (11).pdf
- Microsoft Ame Iso 27001 and 27018 Certification Audit Report - 7.15.2019.Pdf (12).pdf
- Azure - Logging And Auditing.pdf
- Azure - Technical Capabilities.pdf
- Azure - Operational Security.pdf
- Azure - Network Security.pdf
- Azure - Cloud Security Diagnostic Tool.xlsx
- Msft Cloud Architecture Security (13).pdf
- Microsoft Cloud - Overview of General Data Protection Regulation (Gdpr) (14).pdf
- Microsoft Cloud - Enterprise Business Continuity Management (Ebcm) Program.Pdf (15).pdf
- Professional Services - Data Access Summary.Pdf (16).pdf
- Microsoft Professional Services Data Classification Summary.Pdf (17).pdf
- Exit Planning for Microsoft Cloud Services.Pdf (18).pdf
- Microsoft Security Program Policy (1).pdf
- Microsoft Security Program Policy.pdf
- Microsoft Response to Requests for Information.Pdf (19).pdf
- Azure Gdpr Control Mapping 5.24.18 (20).xlsx
- Professional Services Gdpr Control Mapping 10.29.19.Xlsx (21).xlsx
- DANAOS Azure Security and Business Continuity (22).docx

- Cloud SLA Agreement.docx
- Pci Dss 3.2.1 - Azure Kubernetes Service Shared Responsibility Matrix (24).xlsx
- Pci Dss 3.2.1 - Azure Shared Responsibility Matrix (25).xlsx
- Pci Dss 3.2.1 - Microsoft Azure Attestation of Compliance (26).pdf
- Pci Dss 3.2.1 - Microsoft Azure Government Attestation of Compliance (27).pdf