CSO Conference *& Awards*

Produced by CSO | IDC

Implementation of zero trust in document management

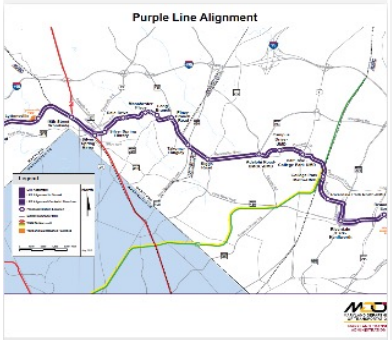
ABOUT OHLA USA

- $1.2 B USD heavy-civil general contracting company
- Multi-regional, multi-company organization
- 70 plus ongoing projects
- 550 salaried employees; over 1000 craft employees
- 15 functional units: Construction | Estimating | Business development | HR | Legal | Accounting | Payroll | Accounts payable | Equipment shop | Plant | Truckbase | Risk | Compliance | IT | Audit

Flood Mitigation Program at the Hugh L. Carey Tunnel and Queens Midtown Tunnel

Painting of Elevated Structures on the #7 Line

UHealth Lennar Foundation Medical Center

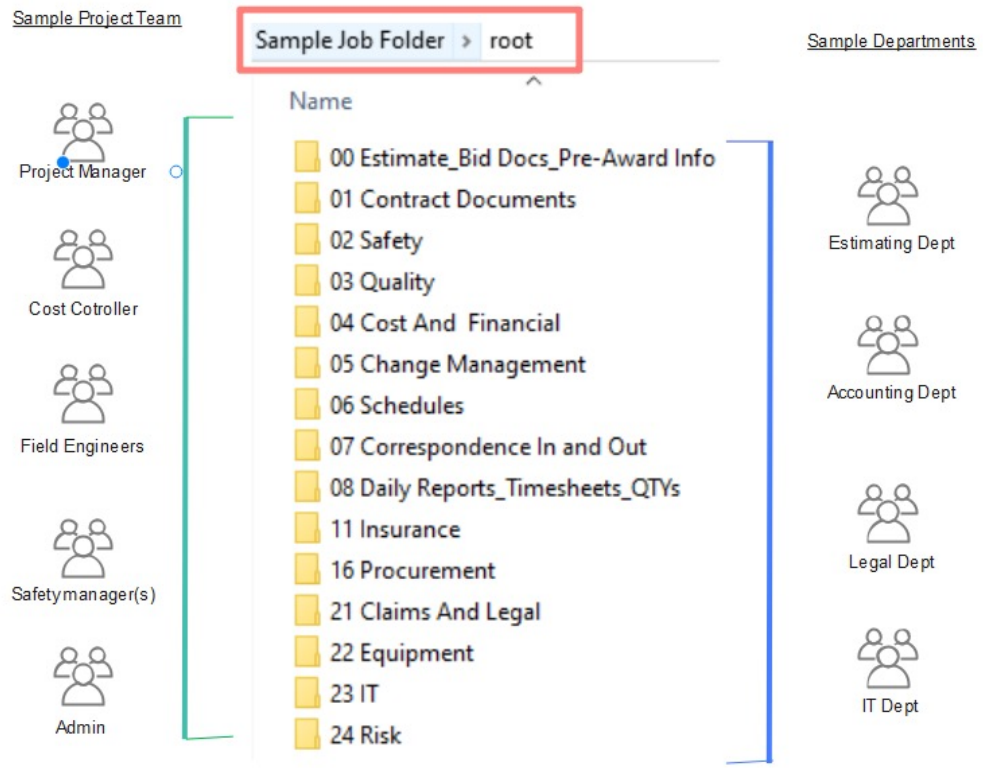


Purple Line Light Rail System

I-5 North Freeway Enhancements

Tucson Solar Power Plant

PRE-TRANSFORMATION



One file server with multiple drives hosting 80 terabytes (TB) of data, with departments and projects organized as subfolders, and NTFS based permissions assigned at the root level of each entity.

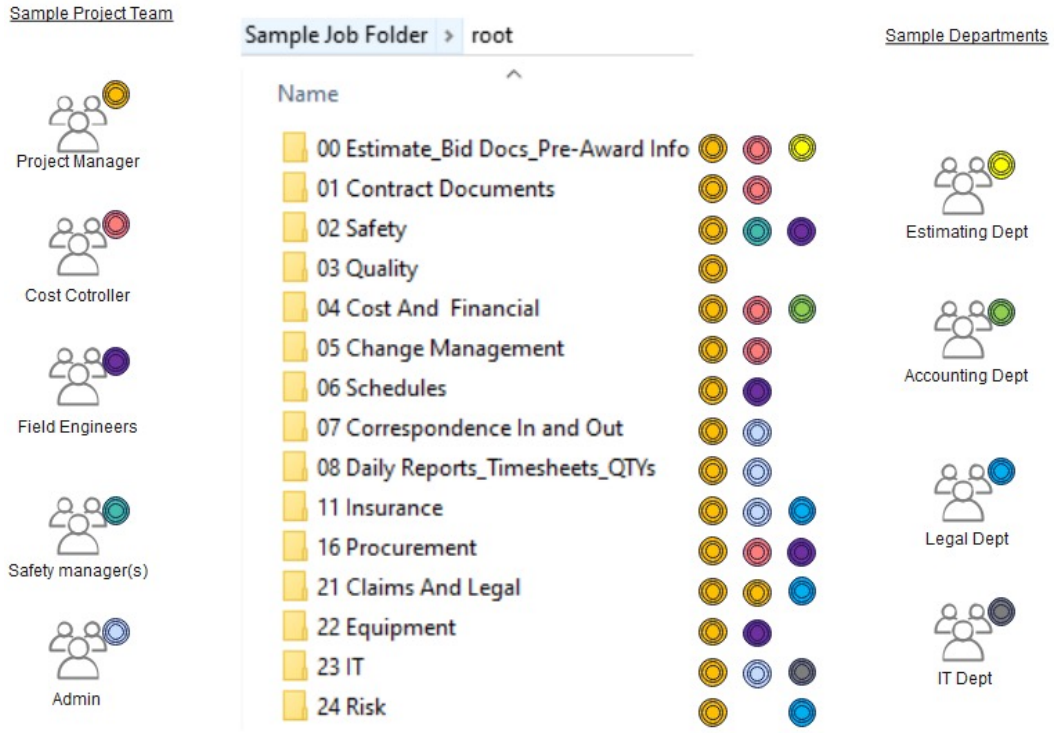
VULNERABILITIES

- Large Attack Surface
- Perimeter-based security
- Lack of Least Privilege Enforcement
- Permissions Misconfiguration
- High Recovery Time Actual (RTA) Compared to Recovery Time Objective (RTO)
- Achieving granular permission settings is costly
- Difficult to implement data loss prevention

THREATS

- Unauthorized Access and Insider Threats
- Data Breach and Malware/Ransomware Attacks
- Compliance Violations
- Data Exfiltration & Exposure
- Extended Downtime and Data Loss

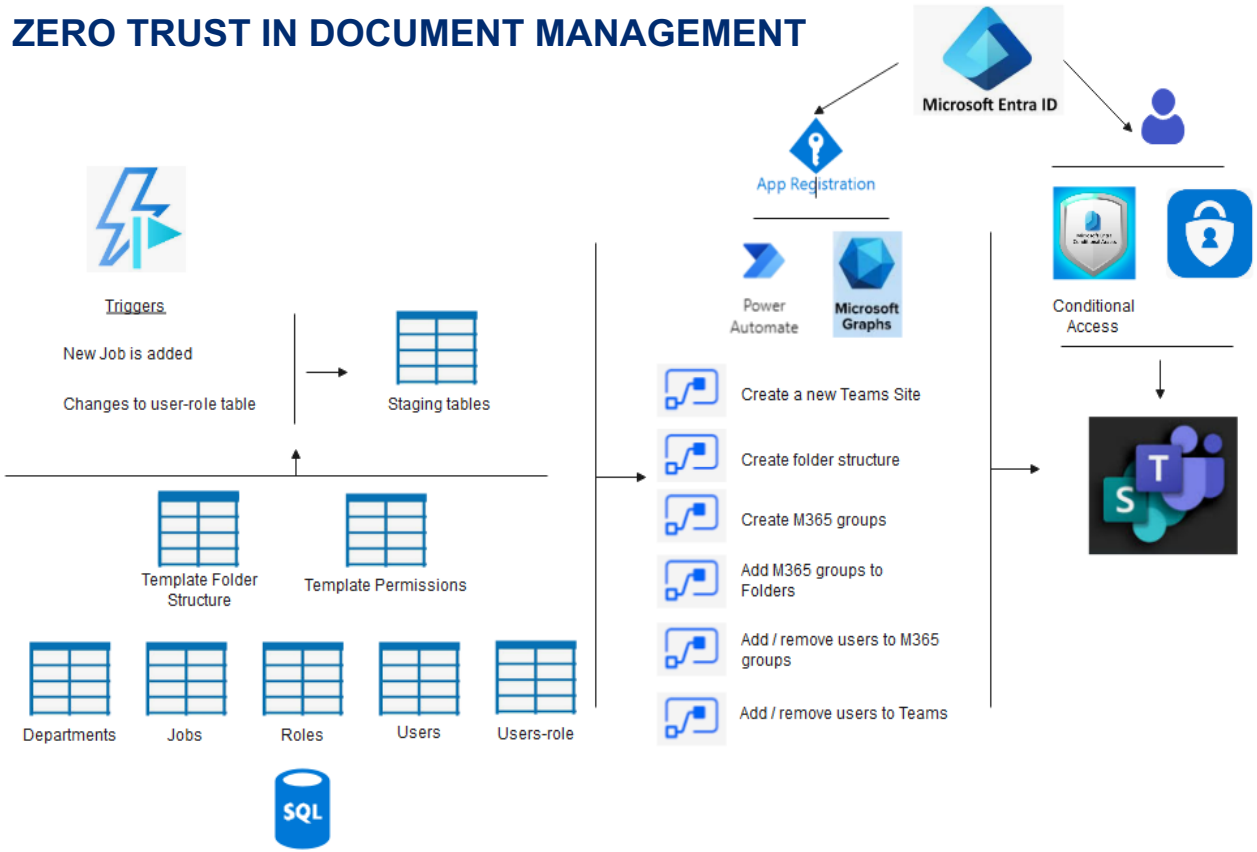
TRANSFORMED STATE



ZERO TRUST PRINCIPLES

- ✓ **Micro-Segmentation**
  - Each project is assigned a dedicated Teams site
  - Granular access control up to the second-level folders
- ✓ **Automation & Dynamic Policy Enforcement**
  - Automated access provisioning based on template configurations
  - Auto-revoking access based on inactivity, with a self-service option for users to regain access
- ✓ **Use Least Privilege Access**
  - administration tasks are automated and handled by service accounts, without human intervention
  - Access contained to specific folders based on role.
- ✓ **Verify Explicitly**
  - EntraID-based Multi-Factor Authentication (MFA)
  - Endpoints managed through Intune
  - Conditional access policies applied
- ✓ **Continuous Verification**
  - User access is tied to HR data for employee termination updates

ZERO TRUST IN DOCUMENT MANAGEMENT



ZERO TRUST PRINCIPLES

- ✓ **Micro-Segmentation**
  - Each project is assigned a dedicated Teams site
  - Granular access control up to the second-level folders
- ✓ **Automation & Dynamic Policy Enforcement**
  - Automated access provisioning based on template configurations
  - Auto-revoking access based on inactivity, with a self-service option for users to regain access
- ✓ **Use Least Privilege Access**
  - administration tasks are automated and handled by service accounts, without human intervention
  - Access contained to specific folders based on role.
- ✓ **Verify Explicitly**
  - EntraID-based Multi-Factor Authentication (MFA)
  - Endpoints managed through Intune
  - Conditional access policies applied
- ✓ **Continuous Verification**
  - User access is tied to HR data for employee termination updates

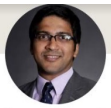
Key Enablers

- Deep understanding of SharePoint & Teams
- Information management needs of the business
- Microsoft Graph API
- Microsoft Power Automate
- *Unified Just-in-time Identity Management, a* 2023 CSO50 Award winning implementation – automates user account creation using Graph API and stores GUIDs for user accounts, needed for authorization automation
- Enterprise architecture database with roles & responsibility
- Custom software development

Next Steps..

- Zero trust in 3rd party collaboration

Happy to chat!



Srivatsan Raghavan
Chief Information Officer