Introduction

Saturday, April 9, 2022 3:23 PM

Personal objectives (Very Important)

- Performance contribution tracker; required for GL30
    - Focus on Data security. Add color commentary (context, examples, etc.) to your offering
- Sales - what are you hearing
- Utilization
- Practice development - keep focus on data security
- Demonstrate how you're performing at your level

Tips for Developing Yourself

- Make time for learning.
- Prioritize your development—if you don't, no one else will.
- Have a plan. Set goals that align to the practice you want to develop. Use the journal to document what you are learning.
- Involve your manager. They can provide additional insights and help you stay accountable.
- Involve others. Seek feedback from others.
- Keep going. The best learning happens when you are outside your comfort zone. This happens mostly through challenging on the job experiences, complimented by what you learn from others and through courses.
- Review: Complete self-skills sort annually, or, when your job/career changes.
- Link your goals: Update your DAP each year to support your MAP goals

++

Internal OAS SharePoint location: Data & Cloud Community of Practice - All Documents (sharepoint.com)

What Are the 34 CliftonStrengths Themes? | EN - Gallup

StrengthsFinder.pdf

++

Practice development

Are you performing at your level

++

[1:43 PM] Branshaw, Athena L

FYI - there is still a "meaningful conversations" folder in GROWTH OFFICE that is out dated it made it confusing when I was looking for this info. there is a new CHANNEL - in OI Provider Growth Office - Meaningful conversation with the files, tool kit, and market trends across the top that has been reviewing.
https://teams.microsoft.com/l/channel/19%3a1ef3c71561524df88b349252314a48e4%40thread.tacv2/Meaningful%2520Conversations?groupId=f2abeba5-e006-4f04-b502-5322e7dede68&tenantId=db05faca-c82a-4b9d-b9c5-0f64b6755421

++

OAS Training site: Percipio

+++

Optum EIS Security: https://hcp.uhg.com/security

One-on-one with Dinesh

Thursday, June 9, 2022 5:48 PM

Meeting 6/09/2022 with Dinesh
Subject: Catch up

To prepare collateral:

Start with why should you be concerned
Define what customer needs
What is the scope of the work to satisfy the client's why
Who will be doing it

The assessment has to have structure
Create client facing value proposition
Value story is the most important part for the client offering

HAP Discussion v3
Data Strategy Assessment Offering
DLT Practice - Data Led Transformations

Get into the delivery mindset

Pricing is based on investment, research, time, client value, resources

Define scope, scope is what;
Approach is how;
Rationale - why would client buy from us;
Develop the staffing model

Need to build a case for it, explain why it is important

++
Meeting 6/30/3033 with Dinesh
Subject: catch up

Assess, identify,
Sales is a key performance indicator
Delivery based selling

setup a meeting with Shin to discuss design review of CDOS/COZEVA

Create whitepapers of thought leadership of the work I'm doing.

Data Security

Thursday, March 31, 2022 7:39 PM

Data Security

Data security is a prevention and mitigation asset. Unplanned downtime can cost businesses a lot of time and money. The cost of a security threat to your information system can have a significant impact on your business.

Data security builds trust in customer's mind for a business. No organization can grow without customer trust and loyalty, and a healthy security posture is a cornerstone of trust.

Data security, beyond good practice and good ethics, is good business. A recent Cisco study made clear, data security will help fuel (and protect) an estimated $5.3trillion in private sector value in the next 10 years. The security goals could be competitive advantage, value-addition, financial gains, simplicity, and trust-value.

Security best practices

- Protect keys, password, security certificates
- Protect data at rest
  - Apply disk encryption to help safeguard your data.
  - Use encryption to help mitigate risks related to unauthorized data access. Encrypt your drives before you write sensitive data to them.
- Protect data in transit
  - Always use SSL/TLS protocols to exchange data across different locations.
  - All transactions occur via HTTPS. You can use Storage REST API over HTTPS.
- Secure email, documents, and sensitive data
- Mitigate and protect against DDoS
- Intrusion Detection and prevention
- Enterprise grade logging

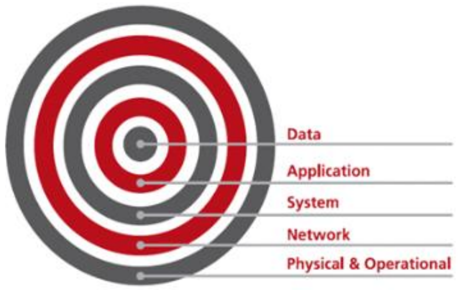
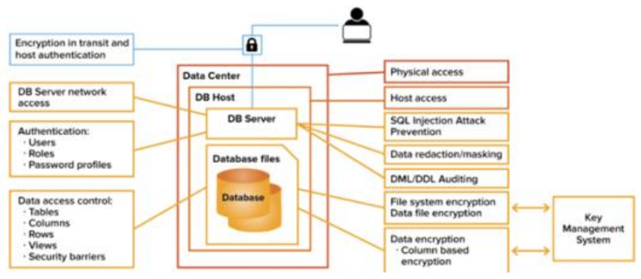
- Choose database that supports: Authentication, Authorization, Trusted Contexts, Auditing, Object Level, Row & Column Access Control, Label-Based Access Control, Encryption controls, and Dynamic Data Masking
- Utilize mature and proven technologies that support data security and data integrity
- Alert security team of unexpected requests or patterns
- No hardcoding user credentials into scripts; User credentials will be configuration and parameter based

- Principle of least privilege
- Zero trust policy
- Adaptive security
- Sensitive data such as, PHI and PII should be encrypted in transit and at rest
- Policy based data archive and data Purge

- Physical Security
- Password Policies
- User Account Policies
- Security Incident handling
- Computer System Usage Policy
- Device Management and Security

Layered Defense

Multi-layered defenses—both hardware- and software-based— work together to help protect against, avoid, repel, and withstand any threat.

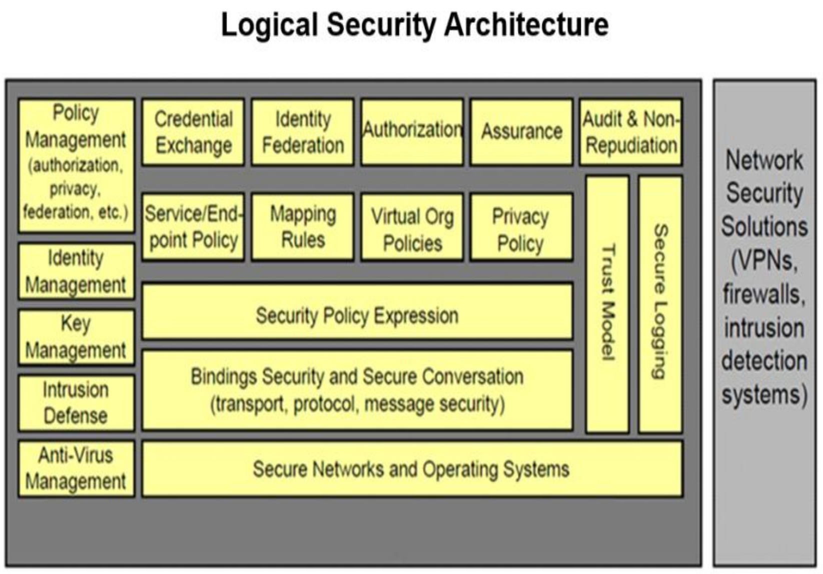
Multi-level, Defense-in-Depth approach to protect against physical and electronic threats: • Physical & Operational Security • Network Security • System Security • Application Security • Data Security	 Data Application System Network Physical & Operational	 Encryption in transit and host authentication DB Server network access Authentication: · Users · Roles · Password profiles Data access control: · Tables · Columns · Rows · Views · Security barriers Data Center DB Host DB Server Database files Database Physical access Host access SQL Injection Attack Prevention Data redaction/masking DML/DDL Auditing File system encryption Data file encryption Data encryption · Column based encryption Key Management System

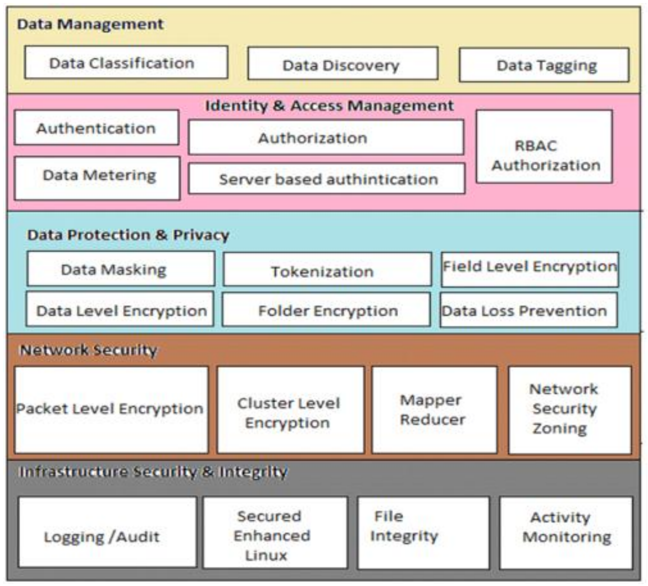
Specific data security aspects

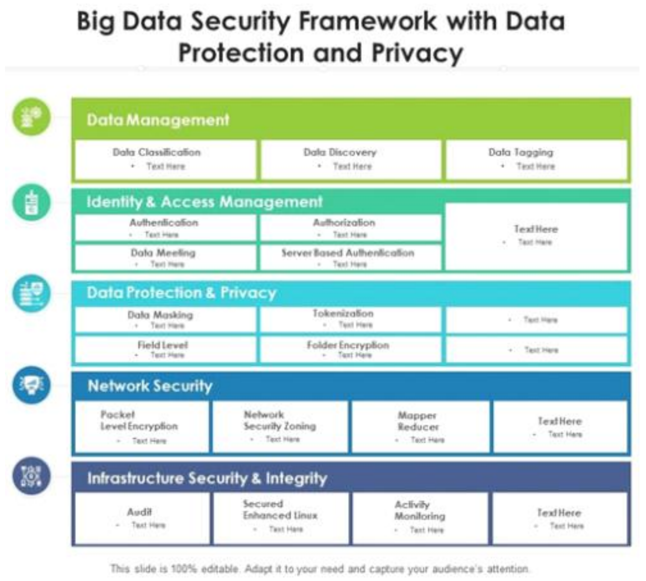
Identity and Access management

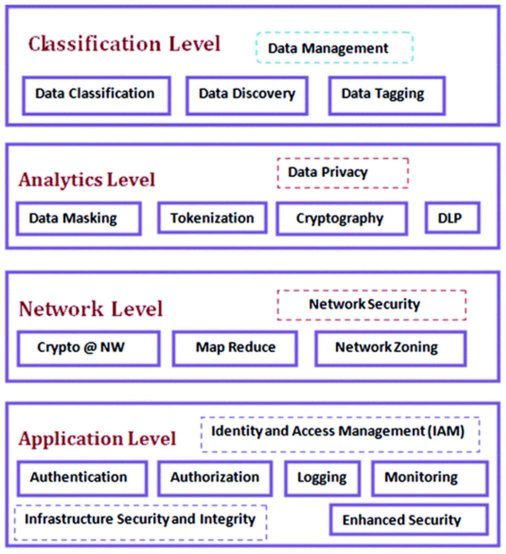
- Identity Management
  - Federated Identity
  - Identity Provisioning/Deprovisioning
  - Attribute Provisioning
- Authentication services
  - Database Login
  - Azure Active Directory

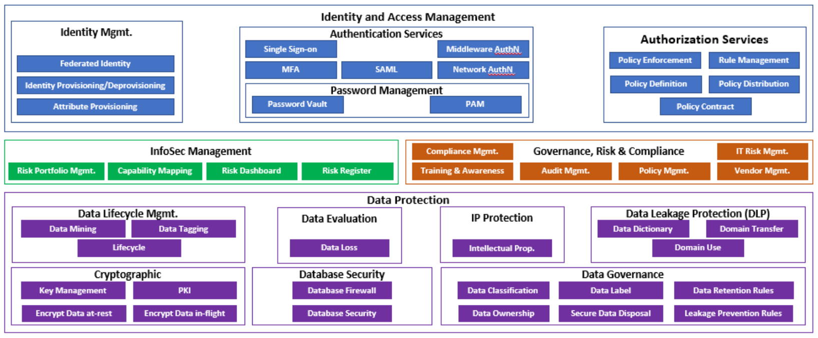
- Single Sign-on
    - MFA
    - SAML
    - Password/Key vault
    - Privileged Access Management (PAM)
  - Authorization services
    - Rules Management
    - Policy Definition
    - Policy Distribution
    - Policy Contract
    - Policy Enforcement
  - InfoSec. Management
    - Risk Portfolio Mgmt.
    - Capability Mapping
    - Risk Dashboard
    - Risk Register
  - Governance, Risk & Compliance
    - Compliance Mgmt.
    - Training & Awareness
    - Audit Mgmt.
    - Policy Mgmt.
  - Optimize identity and access management
    - Treat identity as the primary security perimeter
    - Centralize identity management
    - Turn on conditional access
    - Enable password management
    - Lower exposure of privileged accounts
    - Control locations where resources are located
- Data Protection
  - Data Lifecycle Mgmt.
    - Data Mining
    - Data Tagging
  - Data Evaluation
    - Data Loss
  - Database Security
    - Database Firewall
    - Database Security
    - Authentication - users to prove their identity
    - Authorization - limit users to specific actions and data
    - Data encryption
  - Enable threat protection
    - Implementing secure configurations on database
    - Detect and respond to potential threats as they occur
    - IP protection
  - Data Leakage Protection (DLP)
    - Data Dictionary
    - Domain Transfer
    - Domain Use
  - Data Governance
    - Data Discovery
    - Data Classification
      - Classify (categorize) stored data by sensitivity and business impact
      - Common classifications for data: Public, Private, Internal, Confidential, and Restricted
      - Organizations with weak data classification and file protection may encounter data leakage or misuse
    - Data Ownership
    - Data Label
    - Leakage Prevention Rules
    - Data Retention Rules
    - Secure Data Disposal
  - Enable database auditing
    - Track and log events
    - Review for audits
    - Maintain regulatory compliance, understand database activity, find discrepancies and detect anomalies
  - Monitor storage services for unexpected changes in behavior
    - Monitor the storage services for any unexpected changes in behavior, e.g., slow response times
    - Use logging to analyze a problem in depth
    - Use this data to trace requests, analyze usage trends, and diagnose storage account issues
- Network Security
  - Virtual Networks
  - Firewall
- Threat Protection
  - Threat Detection
  - Auditing
  - Vulnerability Assessment

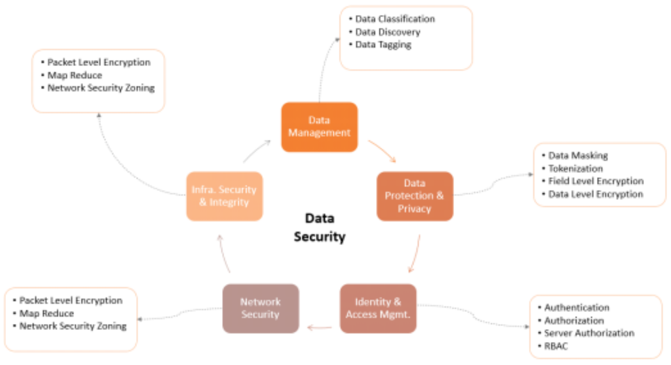

Logical Security Architecture
Policy Management (authorization, privacy, federation, etc.)
Credential Exchange
Identity Federation
Authorization
Assurance
Audit & Non-Repudiation
Identity Management
Service/End-point Policy
Mapping Rules
Virtual Org Policies
Privacy Policy
Trust Model
Secure Logging
Key Management
Security Policy Expression
Intrusion Defense
Bindings Security and Secure Conversation (transport, protocol, message security)
Anti-Virus Management
Secure Networks and Operating Systems
Network Security Solutions (VPNs, firewalls, intrusion detection systems)


Data Management
Data Classification
Data Discovery
Data Tagging
Identity & Access Management
Authentication
Authorization
RBAC Authorization
Data Metering
Server based authintication
Data Protection & Privacy
Data Masking
Tokenization
Field Level Encryption
Data Level Encryption
Folder Encryption
Data Loss Prevention
Network Security
Packet Level Encryption
Cluster Level Encryption
Mapper Reducer
Network Security Zoning
Infrastructure Security & Integrity
Logging /Audit
Secured Enhanced Linux
File Integrity
Activity Monitoring


Big Data Security Framework with Data Protection and Privacy
Data Management
Data Classification
Text Here
Data Discovery
Text Here
Data Tagging
Text Here
Identity & Access Management
Authentication
Text Here
Authorization
Text Here
Text Here
Text Here
Data Metering
Text Here
Server Based Authentication
Text Here
Data Protection & Privacy
Data Masking
Text Here
Tokenization
Text Here
Text Here
Field Level
Text Here
Folder Encryption
Text Here
Text Here
Network Security
Packet Level Encryption
Text Here
Network Security Zoning
Text Here
Mapper Reducer
Text Here
Text Here
Text Here
Infrastructure Security & Integrity
Audit
Text Here
Secured Enhanced Linux
Text Here
Activity Monitoring
Text Here
Text Here
Text Here
This slide is 100% editable. Adapt it to your need and capture your audience's attention.


Classification Level
Data Management
Data Classification
Data Discovery
Data Tagging
Analytics Level
Data Privacy
Data Masking
Tokenization
Cryptography
DLP
Network Level
Network Security
Crypto @ NW
Map Reduce
Network Zoning
Application Level
Identity and Access Management (IAM)
Authentication
Authorization
Logging
Monitoring
Infrastructure Security and Integrity
Enhanced Security


Identity and Access Management
Identity Mgmt.
Federated Identity
Identity Provisioning/Deprovisioning
Attribute Provisioning
Authentication Services
Single Sign-on
Middleware AuthN
MFA
SAML
Network AuthN
Password Management
Password Vault
PAM
Authorization Services
Policy Enforcement
Rule Management
Policy Definition
Policy Distribution
Policy Contract
InfoSec Management
Risk Portfolio Mgmt.
Capability Mapping
Risk Dashboard
Risk Register
Governance, Risk & Compliance
Compliance Mgmt.
IT Risk Mgmt.
Training & Awareness
Audit Mgmt.
Policy Mgmt.
Vendor Mgmt.
Data Protection
Data Lifecycle Mgmt.
Data Mining
Data Tagging
Lifecycle
Data Evaluation
Data Loss
IP Protection
Intellectual Prop.
Data Leakage Protection (DLP)
Data Dictionary
Domain Transfer
Domain Use
Cryptographic
Key Management
PKI
Encrypt Data at-rest
Encrypt Data in-flight
Database Security
Database Firewall
Database Security
Data Governance
Data Classification
Data Label
Data Retention Rules
Data Ownership
Secure Data Disposal
Leakage Prevention Rules


Data Security
Data Management
Data Protection & Privacy
Identity & Access Mgmt.
Network Security
Infra. Security & Integrity
• Data Classification
• Data Discovery
• Data Tagging
• Data Masking
• Tokenization
• Field Level Encryption
• Data Level Encryption
• Authentication
• Authorization
• Server Authorization
• RBAC
• Packet Level Encryption
• Map Reduce
• Network Security Zoning
• Packet Level Encryption
• Map Reduce
• Network Security Zoning

Data Security v0.1

Thursday, March 31, 2022 7:39 PM

Data Security

Data security is a prevention and mitigation asset. Unplanned downtime can cost businesses a lot of time and money. The cost of a security threat to your information system can have a significant impact on your business.

Data security builds trust in customer's mind for a business. No organization can grow without customer trust and loyalty, and a healthy security posture is a cornerstone of trust.

Data security, beyond good practice and good ethics, is good business. A recent Cisco study made clear, data security will help fuel (and protect) an estimated $5.3trillion in private sector value in the next 10 years. The security goals could be competitive advantage, value-addition, financial gains, simplicity, and trust-value.

Security best practices

- Protect keys, password, security certificates
- Protect data at rest
  - Apply disk encryption to help safeguard your data.
  - Use encryption to help mitigate risks related to unauthorized data access. Encrypt your drives before you write sensitive data to them.
- Protect data in transit
  - Always use SSL/TLS protocols to exchange data across different locations.
  - All transactions occur via HTTPS. You can use Storage REST API over HTTPS.
- Secure email, documents, and sensitive data
- ~~Mitigate and protect against DDoS~~
- ~~Intrusion Detection and prevention~~
- Enterprise grade end-to-end logging

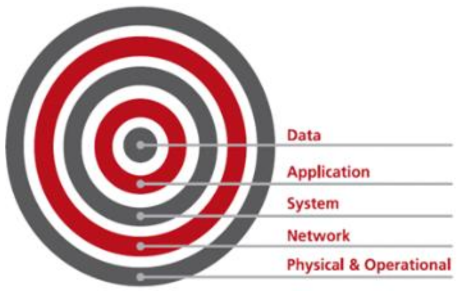
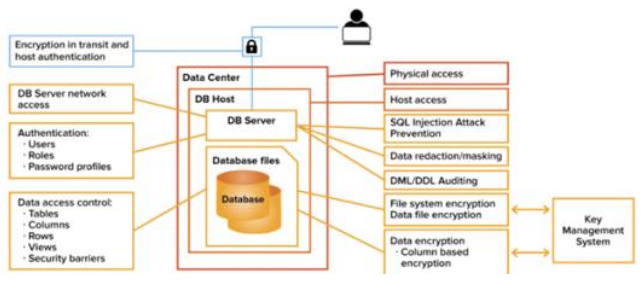
- Choose database that supports: Authentication, Authorization, Trusted Contexts, Auditing, Object Level, Row & Column Access Control, Label-Based Access Control, Encryption controls, and Dynamic Data Masking
- Utilize mature and proven technologies that support data security and data integrity
- ~~Alert security team of unexpected requests or patterns~~
- ~~No hardcoding user credentials into scripts; User credentials will be configuration and parameter based~~

- Principle of least privilege
- Zero trust policy
- Adaptive security
- ~~Sensitive data such as, PHI and PII should be encrypted in transit and at rest~~
- Policy based data archive and data Purge

- Physical Security
- Password Policies
- User Account Policies
- Security Incident handling
- ~~Computer System Usage Policy~~
- ~~Device Management and Security~~

Layered Defense

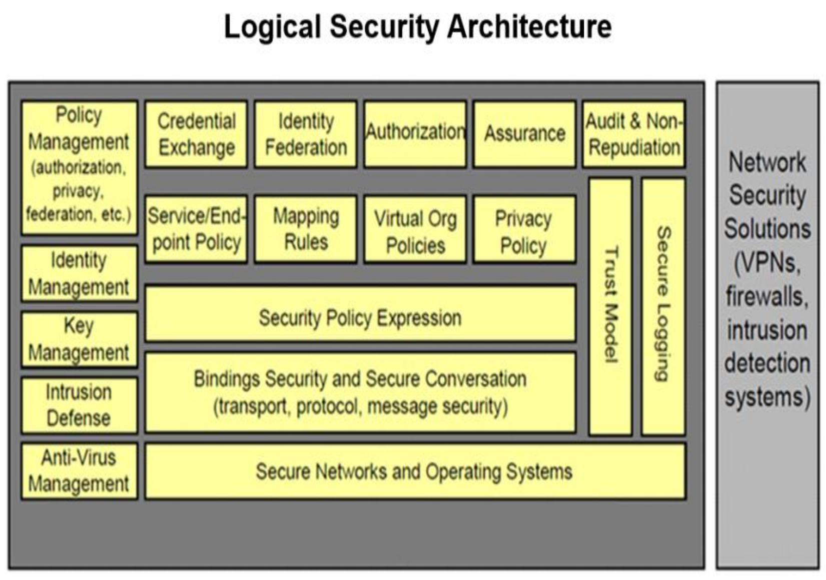
Multi-layered defenses—both hardware- and software-based— work together to help protect against, avoid, repel, and withstand any threat.

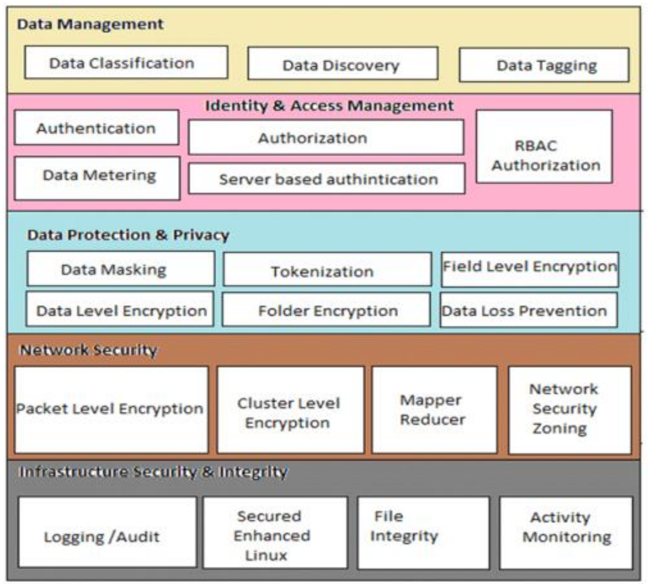
Multi-level, Defense-in-Depth approach to protect against physical and electronic threats: • Physical & Operational Security • Network Security • System Security • Application Security • Data Security	 Data Application System Network Physical & Operational	 Encryption in transit and host authentication DB Server network access Authentication: · Users · Roles · Password profiles Data access control: · Tables · Columns · Rows · Views · Security barriers Data Center DB Host DB Server Database files Database Physical access Host access SQL Injection Attack Prevention Data redaction/masking DML/DDL Auditing File system encryption Data file encryption Data encryption · Column based encryption Key Management System

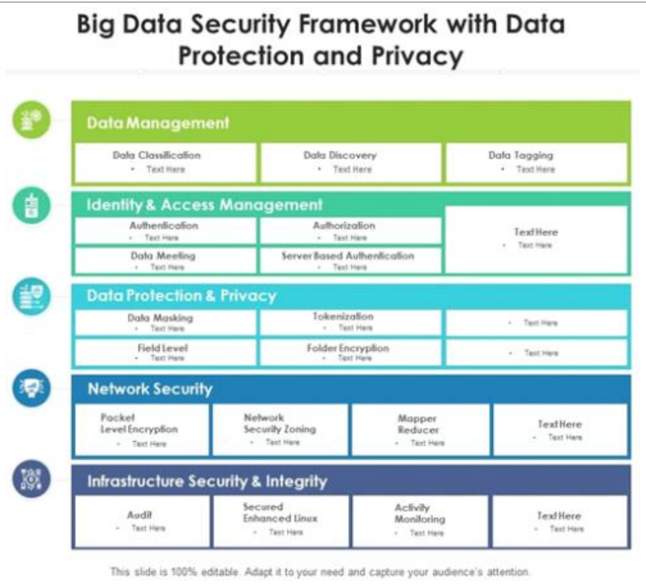
Specific data security aspects

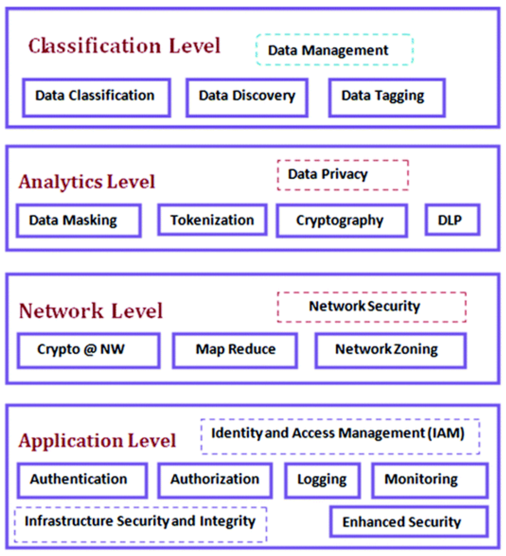
Identity and Access management
- Identity Management
  - Federated Identity
  - Identity Provisioning/Deprovisioning
  - Attribute Provisioning
- Authentication services
  - Database Login
  - Azure Active Directory

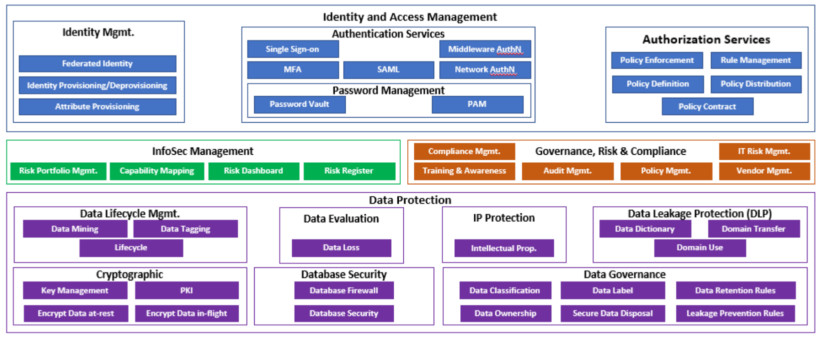
- Single Sign-on
      - MFA
      - SAML
      - Password/Key vault
      - Privileged Access Management (PAM)
  - Authorization services
      - Rules Management
      - Policy Definition
      - Policy Distribution
      - Policy Contract
      - Policy Enforcement
  - InfoSec. Management
      - Risk Portfolio Mgmt.
      - Capability Mapping
      - Risk Dashboard
      - Risk Register
  - Governance, Risk & Compliance
      - Compliance Mgmt.
      - Training & Awareness
      - Audit Mgmt.
      - Policy Mgmt.
  - Optimize identity and access management
      - Treat identity as the primary security perimeter
      - Centralize identity management
      - Turn on conditional access
      - Enable password management
      - Lower exposure of privileged accounts
      - Control locations where resources are located
- Data Protection
  - Data Lifecycle Mgmt.
      - Data Mining
      - Data Tagging
  - Data Evaluation
      - Data Loss
  - Database Security
      - Database Firewall
      - Database Security
      - Authentication - users to prove their identity
      - Authorization - limit users to specific actions and data
      - Data encryption
  - Enable threat protection
      - Implementing secure configurations on database
      - Detect and respond to potential threats as they occur
      - IP protection
  - Data Leakage Protection (DLP)
      - Data Dictionary
      - Domain Transfer
      - Domain Use
  - Data Governance
      - Data Discovery
      - Data Classification
          - Classify (categorize) stored data by sensitivity and business impact
          - Common classifications for data: Public, Private, Internal, Confidential, and Restricted
          - Organizations with weak data classification and file protection may encounter data leakage or misuse
      - Data Ownership
      - Data Label
      - Leakage Prevention Rules
      - Data Retention Rules
      - Secure Data Disposal
  - Enable database auditing
      - Track and log events
      - Review for audits
      - Maintain regulatory compliance, understand database activity, find discrepancies and detect anomalies
  - ~~Monitor storage services for unexpected changes in behavior~~
      - ~~Monitor the storage services for any unexpected changes in behavior, e.g., slow response times~~
      - Use logging to analyze a problem in depth
      - Use logging data to trace requests, analyze usage trends, and diagnose storage account issues
- ~~Network Security~~
  - ~~Virtual Networks~~
  - ~~Firewall~~
- ~~Threat Protection~~
  - ~~Threat Detection~~
  - ~~Auditing~~
  - ~~Vulnerability Assessment~~

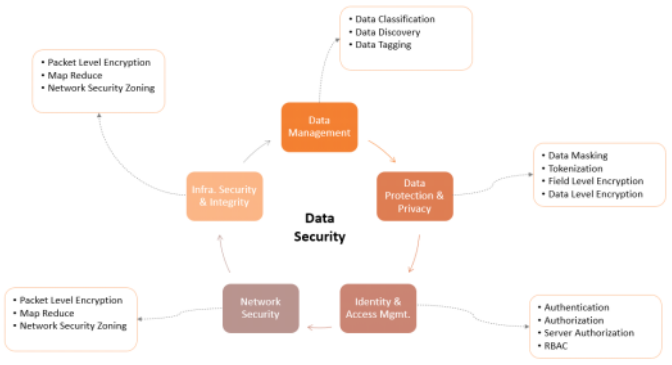

Logical Security Architecture
Policy Management (authorization, privacy, federation, etc.)
Credential Exchange
Identity Federation
Authorization
Assurance
Audit & Non-Repudiation
Service/End-point Policy
Mapping Rules
Virtual Org Policies
Privacy Policy
Trust Model
Secure Logging
Identity Management
Key Management
Security Policy Expression
Intrusion Defense
Bindings Security and Secure Conversation (transport, protocol, message security)
Anti-Virus Management
Secure Networks and Operating Systems
Network Security Solutions (VPNs, firewalls, intrusion detection systems)


Data Management
Data Classification
Data Discovery
Data Tagging
Identity & Access Management
Authentication
Authorization
RBAC Authorization
Data Metering
Server based authintication
Data Protection & Privacy
Data Masking
Tokenization
Field Level Encryption
Data Level Encryption
Folder Encryption
Data Loss Prevention
Network Security
Packet Level Encryption
Cluster Level Encryption
Mapper Reducer
Network Security Zoning
Infrastructure Security & Integrity
Logging /Audit
Secured Enhanced Linux
File Integrity
Activity Monitoring


Big Data Security Framework with Data Protection and Privacy
Data Management
Data Classification
Text Here
Data Discovery
Text Here
Data Tagging
Text Here
Identity & Access Management
Authentication
Text Here
Authorization
Text Here
Text Here
Text Here
Data Meeting
Text Here
Server Based Authentication
Text Here
Data Protection & Privacy
Data Masking
Text Here
Tokenization
Text Here
Text Here
Field Level
Text Here
Folder Encryption
Text Here
Text Here
Network Security
Packet Level Encryption
Text Here
Network Security Zoning
Text Here
Mapper Reducer
Text Here
Text Here
Text Here
Infrastructure Security & Integrity
Audit
Text Here
Secured Enhanced Linux
Text Here
Activity Monitoring
Text Here
Text Here
Text Here
This slide is 100% editable. Adapt it to your need and capture your audience's attention.


Classification Level
Data Management
Data Classification
Data Discovery
Data Tagging
Analytics Level
Data Privacy
Data Masking
Tokenization
Cryptography
DLP
Network Level
Network Security
Crypto @ NW
Map Reduce
Network Zoning
Application Level
Identity and Access Management (IAM)
Authentication
Authorization
Logging
Monitoring
Infrastructure Security and Integrity
Enhanced Security


Identity and Access Management
Identity Mgmt.
Federated Identity
Identity Provisioning/Deprovisioning
Attribute Provisioning
Authentication Services
Single Sign-on
Middleware AuthN
MFA
SAML
Network AuthN
Password Management
Password Vault
PAM
Authorization Services
Policy Enforcement
Rule Management
Policy Definition
Policy Distribution
Policy Contract
InfoSec Management
Risk Portfolio Mgmt.
Capability Mapping
Risk Dashboard
Risk Register
Compliance Mgmt.
Governance, Risk & Compliance
IT Risk Mgmt.
Training & Awareness
Audit Mgmt.
Policy Mgmt.
Vendor Mgmt.
Data Protection
Data Lifecycle Mgmt.
Data Mining
Data Tagging
Lifecycle
Data Evaluation
Data Loss
IP Protection
Intellectual Prop.
Data Leakage Protection (DLP)
Data Dictionary
Domain Transfer
Domain Use
Cryptographic
Key Management
PKI
Encrypt Data at-rest
Encrypt Data in-flight
Database Security
Database Firewall
Database Security
Data Governance
Data Classification
Data Label
Data Retention Rules
Data Ownership
Secure Data Disposal
Leakage Prevention Rules


• Data Classification
• Data Discovery
• Data Tagging
• Packet Level Encryption
• Map Reduce
• Network Security Zoning
Data Management
Infra. Security & Integrity
Data Protection & Privacy
• Data Masking
• Tokenization
• Field Level Encryption
• Data Level Encryption
Data Security
Network Security
Identity & Access Mgmt.
• Packet Level Encryption
• Map Reduce
• Network Security Zoning
• Authentication
• Authorization
• Server Authorization
• RBAC

Data Security v0.2

Thursday, March 31, 2022 7:39 PM

Data Security

Data security is a prevention and mitigation asset. Unplanned downtime can cost businesses a lot of time and money. The cost of a security threat to your information system can have a significant impact on your business.

Data security builds trust in customer's mind for a business. No organization can grow without customer trust and loyalty, and a healthy security posture is a cornerstone of trust.

Data security, beyond good practice and good ethics, is good business. A recent Cisco study made clear, data security will help fuel (and protect) an estimated $5.3trillion in private sector value in the next 10 years. The security goals could be competitive advantage, value-addition, financial gains, simplicity, and trust-value.

Security best practices

- Protect keys, password, security certificates
- Protect data at rest
- Protect data in transit
- Secure email, documents, and sensitive data
- Enterprise grade end-to-end logging

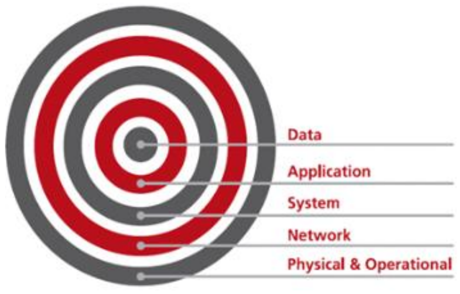
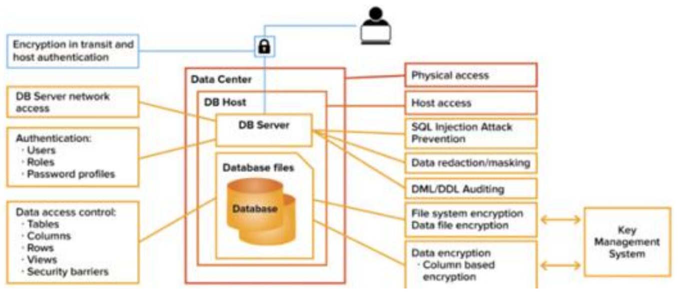
- Choose database that supports: Authentication, Authorization, Trusted Contexts, Auditing, Object Level, Row & Column Access Control, Label-Based Access Control, Encryption controls, and Dynamic Data Masking
- Utilize mature and proven technologies that support data security and data integrity

- Principle of least privilege
- Zero trust policy
- Adaptive security
- Policy based data archive and data Purge

- Physical Security
- Password Policies
- User Account Policies
- Security Incident handling

Layered Defense

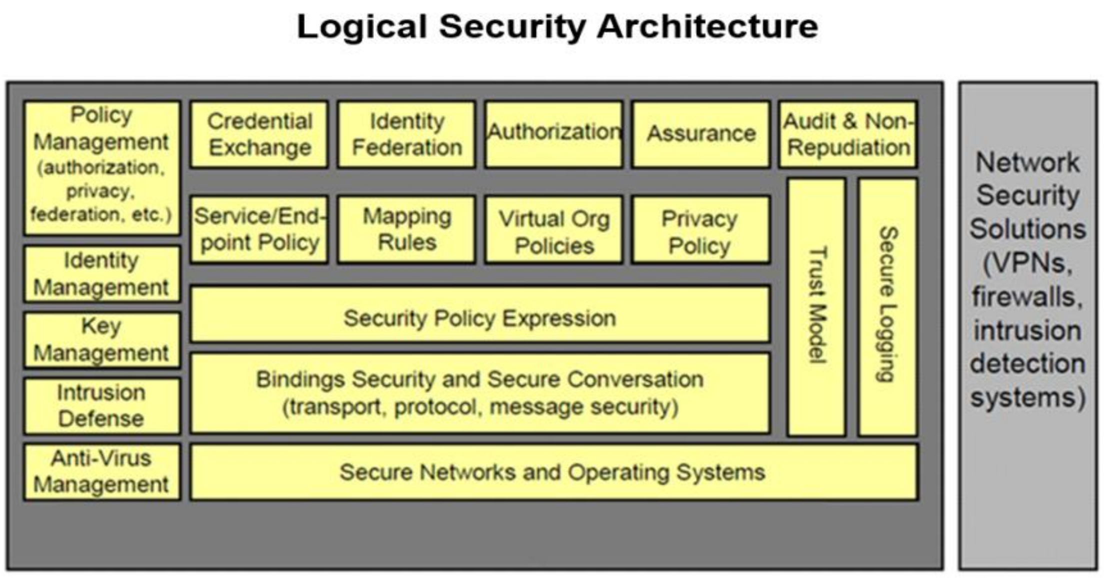
Multi-layered defenses—both hardware- and software-based— work together to help protect against, avoid, repel, and withstand any threat.

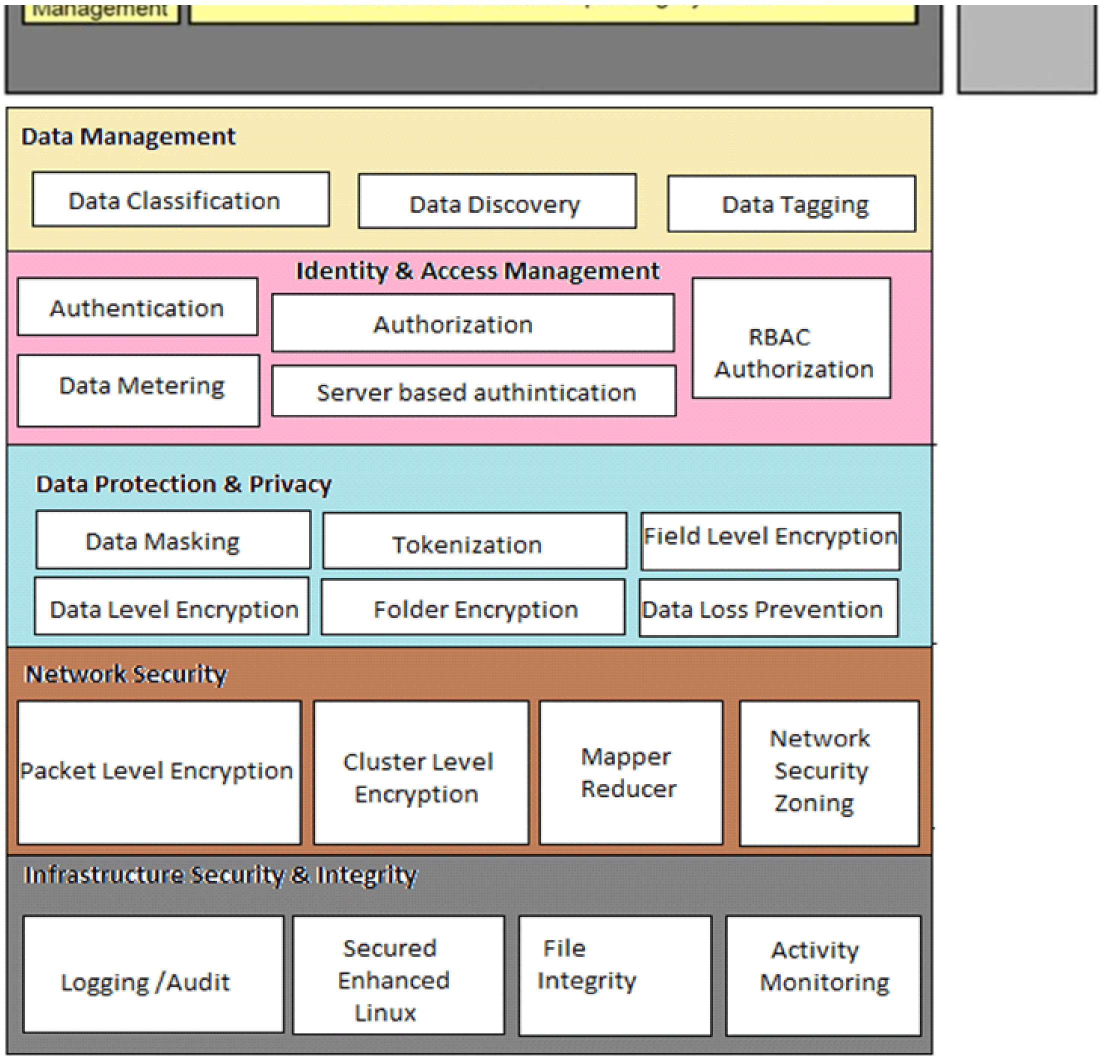
Multi-level, Defense-in-Depth approach to protect against physical and electronic threats: • Physical & Operational Security • Network Security • System Security • Application Security • Data Security	 Data Application System Network Physical & Operational	 Encryption in transit and host authentication DB Server network access Authentication: · Users · Roles · Password profiles Data access control: · Tables · Columns · Rows · Views · Security barriers Data Center DB Host DB Server Database files Database Physical access Host access SQL Injection Attack Prevention Data redaction/masking DML/DDL Auditing File system encryption Data file encryption Data encryption · Column based encryption Key Management System

Specific data security aspects

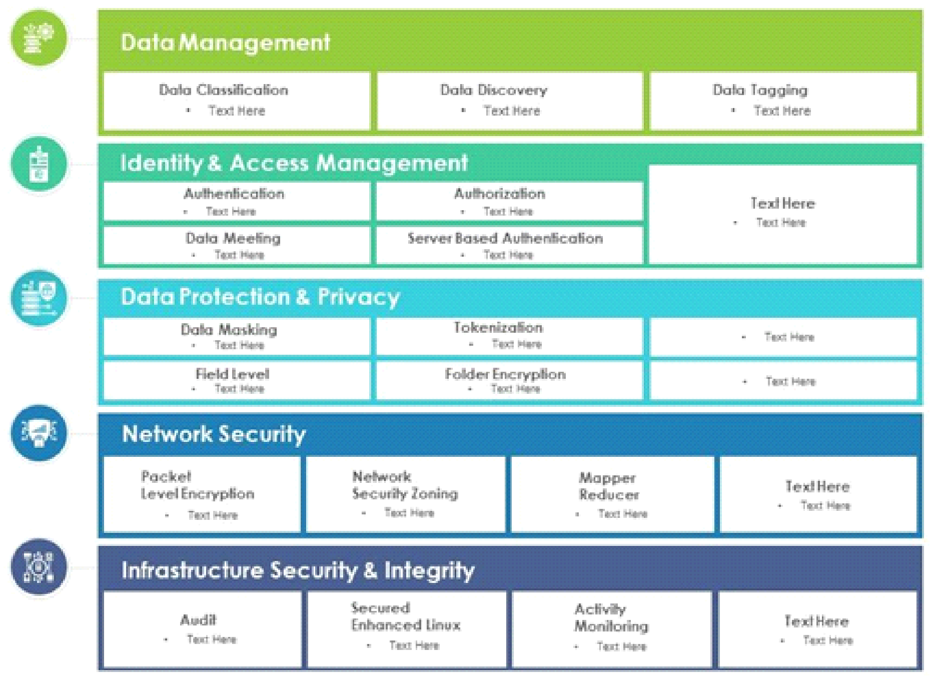
Identity and Access management
- Identity Management
  - Federated Identity
  - Identity Provisioning/Deprovisioning
  - Attribute Provisioning
- Authentication services
  - Database Login
  - Azure Active Directory
  - Single Sign-on
  - MFA
  - SAML
  - Password/Key vault
  - Privileged Access Management (PAM)
- Authorization services
  - Rules Management
  - Policy Definition
  - Policy Distribution
  - Policy Contract
  - Policy Enforcement
- InfoSec. Management
  - Risk Portfolio Mgmt.

- Capability Mapping
    - Risk Dashboard
    - Risk Register
  - Governance, Risk & Compliance
    - Compliance Mgmt.
    - Training & Awareness
    - Audit Mgmt.
    - Policy Mgmt.
  - Optimize identity and access management
    - Treat identity as the primary security perimeter
    - Centralize identity management
    - Turn on conditional access
    - Enable password management
    - Lower exposure of privileged accounts
    - Control locations where resources are located
- Data Protection
  - Data Lifecycle Mgmt.
    - Data Mining
    - Data Tagging
  - Data Evaluation
    - Data Loss
  - Database Security
    - Database Firewall
    - Database Security
    - Authentication - users to prove their identity
    - Authorization - limit users to specific actions and data
    - Data encryption
  - Enable threat protection
    - Implementing secure configurations on database
    - Detect and respond to potential threats as they occur
    - IP protection
  - Data Leakage Protection (DLP)
    - Data Dictionary
    - Domain Transfer
    - Domain Use
  - Data Governance
    - Data Discovery
    - Data Classification
      - Classify (categorize) stored data by sensitivity and business impact
      - Common classifications for data: Public, Private, Internal, Confidential, and Restricted
      - Organizations with weak data classification and file protection may encounter data leakage or misuse
    - Data Ownership
    - Data Label
    - Leakage Prevention Rules
    - Data Retention Rules
    - Secure Data Disposal
  - Enable database auditing
    - Track and log events
    - Review for audits
    - Maintain regulatory compliance, understand database activity, find discrepancies and detect anomalies
  - Logging
    - Use logging to analyze a problem in depth
    - Use logging data to trace requests, analyze usage trends, and diagnose storage account issues

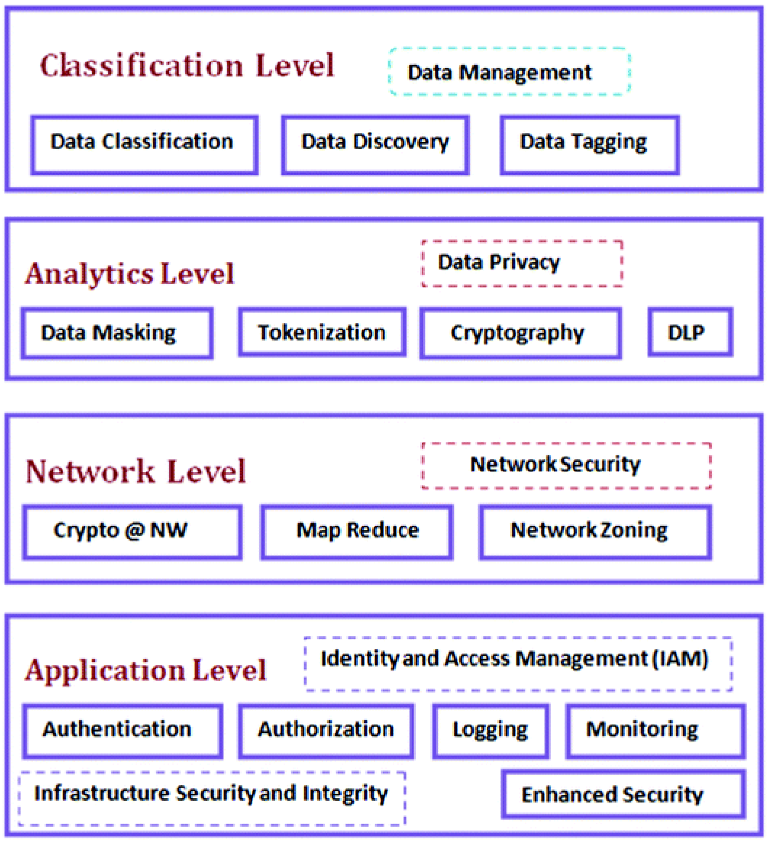

Logical Security Architecture
Policy Management (authorization, privacy, federation, etc.)
Credential Exchange
Identity Federation
Authorization
Assurance
Audit & Non-Repudiation
Service/End-point Policy
Mapping Rules
Virtual Org Policies
Privacy Policy
Trust Model
Secure Logging
Identity Management
Key Management
Security Policy Expression
Bindings Security and Secure Conversation (transport, protocol, message security)
Intrusion Defense
Anti-Virus Management
Secure Networks and Operating Systems
Network Security Solutions (VPNs, firewalls, intrusion detection systems)

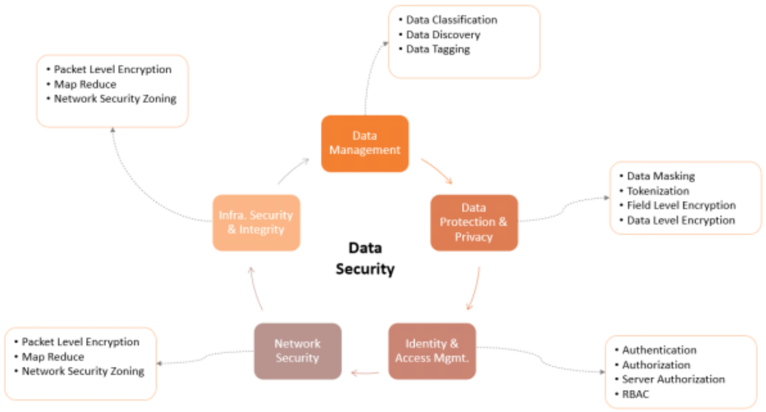


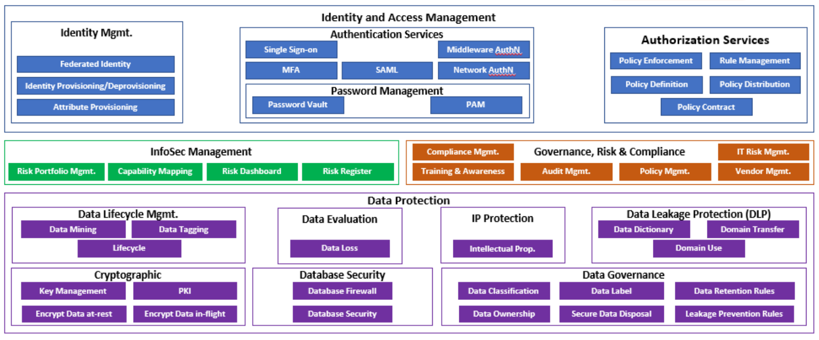
Big Data Security Framework with Data Protection and Privacy



This slide is 100% editable. Adapt it to your need and capture your audience's attention.


Classification Level
Data Management
Data Classification
Data Discovery
Data Tagging
Analytics Level
Data Privacy
Data Masking
Tokenization
Cryptography
DLP
Network Level
Network Security
Crypto @ NW
Map Reduce
Network Zoning
Application Level
Identity and Access Management (IAM)
Authentication
Authorization
Logging
Monitoring
Infrastructure Security and Integrity
Enhanced Security


• Data Classification
• Data Discovery
• Data Tagging
• Packet Level Encryption
• Map Reduce
• Network Security Zoning
Data Management
Data Protection & Privacy
• Data Masking
• Tokenization
• Field Level Encryption
• Data Level Encryption
Infra. Security & Integrity
Data Security
Network Security
Identity & Access Mgmt.
• Packet Level Encryption
• Map Reduce
• Network Security Zoning
• Authentication
• Authorization
• Server Authorization
• RBAC


Identity and Access Management
Identity Mgmt.
Federated Identity
Identity Provisioning/Deprovisioning
Attribute Provisioning
Authentication Services
Single Sign-on
Middleware AuthN
MFA
SAML
Network AuthN
Password Management
Password Vault
PAM
Authorization Services
Policy Enforcement
Rule Management
Policy Definition
Policy Distribution
Policy Contract
InfoSec Management
Risk Portfolio Mgmt.
Capability Mapping
Risk Dashboard
Risk Register
Compliance Mgmt.
Governance, Risk & Compliance
IT Risk Mgmt.
Training & Awareness
Audit Mgmt.
Policy Mgmt.
Vendor Mgmt.
Data Protection
Data Lifecycle Mgmt.
Data Mining
Data Tagging
Lifecycle
Data Evaluation
Data Loss
IP Protection
Intellectual Prop.
Data Leakage Protection (DLP)
Data Dictionary
Domain Transfer
Domain Use
Cryptographic
Key Management
PKI
Encrypt Data at-rest
Encrypt Data in-flight
Database Security
Database Firewall
Database Security
Data Governance
Data Classification
Data Label
Data Retention Rules
Data Ownership
Secure Data Disposal
Leakage Prevention Rules

Miscellaneous

Sunday, March 27, 2022 5:08 PM

Data Security

Data security adds value by **preventing and mitigating risks**. It is essentially a prevention and mitigation asset. Unplanned downtime can cost businesses a lot of time and money. The cost of a security threat to your information system can have a significant impact on your business.

No organization can grow without customer trust and loyalty, and a healthy security posture is a cornerstone of trust.

It is clear that data security — beyond good practice and good ethics — is good business. A recent Cisco study made clear, data security will help fuel (and protect) an estimated $5.3trillion in private sector value in the next 10 years. The security goals may be competitive advantage, value-addition, financial gains, simplicity, trust-value.

Security best practices

- Protect keys
- Protect data at rest
  - Apply disk encryption to help safeguard your data.
  - Use encryption to help mitigate risks related to unauthorized data access. Encrypt your drives before you write sensitive dat a to them.
- Protect data in transit
- Always use SSL/TLS protocols to exchange data across different locations.
  - Secure access from multiple workstations located on-premises to an Azure virtual network. Use site-to-site VPN
  - Secure access from an individual workstation located on-premises to an Azure virtual network. Use point-to-site VPN.
  - Move larger data sets over a dedicated high-speed WAN link. Use ExpressRoute.
  - Interact with Azure Storage through the Azure portal. All transactions occur via HTTPS. You can also use Storage REST API over HTTPS.
- Secure email, documents, and sensitive data
- Configure logging to monitor how your organization is using the protection service
- Enforce multi-factor verification for users, especially your administrator accounts
- Encrypt your virtual hard disk files to protect your boot volume and data volumes at rest, along with encryption keys and secrets
- Mitigate and protect against DDoS

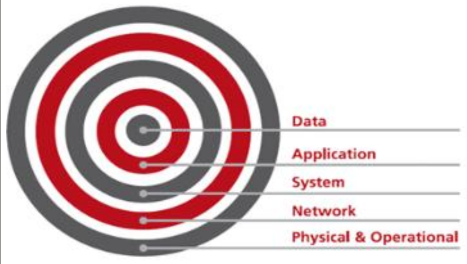
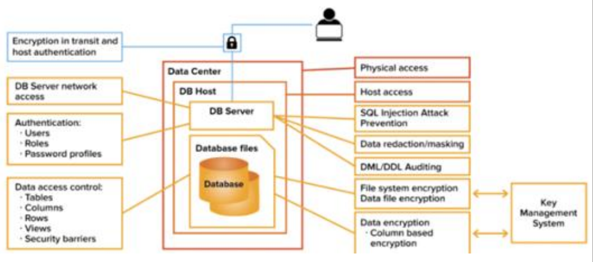
- Solution controls access to data based on roles
- Database that supports: Authentication, Authorization, Trusted Contexts, Auditing, Object Level, Row & Column Access Control, Label-Based Access Control, Encryption controls, and Dynamic Data Masking
- Mature and proven technologies that support data security and data integrity
- Unexpected requests reported to the security team
- Data security and protection for data in-flight and data at rest
- No hardcoding user credentials into scripts; User credentials will be configuration and parameter based

- Principle of least privilege
- Zero trust policy
- Intrusion Detection and prevention
- Adaptive security
- Enterprise grade logging
- Sensitive data, like PHI - Protected Health Information and PII - Personally Identifiable Information should be encrypted in transit and at rest
- Role Based Access Control (RBAC)
- Policy based data archive and data Purge

- Physical Security
- Cryptographic Parameters
- Password Policies
- User Account Policies
- Security Incident handling
- Computer System Usage Policy
- Device Management and Security

Layered Defense

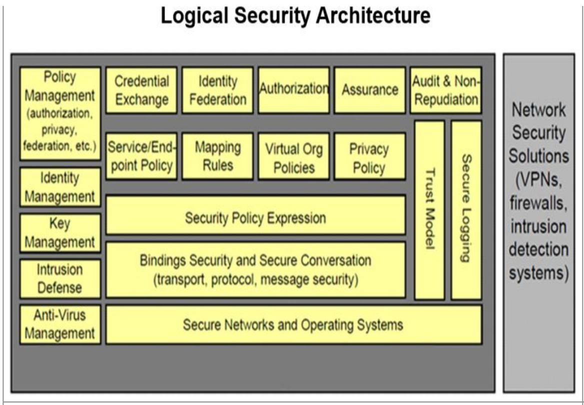
Layer upon layer of defenses—both hardware- and software-based— work together to help protect against, avoid, repel, and withstand any threat.

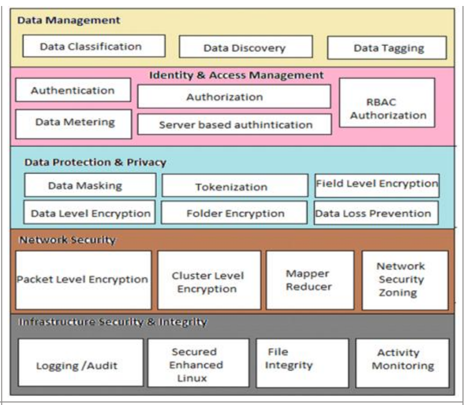
Multi-level, Defense-in-Depth approach to protect against physical and electronic threats: • Physical & Operational Security • Network Security • System Security • Application Security • Data Security	 Data Application System Network Physical & Operational	 Encryption in transit and host authentication DB Server network access Authentication: · Users · Roles · Password profiles Data access control: · Tables · Columns · Rows · Views · Security barriers Data Center DB Host DB Server Database files Database Physical access Host access SQL Injection Attack Prevention Data redaction/masking DML/DDL Auditing File system encryption Data file encryption Data encryption · Column based encryption Key Management System

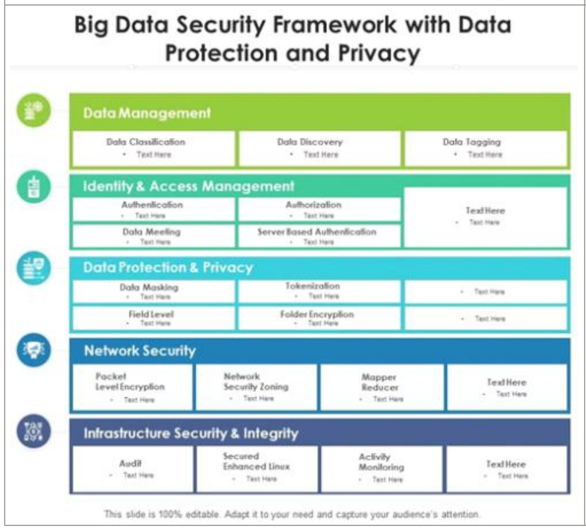
Specific data security aspects

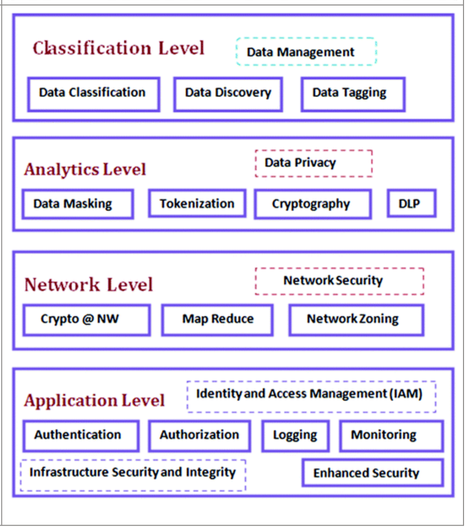
Identity and Access management
- Identity Management
  - Federated Identity
  - Identity Provisioning/Deprovisioning
  - Attribute Provisioning
- Authentication services
  - Database Login
  - Azure Active Directory
  - Single Sign-on
  - MFA
  - SAML
  - Password/Key vault
  - Privileged Access Management (PAM)
- Authorization services
  - Rules Management

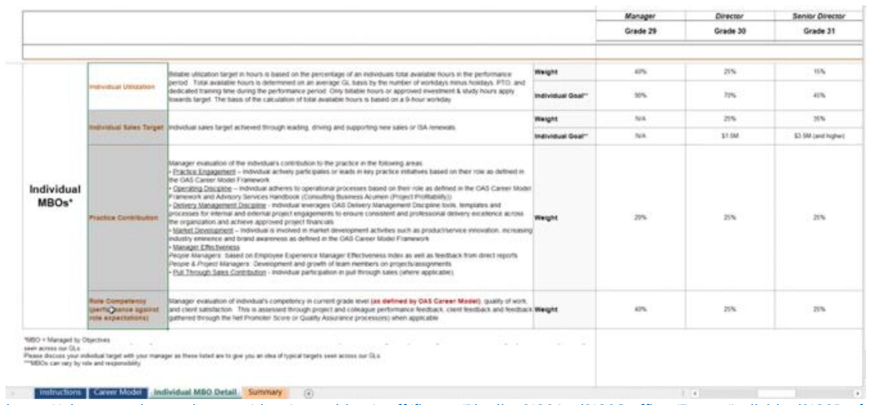
        - Policy Enforcement
        - Policy Definition
        - Policy Distribution
        - Policy Contract
    - InfoSec. Management
        - Risk Portfolio Mgmt.
        - Capability Mapping
        - Risk Dashboard
        - Risk Register
    - Governance, Risk & Compliance
        - Compliance Mgmt.
        - Training & Awareness
        - Audit Mgmt.
        - Policy Mgmt.
    - Optimize identity and access management
        - Treat identity as the primary security perimeter
        - Centralize identity management
        - Enable single sign-on
        - Turn on conditional access
        - Enable password management
        - Enforce multi-factor verification for users
        - Use role-based access control
        - Lower exposure of privileged accounts
        - Control locations where resources are located
- Data Protection
    - Data Lifecycle Mgmt.
        - Data Mining
        - Data Tagging
        - Lifecycle
    - Data Evaluation
        - Data Loss
    - Database Security
        - Database Firewall
        - Database Security
        - Authentication for users to prove their identity
        - Authorization to limit users to specific actions and data
        - Data encryption
    - Enable threat protection
        - Discover and classify most sensitive data so you can protect your data.
        - Implementing secure configurations on your database so you can protect your database.
        - Detecting and responding to potential threats as they occur so you can quickly respond and remediate
    - IP protection
        - Intellectual Property
    - Data Leakage Protection (DLP)
        - Data Dictionary
        - Domain Transfer
        - Domain Use
    - Data Governance
        - Data Discovery
        - Data Classification
            - Classify (categorize) stored data by sensitivity and business impact to determine the risks associated with the data
            - Common classifications for data: Public, Private, Internal, Confidential, and Restricted
            - Organizations weak on data classification and file protection might be more susceptible to data leakage or data misuse
        - Data Ownership
        - Data Label
        - Data Retention Rules
        - Leakage Prevention Rules
        - Secure Data Disposal
    - Enable database auditing
        - Track and log events
        - Store and viewing audits
        - Maintain regulatory compliance, understand database activity, find discrepancies and detect anomalies
    - Monitor storage services for unexpected changes in behavior
        - Monitor the storage services for any unexpected changes in behavior, e.g., slow response times
        - Use logging to analyze a problem in depth
        - Use this data to trace requests, analyze usage trends, and diagnose issues with your storage account
- Network Security
    - Virtual Networks
    - Firewall
- Threat Protection
    - Threat Detection
    - Auditing
    - Vulnerability Assessment


Logical Security Architecture
Policy Management (authorization, privacy, federation, etc.)
Credential Exchange
Identity Federation
Authorization
Assurance
Audit & Non-Repudiation
Service/End-point Policy
Mapping Rules
Virtual Org Policies
Privacy Policy
Identity Management
Key Management
Security Policy Expression
Intrusion Defense
Bindings Security and Secure Conversation (transport, protocol, message security)
Anti-Virus Management
Secure Networks and Operating Systems
Trust Model
Secure Logging
Network Security Solutions (VPNs, firewalls, intrusion detection systems)









				Manager	Director	Senior Director
				Grade 29	Grade 30	Grade 31
Individual MBOs*	Individual Utilization	Billable utilization target in hours is based on the percentage of an individuals total available hours in the performance period. Total available hours is determined on an average GL basis by the number of workdays minus holidays, PTO, and dedicated training time during the performance period. Only billable hours or approved investment & study hours apply towards target. The basis of the calculation of total available hours is based on a 9-hour workday	Weight	40%	25%	15%
			Individual Goal**	90%	70%	45%
	Individual Sales Target	Individual sales target achieved through leading, driving and supporting new sales or ISA renewals	Weight	N/A	25%	35%
			Individual Goal**	N/A	$1.5M	$3.5M (and higher)
	Practice Contribution	Manager evaluation of the individual's contribution to the practice in the following areas: • Practice Engagement – individual actively participates or leads in key practice initiatives based on their role as defined in the OAS Career Model Framework • Operating Discipline – individual adheres to operational processes based on their role as defined in the OAS Career Model Framework and Advisory Services Handbook (Consulting Business Acumen (Project Profitability)) • Delivery Management Discipline - individual leverages OAS Delivery Management Discipline tools, templates and processes for internal and external project engagements to ensure consistent and professional delivery excellence across the organization and achieve approved project financials • Market Development – individual is involved in market development activities such as product/service innovation, increasing industry eminence and brand awareness as defined in the OAS Career Model Framework • Manager Effectiveness People Managers: based on Employee Experience Manager Effectiveness index as well as feedback from direct reports People & Project Managers: Development and growth of team members on projects/assignments • Pull Through Sales Contribution - individual participation in pull through sales (where applicable)	Weight	20%	25%	25%
	Role Competency (performance against role expectations)	Manager evaluation of individual's competency in current grade level (as defined by OAS Career Model), quality of work, and client satisfaction. This is assessed through project and colleague performance feedback, client feedback and feedback gathered through the Net Promoter Score or Quality Assurance process(es) when applicable	Weight	40%	25%	25%

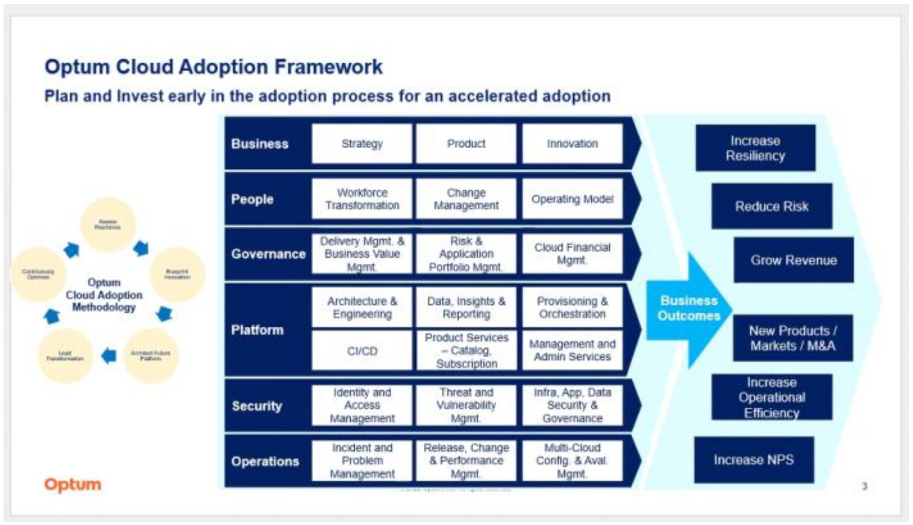
*MBO = Managed by Objectives
seen across our GLs
Please discuss your individual target with your manager as these listed are to give you an idea of typical targets seen across our GLs
**MBOs can vary by role and responsibility

Instructions | Career Model | Individual MBO Detail | Summary

https://uhgazure.sharepoint.com/sites/consulting/staff/finops/Pipeline%20And%20Staffing/Forms/Individual%20Performance%20Dashboard.aspx?RootFolder=/sites/consulting/staff/finops/Pipeline%20And%20Staffing/Finance%20and%20Ops%20Reporting/Individual%20Performance%20Dashboard
Sales target: $1.5M
Based on the role on a sale, you're eligible for 100% credit
They are focused on originating the pippeline
+++

Protect Data

Backup Data - Make regular backups of files, and store backup copies offsite
Anti-Malware - Protect your data against viruses by running anti-virus software
Password Security - Use a system of passwords so that access to data is restricted
Data Encryption - Use data encryption techniques to code data so that it makes no apparent sense
Access Control - Allow only authorized staff into certain computer areas
Lock Services - Always logoff or turn terminals off and if possible, lock them
Protect Data - Avoid accidental deletion of files by write-protecting disks
Store Data Safely - Safe storage of important files stored on removable disks, e.g., locked away in a fireproof and waterproof safe
+++



Optum Cloud Adoption Framework

Plan and Invest early in the adoption process for an accelerated adoption

Optum Cloud Adoption Methodology

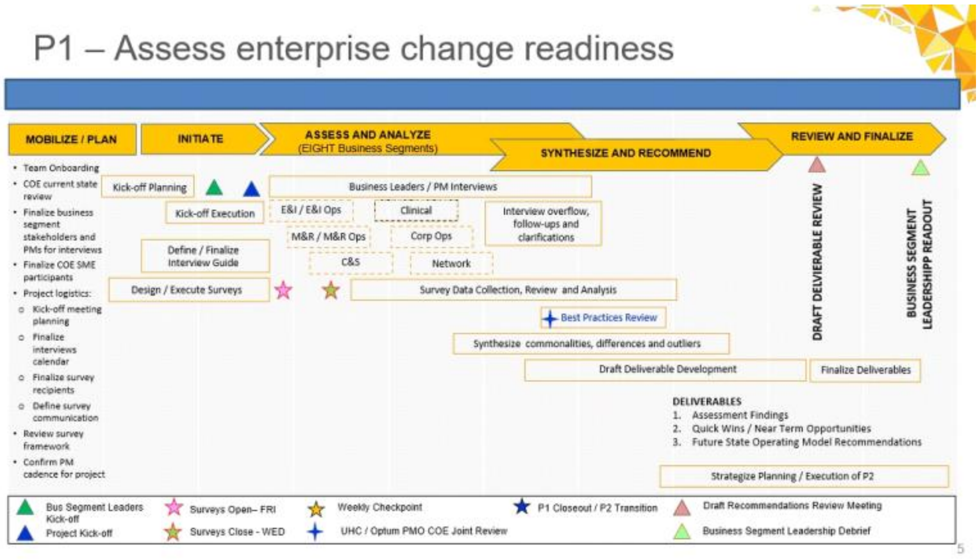
Business	Strategy	Product	Innovation
People	Workforce Transformation	Change Management	Operating Model
Governance	Delivery Mgmt. & Business Value Mgmt.	Risk & Application Portfolio Mgmt.	Cloud Financial Mgmt.
Platform	Architecture & Engineering	Data, Insights & Reporting	Provisioning & Orchestration
	CI/CD	Product Services – Catalog, Subscription	Management and Admin Services
Security	Identity and Access Management	Threat and Vulnerability Mgmt.	Infra, App, Data Security & Governance
Operations	Incident and Problem Management	Release, Change & Performance Mgmt.	Multi-Cloud Config. & Aval. Mgmt.

Business Outcomes

- Increase Resiliency
- Reduce Risk
- Grow Revenue
- New Products / Markets / M&A
- Increase Operational Efficiency
- Increase NPS

Optum

3



P1 – Assess enterprise change readiness

MOBILIZE / PLAN | INITIATE | ASSESS AND ANALYZE (EIGHT Business Segments) | SYNTHESIZE AND RECOMMEND | REVIEW AND FINALIZE

- Team Onboarding
- COE current state review
- Finalize business segment stakeholders and PMs for interviews
- Finalize COE SME participants
- Project logistics:
  - Kick-off meeting planning
  - Finalize interviews calendar
  - Finalize survey recipients
  - Define survey communication
- Review survey framework
- Confirm PM cadence for project

Kick-off Planning

Kick-off Execution

Define / Finalize Interview Guide

Design / Execute Surveys

Business Leaders / PM Interviews

E&I / E&I Ops | Clinical | M&R / M&R Ops | Corp Ops | C&S | Network

Interview overflow, follow-ups and clarifications

Survey Data Collection, Review and Analysis

Best Practices Review

Synthesize commonalities, differences and outliers

Draft Deliverable Development

Finalize Deliverables

DRAFT DELVIERABLE REVIEW

BUSINESS SEGMENT LEADERSHIPP READOUT

DELIVERABLES
1. Assessment Findings
2. Quick Wins / Near Term Opportunities
3. Future State Operating Model Recommendations

Strategize Planning / Execution of P2

▲ Bus Segment Leaders Kick-off
▲ Project Kick-off
☆ Surveys Open– FRI
☆ Surveys Close - WED
☆ Weekly Checkpoint
✦ UHC / Optum PMO COE Joint Review
★ P1 Closeout / P2 Transition
▲ Draft Recommendations Review Meeting
▲ Business Segment Leadership Debrief

5

++

Durga	Dave
Value Propositions of going to cloud - WHy enterprises should go to cloud 1st pillar - Business Pillar, High level of data reuse 2nd pillar - Technology advantage, scalability, API, Management of data usage 3rd Pillar - Platform product development and enablement in the cloud Data Security plays important role in each part, Data secuirty centricity important in all Data Security Centricity - Managing data - Managing privacy - Analytics on data - What is the technology we need to make transformative impact in data security - Holistic data - Don't have multiple coipes of the data otherwise difficult to manage - Move the data, Tokenize it - For the clients that are new and going to cloud, What should they plan - Two things frighten executives - Ransomware (IT have good hygiene - Monitoring human interaction, DR) and Human Intervention(use automation to manage cloud, allow audit) - Adaptive Data	Value prop why should health care go to cloud - what is value prop 3 pillars: Business value - Data reuse Technology advantage - Scalability, API, Management of data usage Platform and Product enablement - elements in the cloud enable its usage much faster Management of data containment and usage Plays important role More data security centric Highlight where data security shows its value Data security centric challenges Understand consent centric models What technologies we would need Wholistic and pragmatic governance Data secure and available Governance becomes more difficult Avoid multiple copies Ransomware and human intervention Have good hygiene - leverage monitoring Use automation can be a challenge as well

The global healthcare cloud computing market is expected to hit $35 billion by 2022, with an annualized growth rate of 11.6% - BCC research
Approx. 69% of respondents in a 2018 survey indicated that the hospital they worked at did not have a plan for moving existing data centers to the cloud

What frightens executives the most: Ransomware, human interaction and BCDR

Value Prop of going to the cloud; **why should health care go to cloud?**

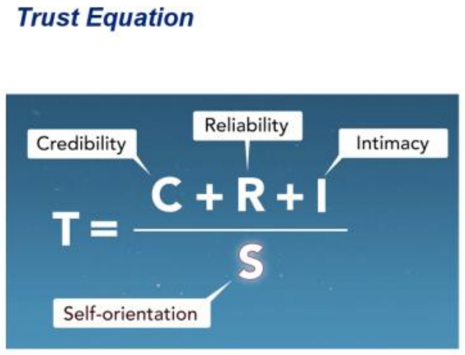
- Pillars
  - Business pillar - High level data reuse
  - Technology advantage - Scalability, API, Management of data usage
  - Platform and product - Enablement of platform and product development
- Faster and easier adoption of new capabilities
- A secure, integrated and scalable foundation
- Can evolve to meet the changing needs of tomorrow

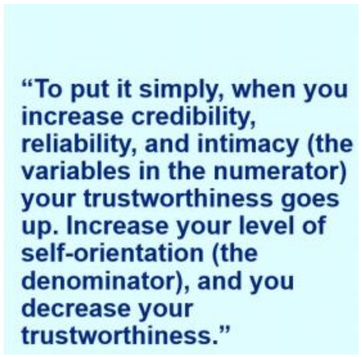
- Lower initial investment; pay-as-you-go payment method, pay only for what you use
- Reallocate time and energy from maintenance to innovation

Data Security plays important role in all aspects of data security; thus the approach has to be security centric

Best practices
Holistic data approach
Holistic and pragmatic governance
Avoid multiple copies of data
Encrypt data at-rest and in flight
Securely transmit data and tokenize it where needed
Understand and implement consent centric models
Ensure data is secure and available
Implement policy based access and serve data on need to know
For new clients to move data to the cloud - plan properly
    Data security
    Data security zones
    Sound policies
    Table, row and column level access control
    Proper governance
    Access control
    Policy based data backup, archival and data retention
    Guard data with proper access controls, policies, governance
++
MBO - what you be $1M target, that will get us the sales credit
Real result count, ust effort does not.
++

Trusted advisor




"To put it simply, when you increase credibility, reliability, and intimacy (the variables in the numerator) your trustworthiness goes up. Increase your level of self-orientation (the denominator), and you decrease your trustworthiness."

++
Data security in cloud computing is a never ending concern
Security threats are always evolving
Cloud computing has enabled users to store data online and making it available when and where it's needed
This flexibility and ease of use presents its own set of risks. These risks should be understood and carefully managed
The most common data security challenges in cloud computing are:
- Lack of data visibility and control
- Cloud misconfiguration can leave data open and unprotected
- Unauthorized access to cloud data
- Cyberattacks and data breaches
- Denial of service attacks
- Hijacking of accounts
- Insecure interfaces and APIs
- Malicious insiders
- Data loss in cloud computing
- Oversight and negligence in cloud data management

Lack of Data Visibility & Control
You should be able to see as much data as needed/allowed and as easily as possible, in order to make appropriate decisions.
To protect data you need to provide real-time data reporting

Cloud Misconfiguration Leaves Data Wide Open & Unprotected
There could be many types of Cloud misconfigurations, such as:
- Granting public access where it shouldn't be
- Improperly creating network functions
- storing passwords or keys in open areas
- offering public access to unencrypted data
- Lack of awareness, oversight, lack of controls, or negligence on behalf of someone else

Cloud misconfiguration is one of the more common data security challenges
Keep track of who is accessing your cloud data.
Even one small mistake could cause a data security issue in your cloud system.

Unauthorized Access to Cloud Data

You must limit the number of people who can get access to your information. The more people who have access, the higher the likelihood that your information could be leaked or may not be kept as secure as you want it to be.
Your data should always be protected, which means you want to have encryption and passwords in place to keep unwanted people from accessing the data.
Unauthorized access is a security breach or data breach, whether the person who accesses it does anything with the information they find or not.
And that could undermine the integrity of your company and the trust your customers have in your abilities.
Preventing these unauthorized breaches is crucial, and luckily there are plenty of ways to make sure it doesn't happen… or at least to lessen the chances of it happening.
First, make sure you have a strong password policy, and even a two-factor or multifactor authentication. This ensures no one is going to get into your information by mistake (someone accidentally clicking on the wrong file).
Look into physical security practices, as well, so users and team members know not to simply walk away from their desks, leaving important and confidential information easily accessible.
Also, monitor user activity so you know who is accessing information, when they are accessing it, and from where, so you can always recognize unauthorized or suspicious activity.
Finally, protect your system from viruses and malware that can allow nefarious users to access your information through direct attacks.

Cyberattacks & Data Breaches

You may not even remember the cyberattack at Yahoo, which happened in 2013. Even worse, the company didn't even announce that a breach had occurred until 2016, three years after the event occurred.
A single Yahoo employee allowed the data breach to happen by clicking on a spear-phishing email that ultimately led to over three billion accounts being accessed by unauthorized agents.
In fact, there were four people who were ultimately indicted for the attack.
This data breach undermined the confidence that users had in the company, because it released personal and proprietary information about the company and customers.
Cyberattacks and data breaches are one of the most common data security challenges in cloud computing; and they can happen to any company, no matter how large the company is.
The most common ways that this occurs is through:

- weak passwords
- stolen passwords
- vulnerable applications
- malware
- social engineering
- providing easy access to multiple users
- insider threats
- brute force attacks
- improper configurations and user errors

It's no wonder these attacks have become very common!
But just what can you do to protect your company and prevent those breaches from happening in the first place?
Start by keeping out as many people as possible. Giving access to too many people means there are a lot of loose ends and a lot of potential access points for a hacker.
In addition to that, you want to look at your general security processes, like firewalls, VPNs, updates, and of course, the way that you train your employees.

Denial of Service (DoS) Attacks

A denial-of-service attack is one that keeps users from being able to access a service, and it can be done to keep your customers off your website, or to keep your team members from accessing your system to get work done.
DoS attacks flood a website with so much traffic that it interrupts services, and it could come from anywhere in the world.
Flooding services, which send an overabundance of traffic to the server, can cause the system to slow down.
This results in difficulty for users trying to access the service, which can cause serious trouble for the organization.
Crashing services are the second method of DoS attacks.
They involve exploiting the vulnerabilities within the organization to crash the website and make sure it is unable to fulfill its service.
In both methods, the goal is to render the service useless to customers.
Unfortunately, they tend to succeed, which is why it’s important to prevent them from the start.
Some of the best ways to prevent these types of attacks from happening are:

- to have even more bandwidth, which offers availability even during high spikes of activity
- redundancy in infrastructure to make it harder for a user with malicious intent from interfering with the website
- configuring the network hardware, specifically to prevent these activities
- using hardware and software systems for protection

Hijacking of Accounts

When someone can access your information and your account by hacking into it, they will have complete access to everything that you have access to.
That means they can view, edit, send, share, or do whatever they like with that information.
It can happen by someone getting ahold of your password or by a brute force attack, or any other reason.
When it occurs, it means that person is in control of your account.
Sometimes they might allow you to also have access, making changes or wreaking havoc in the background.
… But other times, they might completely lock you out of the account before making their changes or doing whatever it is they want with your account.
This could mean huge changes being made that are unauthorized and even harmful to your company or customers. It could even mean large amounts of money being transferred to the hacker.
To prevent this, it’s essential that your company uses a high-quality cloud service provider, implementing a process of secure access, and encrypting the data.
By doing all three of these things from the start, you can drastically mitigate the amount of damage a hacker can cause, because it makes it difficult for a nefarious person to get into your account in the first place.

Insecure Interfaces/APIs

There can be serious security concerns with APIs in the overall cloud computing process.
That’s why it’s crucial to have overall security and protection all the way around.
If you don’t, you leave yourself open to unauthorized people getting access to your data and information. And once a hacker has that information they need, they can do whatever they want with it.
The easier you make it for someone to get access to your information, the more likely that someone is going to do it. And that means your information or your customers’ information can be leaked onto the web.
Protecting the entire system, and especially your interfaces and API, must be a priority in your company from the get-go.
You want to make sure that your API is designed in a way that is cohesive and useful for your team.
It needs to have overall authentication and access control so only the right people are getting access.

Malicious Insider

Disgruntled employees can be a whole lot more trouble than you might think.
In fact, they can cause more than just a strain on your business. They can cost a company lost revenue when they are not happy with the workplace, coworkers, or the management.
These individuals can choose to sell out their company in a data breach or could otherwise scam the organization they work for.
A malicious insider is someone who works within your organization, used to work there, or works in some way adjacent to your organization; but instead of being loyal and supportive of the company, they are looking to undermine the company.
Since they already have access to the company's private information and know how the company operates, they can potentially be more harmful than any other type of hacker.
Identifying these potentially malicious insiders before they become a problem is essential in protecting your data.
You should generally be looking for people who have:

- an official record of security violations, harassment, or hacking
- a history of non-compliance with policies in the company
- falsified information to get themselves hired
- unprofessional behavior
- abusive behavior in the workplace
- personality conflicts
- even misuse of privileges within the company

These individuals may have poor performance, a suspicious level of interest in projects that don't concern them and may violate policies or use their leave time frequently.
Performing company-wide risk assessments regularly, as well as documenting controls and who has access to information is essential to avoid these characters.
Setting up a system of security software and applications, as well as physical security that prevents suspicious activity is essential to protecting physical and digital information.
You should ensure that remote access is strictly controlled, and passwords are held to high standards by the policy.
Lastly, make sure that you have adequate surveillance, destroy old information or systems appropriately, and use dual authentication, wherever possible.

Data Loss in Cloud Computing

Losing information could happen by accidental deletion or by malicious intent.
Either way, it results in a disastrous disruption of your business activities.
As many as 70% of small businesses go out of business as a result of large data losses.
So, how does it happen?
Most commonly, it is a human error. Someone accidentally deletes a file or string of files while working.
It could also be caused by:

- viruses or malware
- damage to a hard drive
- power outages that cause a disruption in backup creation
- theft of physical computers and information that has yet to be backed up
- liquid damage to hardware
- natural disasters
- software corruption
- improper hardware formatting

- And, of course, hackers or insiders that purposely remove information.

Taking care of these problems as quickly as possible means having systems in place to protect your information.
Having a backup of your information in place always is the first and most important step.
In addition to that, make sure you have set in place anti-virus software, control of employee access, and overall maintenance for your computer system are important parts.

Oversight & Negligence in Cloud Data Management

Protecting your company and the information you use depends on you being proactive about it and paying careful attention to every step of the process.
Protecting data means avoiding things like general oversight or negligence on behalf of any of your team members, because simple negligence or not recognizing a problem could mean a huge loss of data and a large-scale security breach.
Avoiding negligence and oversight requires cybersecurity automation, which will automate certain security processes within your organization.
It can be programmed to detect and even fix cyber threats, without requiring any human assistance. But of course, it's not going to catch absolutely every problem.
Cybersecurity automation is an excellent resource, because it might catch things that the average person would miss, and it can act quickly and thoroughly.
Oversight and negligence are one of the more common data security challenges in cloud computing, and they could be solved with a combination of both the human eye and software implementation.
++

Data Security In The Cloud

Data located in the cloud is a particular area of security based on the data's location
Cloud is designed to incorporate a wider network and range of accessibility
Data can be accessed from any location, enabling greater efficiency and productivity
From a security perspective, these qualities open a unique set of entry points and attack vectors

There are three types of cloud deployment models: Public Cloud, Private Cloud and Hybrid Cloud (mixture of Public and Private Cloud). They dictate how data is stored; how customers interact with it and how applications (deployed on cloud) run.

Implementing access control policies, devising encryption solutions, providing employee training, and securing endpoints are some of the best ways to begin securing data in the cloud from unauthorized access.

Compliance, monitoring, and auditing are added steps to make sure your security measures are effective or need the necessary improvements.
From <https://purplesec.us/learn/data-security-strategies/#Cloud>

Data Security Assessment

The data security assessment is **an independent appraisal of the security and effectiveness of IT use**. Data security risk assessment can be broken down into three steps:

1. Identify what the risks are to your critical systems and sensitive data
2. Identify and organize your data by the weight of the risk associated with it
3. Take action to mitigate the risks. You can start with:
   a. Is company data subject to least privilege and/or zero trust access controls?
   b. Do you use network segmentation to limit data access?
   c. Do you have strong identity management processes?
   d. Data security assessments consider the ease and breadth of access to corporate data.
   e. They identify areas where companies should apply new controls to restrict access to data on an as needed basis.

Key components:

- **Threat** — An event that could harm an organization's people or assets
- **Vulnerability** — A weak point that could allow a threat to cause damage
- **Impact** — Total damage the organization would incur if a vulnerability were exploited
- **Likelihood** — Probability that a threat will occur

From <https://www.lepide.com/blog/how-to-perform-an-it-risk-assessment/>
From <https://blog.netwrix.com/2018/01/16/how-to-perform-it-risk-assessment/>
++

Data Security Risk Assessment Checklist

Three key stages: governing access to data, analyzing user behavior, and auditing security states.

1. **Governing Access to Data** - Assess user permissions to sensitive data
   Location of sensitive data; what it is and who has access to it
   Monitor and audit regularly
   Users with Admin Privileges; Permission Changes; Changes to Security Groups/Configurations
2. **Analyzing User Behavior -** Identify and analyze the behavior of high risk users
   Modifications to Data; Failed Logins
3. **Auditing Security States**
   Inactive/Disabled Users; Users with Passwords that Never Expire; Open Shares and Empty Security Groups

From <https://www.lepide.com/blog/data-security-risk-assessment-checklist/>
++

How to perform a security risk assessment

Prioritize the Information Security Risks

- The likelihood that the threat will exploit the vulnerability
- The approximate cost of each of these occurrences
- The adequacy of the existing or planned information system security controls
- A risk-level matrix should be created

Recommend Controls

The risk levels determines the actions needed to mitigate the risk. General guidelines for each level of risk:

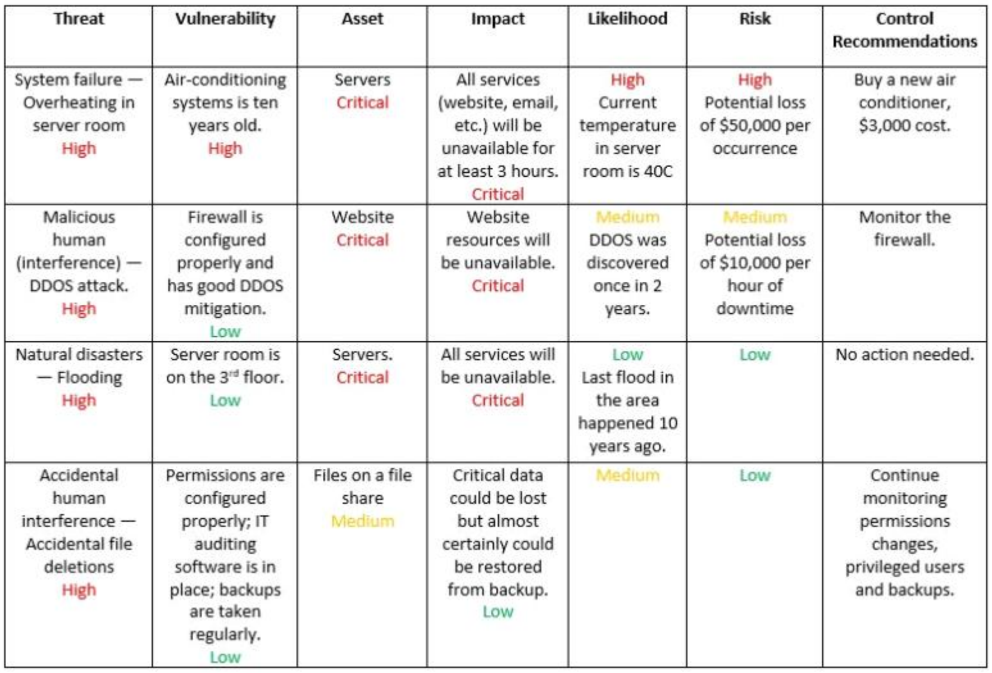
- **High** — An immediate corrective plan
- **Medium** — A corrective plan within a reasonable period of time
- **Low** — Accept the risk or implement corrective actions

Also consider:

- Organizational policies
- Cost-benefit analysis
- Operational impact
- Feasibility
- Applicable regulations
- The overall effectiveness of the recommended controls
- Safety and reliability

Document the Results

For each threat, the report should describe the corresponding vulnerabilities, assets at risk, impact to IT infrastructure, the likelihood and the control recommendations. See below a sample report:



Threat	Vulnerability	Asset	Impact	Likelihood	Risk	Control Recommendations
System failure — Overheating in server room High	Air-conditioning systems is ten years old. High	Servers Critical	All services (website, email, etc.) will be unavailable for at least 3 hours. Critical	High Current temperature in server room is 40C	High Potential loss of $50,000 per occurrence	Buy a new air conditioner, $3,000 cost.
Malicious human (interference) — DDOS attack. High	Firewall is configured properly and has good DDOS mitigation. Low	Website Critical	Website resources will be unavailable. Critical	Medium DDOS was discovered once in 2 years.	Medium Potential loss of $10,000 per hour of downtime	Monitor the firewall.
Natural disasters — Flooding High	Server room is on the 3rd floor. Low	Servers. Critical	All services will be unavailable. Critical	Low Last flood in the area happened 10 years ago.	Low	No action needed.
Accidental human interference — Accidental file deletions High	Permissions are configured properly; IT auditing software is in place; backups are taken regularly. Low	Files on a file share Medium	Critical data could be lost but almost certainly could be restored from backup. Low	Medium	Low	Continue monitoring permissions changes, privileged users and backups.

From <https://blog.netwrix.com/2018/01/16/how-to-perform-it-risk-assessment/>
++
From <https://purplesec.us/learn/security-risk-assessment/>
++
++
[9 Data Security Strategies You Need To Implement In 2022 (purplesec.us)]

Data Security Strategies

1. Identify Data Security Risks
2. Conduct An Asset Inventory
3. Implement A Data Security Policy
4. Mobile Data Security
5. Secure Your Database
6. Data Security In The Cloud
7. Track User Behavior
8. Respect Data Privacy
9. Enforce And Maintain Least-Privilege

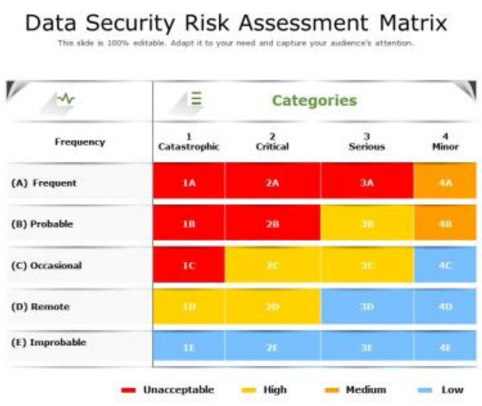
From <https://purplesec.us/learn/data-security-strategies/#Strategies>

common data security solutions:

- Security Awareness
- Data Encryption
- Data Classification
- Data Loss Prevention
- Data Backup And Recovery
- Data Segmentation
- Vulnerability Management
- Network Firewalls
- Physical Security
- Endpoint Protection

From: <https://purplesec.us/learn/data-security-strategies/>

++

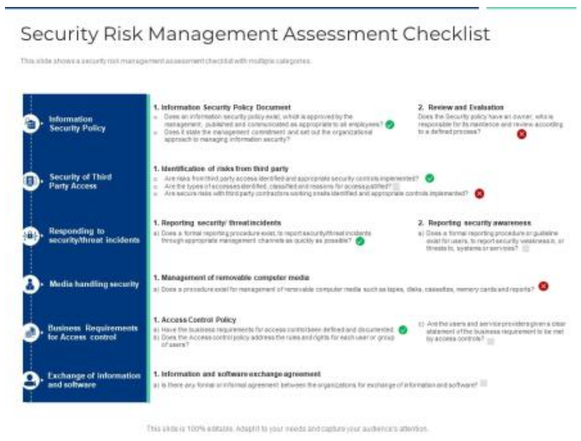


Data Security Risk Assessment Matrix

This slide is 100% editable. Adapt it to your need and capture your audience's attention.

	Categories			
Frequency	1 Catastrophic	2 Critical	3 Serious	4 Minor
(A) Frequent	1A	2A	3A	4A
(B) Probable	1B	2B	3B	4B
(C) Occasional	1C	2C	3C	4C
(D) Remote	1D	2D	3D	4D
(E) Improbable	1E	2E	3E	4E

🟥 Unacceptable 🟨 High 🟧 Medium 🟦 Low



Security Risk Management Assessment Checklist

This slide shows a security risk management assessment checklist with multiple categories.

Information Security Policy

1. Information Security Policy Document
   - Does an information security policy exist, which is approved by the management, published and communicated as appropriate to all employees? ✓
   - Does it state the management commitment and set out the organizational approach to managing information security?

2. Review and Evaluation
   Does the Security policy have an owner, who is responsible for its maintence and review according to a defined process? ✗

Security of Third Party Access

1. Identification of risks from third party
   - Are risks from third party access identified and appropriate security controls implemented? ✓
   - Are the types of accesses identified, classified and reasons for access justified? ☐
   - Are secure risks with third party contractors working onsite identified and appropriate controls implemented? ✗

Responding to security/threat incidents

1. Reporting security/ threat incidents
   a) Does a formal reporting procedure exist, to report security/threat incidents through appropriate management channels as quickly as possible? ✓

2. Reporting security awareness
   a) Does a formal reporting procedure or guideline exist for users, to report security weakness in, or threats to, systems or services? ☐

Media handling security

1. Management of removable computer media
   a) Does a procedure exist for management of removable computer media such as tapes, disks, cassettes, memory cards and reports? ✗

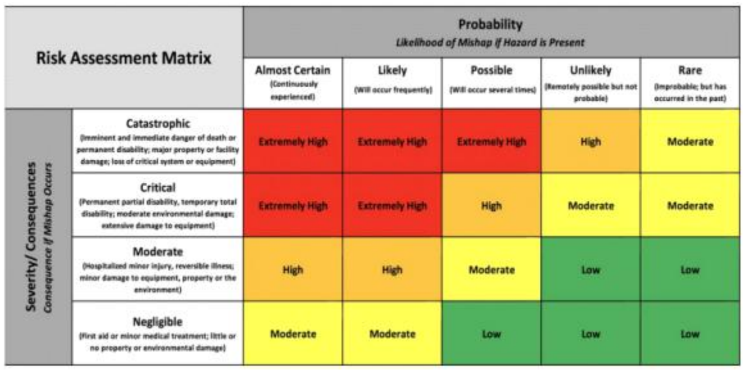
Business Requirements for Access control

1. Access Control Policy
   a) Have the business requirements for access control been defined and documented ✓
   b) Does the Access control policy address the rules and rights for each user or group of users?
   c) Are the users and service providers given a clear statement of the business requirement to be met by access controls? ☐

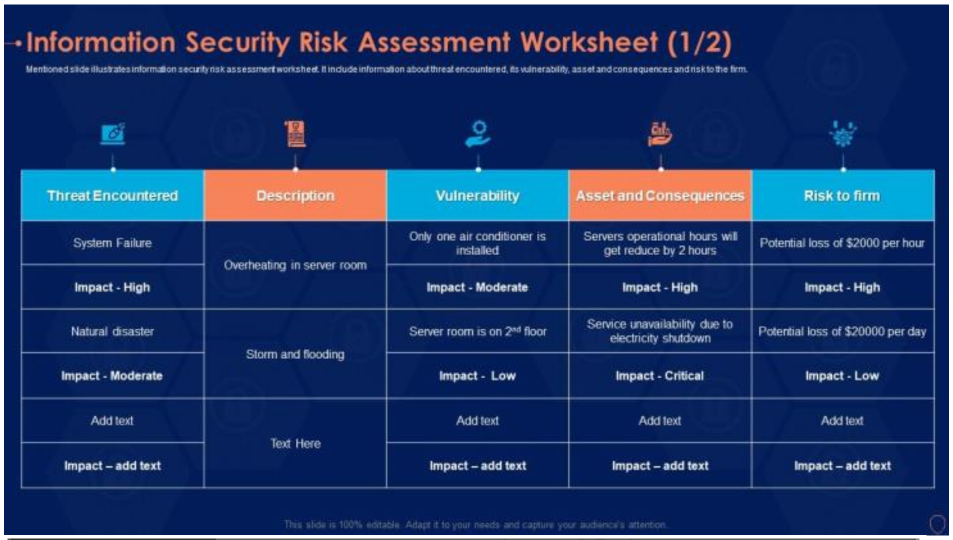
Exchange of information and software

1. Information and software exchange agreement
   a) Is there any formal or informal agreement between the organizations for exchange of information and software? ☐

This slide is 100% editable. Adapt it to your needs and capture your audience's attention.



Risk Assessment Matrix		Probability *Likelihood of Mishap if Hazard is Present*				
		Almost Certain (Continuously experienced)	Likely (Will occur frequently)	Possible (Will occur several times)	Unlikely (Remotely possible but not probable)	Rare (Improbable; but has occurred in the past)
Severity/ Consequences *Consequence if Mishap Occurs*	Catastrophic (Imminent and immediate danger of death or permanent disability; major property or facility damage; loss of critical system or equipment)	Extremely High	Extremely High	Extremely High	High	Moderate
	Critical (Permanent partial disability, temporary total disability; moderate environmental damage; extensive damage to equipment)	Extremely High	Extremely High	High	Moderate	Moderate
	Moderate (Hospitalized minor injury, reversible illness; minor damage to equipment, property or the environment)	High	High	Moderate	Low	Low
	Negligible (First aid or minor medical treatment; little or no property or environmental damage)	Moderate	Moderate	Low	Low	Low

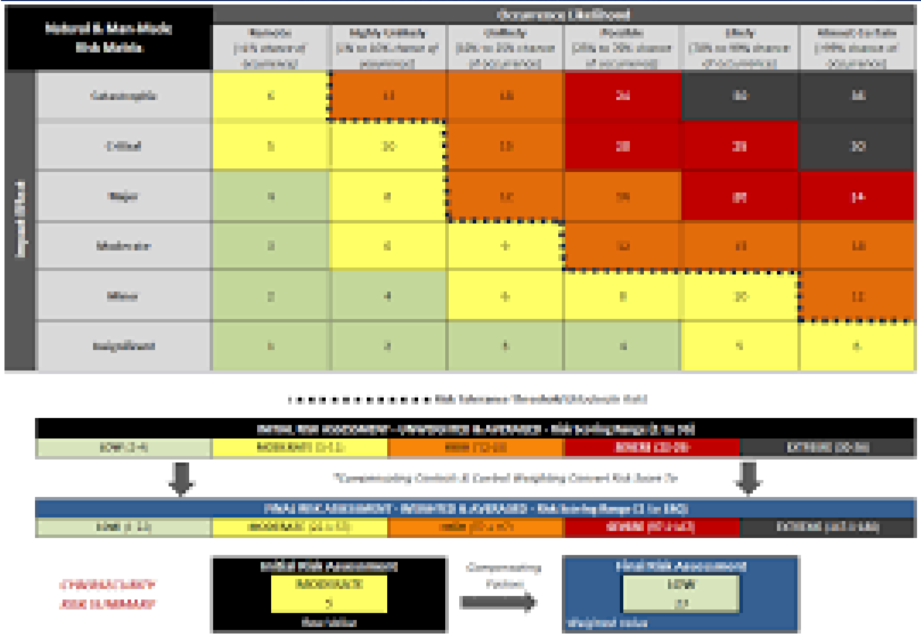


Information Security Risk Assessment Worksheet (1/2)

Mentioned slide illustrates information security risk assessment worksheet. It include information about threat encountered, its vulnerability, asset and consequences and risk to the firm.

Threat Encountered	Description	Vulnerability	Asset and Consequences	Risk to firm
System Failure	Overheating in server room	Only one air conditioner is installed	Servers operational hours will get reduce by 2 hours	Potential loss of $2000 per hour
Impact - High		**Impact - Moderate**	**Impact - High**	**Impact - High**
Natural disaster	Storm and flooding	Server room is on 2nd floor	Service unavailability due to electricity shutdown	Potential loss of $20000 per day
Impact - Moderate		**Impact - Low**	**Impact - Critical**	**Impact - Low**
Add text	Text Here	Add text	Add text	Add text
Impact – add text		**Impact – add text**	**Impact – add text**	**Impact – add text**

This slide is 100% editable. Adapt it to your needs and capture your audience's attention.



Natural & Man-Made Risk Matrix	Occurrence Likelihood					
	Remote [illegible]	Highly Unlikely [illegible]	Unlikely [illegible]	Possible [illegible]	Likely [illegible]	Almost Certain [illegible]
Catastrophic	6	12	18	24	30	36
Critical	5	10	15	20	25	30
Major	4	8	12	16	20	24
Moderate	3	6	9	12	15	18
Minor	2	4	6	8	10	12
Insignificant	1	2	3	4	5	6

Impact [illegible]

Risk Tolerance Threshold [illegible]

[illegible]

LOW [illegible]	MODERATE [illegible]	HIGH [illegible]	SEVERE [illegible]	EXTREME [illegible]

[illegible]

FINAL RISK ASSESSMENT [illegible]

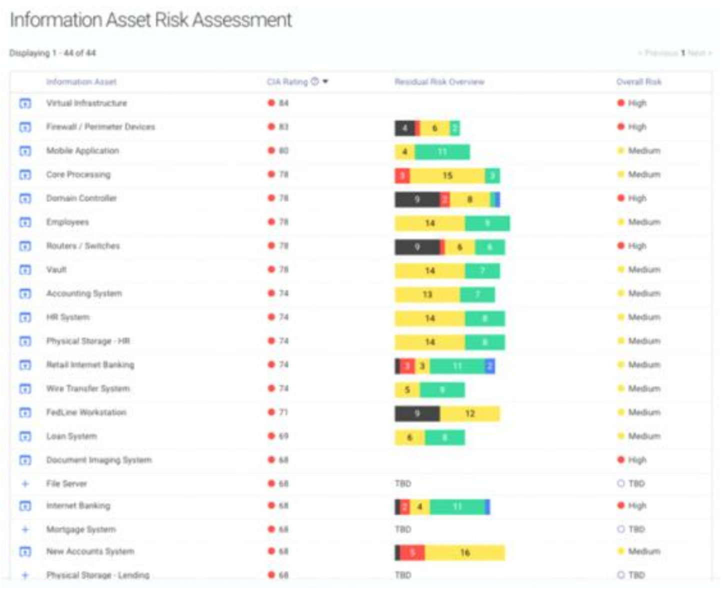
LOW [illegible]	MODERATE [illegible]	HIGH [illegible]	SEVERE [illegible]	EXTREME [illegible]

[illegible] RISK SUMMARY

Initial Risk Assessment
MODERATE
5
Raw Value

Compensating Factors

Final Risk Assessment
LOW
[illegible]
Weighted Value



Information Asset Risk Assessment

Displaying 1 - 44 of 44 ‹ Previous 1 Next ›

Information Asset	CIA Rating	Residual Risk Overview	Overall Risk
Virtual Infrastructure	● 84		● High
Firewall / Perimeter Devices	● 83	4 6 2	● High
Mobile Application	● 80	4 11	● Medium
Core Processing	● 78	3 15 3	● Medium
Domain Controller	● 78	9 2 8	● High
Employees	● 78	14 9	● Medium
Routers / Switches	● 78	9 6 6	● High
Vault	● 78	14 7	● Medium
Accounting System	● 74	13 7	● Medium
HR System	● 74	14 8	● Medium
Physical Storage - HR	● 74	14 8	● Medium
Retail Internet Banking	● 74	3 3 11 2	● Medium
Wire Transfer System	● 74	5 9	● Medium
FedLine Workstation	● 71	9 12	● Medium
Loan System	● 69	6 8	● Medium
Document Imaging System	● 68		● High
File Server	● 68	TBD	○ TBD
Internet Banking	● 68	2 4 11	● High
Mortgage System	● 68	TBD	○ TBD
New Accounts System	● 68	5 16	● Medium
Physical Storage - Lending	● 68	TBD	○ TBD

Data Security Risk Assessment Template

Data Security Risk Assessment Template

01

This slide is 100% editable. Adapt it to your needs and capture your audience's attention.

Text Here

02

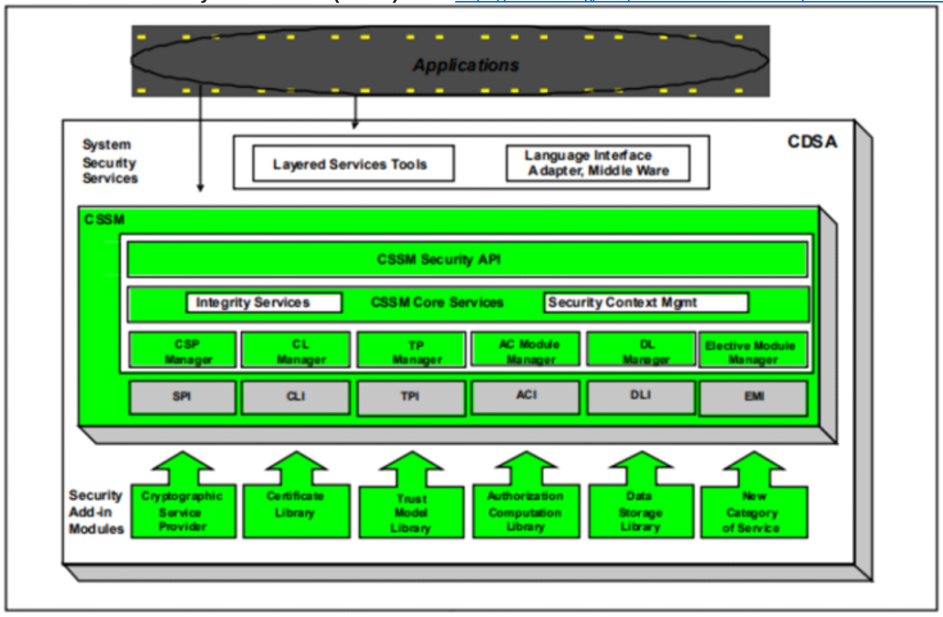
This slide is 100% editable. Adapt it to your needs and capture your audience's attention.

Text Here

03

This slide is 100% editable. Adapt it to your needs and capture your audience's attention.

Common Data Security Architecture (CDSA) From <https://cio-wiki.org/wiki/Common_Data_Security_Architecture_%28CDSA%29>



++

Data Breaches

- In June 2020, Wattpad, the website where people can write their own stories, suffered a data breach that exposed almost 268 million records. The breach exposed personal information including usernames, IP addresses and even passwords stored as bcrypt hashes.
- In May, 2019, the Australian graphic designing application called Canva suffered an attack that breached 137 million user accounts. The data breach included exposed usernames, passwords, email addresses and even city of residence.
- Sina Weibo experienced a breach in early 2020 where 538 million user accounts were compromised. This breach exposed usernames, numbers, locations and even real names.

+++

Data Security Implementation

- Establish the desired security state
- Conduct a physical and logical review of the IT security components
- Assemble a data security team and assign responsibilities
- Align IT security components with business' goals
- Implement Element Level Security at the Individual Document Level
- Identify and classify sensitive data
- Create a data usage policy
- Control access to sensitive data
- Implement change management and database auditing
- Use data encryption
- Back up your data
- Use redundant data storage
- Apply a proper patch management strategy
- Protect your data from insider threats
- Use endpoint security systems to protect your data
- Perform vulnerability assessments and cybersecurity penetration tests
  From <https://www.datacenterknowledge.com/industry-perspectives/three-must-implement-data-security-steps-reduce-vulnerabilities>

Data security techniques and technologies

- Administrative controls
- Physical security
- Logical controls
- Organizational standards
- Safeguarding techniques

- Data encryption
- Data masking
- Data erasure
- Data resilience

Attacks against which the data need to be protected

Internal Threats include:

- Social engineering
- Shadow IT
- Data sharing outside the company
- Use of unauthorized devices
- Physical theft

External Threats include:

- Hacking
- Malware
- Phishing attacks

Features of the data security solution

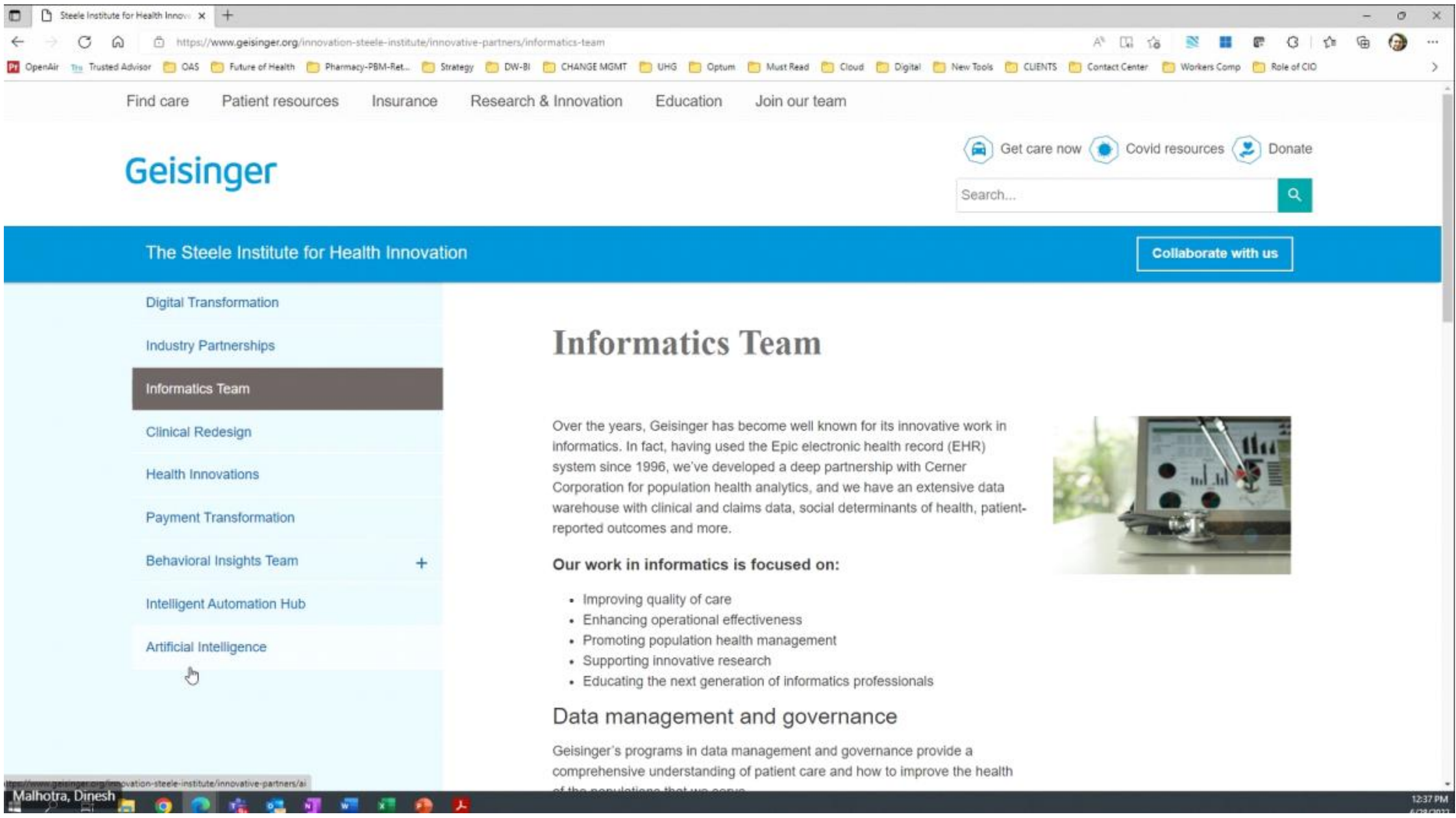
- Catalog & collect on-premises, hybrid and multi cloud data assets into a single repository
- Discover sensitive data attributes out-of-the-box
- Utilize People-Data-Graph to link personal data to its owners and fulfill privacy use-cases
- Detect and classify unstructured data for effective governance, protection and privacy
- Highlight data risk with each data set using a risk score
- Run security and privacy functions in an automated way

Best practices for implementing data security controls

- Understand the nature of data that needs to be protected, e.g., databases
- Track any foreseeable threats
- Follow industry best practices
- Consider the costs implications

From <https://www.netwrix.com/data_security_best_practices.html>

++



Informatics Team

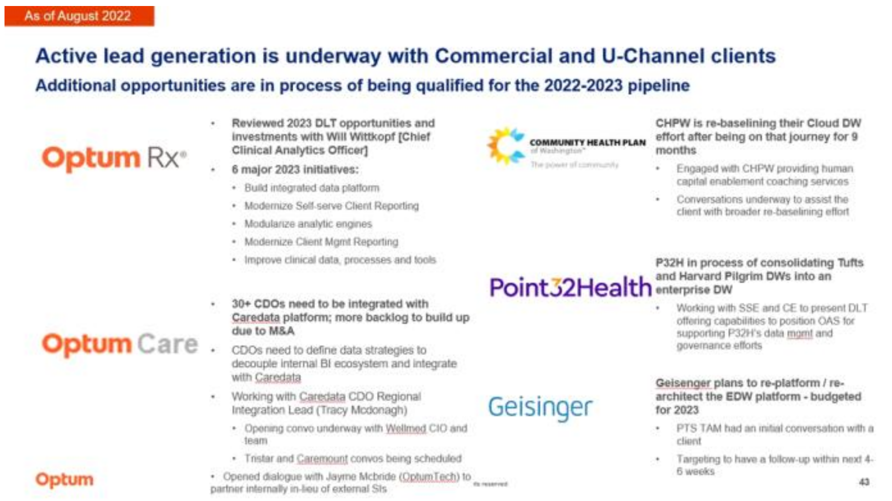
Over the years, Geisinger has become well known for its innovative work in informatics. In fact, having used the Epic electronic health record (EHR) system since 1996, we've developed a deep partnership with Cerner Corporation for population health analytics, and we have an extensive data warehouse with clinical and claims data, social determinants of health, patient-reported outcomes and more.

Our work in informatics is focused on:

- Improving quality of care
- Enhancing operational effectiveness
- Promoting population health management
- Supporting innovative research
- Educating the next generation of informatics professionals

Data management and governance

Geisinger's programs in data management and governance provide a comprehensive understanding of patient care and how to improve the health


As of August 2022

Active lead generation is underway with Commercial and U-Channel clients

Additional opportunities are in process of being qualified for the 2022-2023 pipeline

Optum Rx®

- **Reviewed 2023 DLT opportunities and investments with Will Wittkopf [Chief Clinical Analytics Officer]**
- **6 major 2023 initiatives:**
  - Build integrated data platform
  - Modernize Self-serve Client Reporting
  - Modularize analytic engines
  - Modernize Client Mgmt Reporting
  - Improve clinical data, processes and tools

Optum Care

- **30+ CDOs need to be integrated with Caredata platform; more backlog to build up due to M&A**
- CDOs need to define data strategies to decouple internal BI ecosystem and integrate with Caredata
- Working with Caredata CDO Regional Integration Lead (Tracy Mcdonagh)
  - Opening convo underway with Wellmed CIO and team
  - Tristar and Caremount convos being scheduled
- Opened dialogue with Jayme Mcbride (OptumTech) to partner internally in-lieu of external SIs

COMMUNITY HEALTH PLAN of Washington™ The power of community

CHPW is re-baselining their Cloud DW effort after being on that journey for 9 months

- Engaged with CHPW providing human capital enablement coaching services
- Conversations underway to assist the client with broader re-baselining effort

Point32Health

P32H in process of consolidating Tufts and Harvard Pilgrim DWs into an enterprise DW

- Working with SSE and CE to present DLT offering capabilities to position OAS for supporting P32H's data mgmt and governance efforts

Geisinger

Geisenger plans to re-platform / re-architect the EDW platform - budgeted for 2023

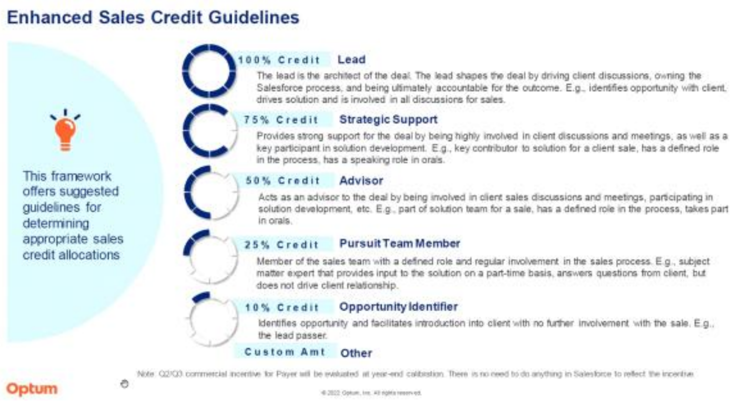
- PTS TAM had an initial conversation with a client
- Targeting to have a follow-up within next 4-6 weeks

Optum

its reserved

43

++



Enhanced Sales Credit Guidelines

This framework offers suggested guidelines for determining appropriate sales credit allocations

100% Credit **Lead**
The lead is the architect of the deal. The lead shapes the deal by driving client discussions, owning the Salesforce process, and being ultimately accountable for the outcome. E.g., identifies opportunity with client, drives solution and is involved in all discussions for sales.

75% Credit **Strategic Support**
Provides strong support for the deal by being highly involved in client discussions and meetings, as well as a key participant in solution development. E.g., key contributor to solution for a client sale, has a defined role in the process, has a speaking role in orals.

50% Credit **Advisor**
Acts as an advisor to the deal by being involved in client sales discussions and meetings, participating in solution development, etc. E.g., part of solution team for a sale, has a defined role in the process, takes part in orals.

25% Credit **Pursuit Team Member**
Member of the sales team with a defined role and regular involvement in the sales process. E.g., subject matter expert that provides input to the solution on a part-time basis, answers questions from client, but does not drive client relationship.

10% Credit **Opportunity Identifier**
Identifies opportunity and facilitates introduction into client with no further involvement with the sale. E.g., the lead passer.

Custom Amt **Other**

Note: Q2/Q3 commercial incentive for Payer will be evaluated at year-end calibration. There is no need to do anything in Salesforce to reflect the incentive.

Optum

© 2022 Optum, Inc. All rights reserved.

Notes

Wednesday, March 30, 2022 5:52 PM

Dinesh notes 03/29/2022

Data Security

- Data in motion
- Data at rest
- Encryption
- Scalability, affordability
- 90% have started
- Cloud migration
- Authorization
- Hybrid on-prem and cloud
- Multicloud strategy
- Data Security
  - broader information security - cyber security
  - Different dimensions of security
    - HIPAA, PHII, Masking, obfuscation
    - role based access control, security at column level, manage privileges, authorization, scanning tools

Data masking and Data tokenization

Information and Data security SME
Durga and John to be included as well
John is in Optum Tech.
Data Leakage Protection (DLP)
Legal protection
Privacy
Microsoft: identity and access management, threat protection, information protection and cloud security
++

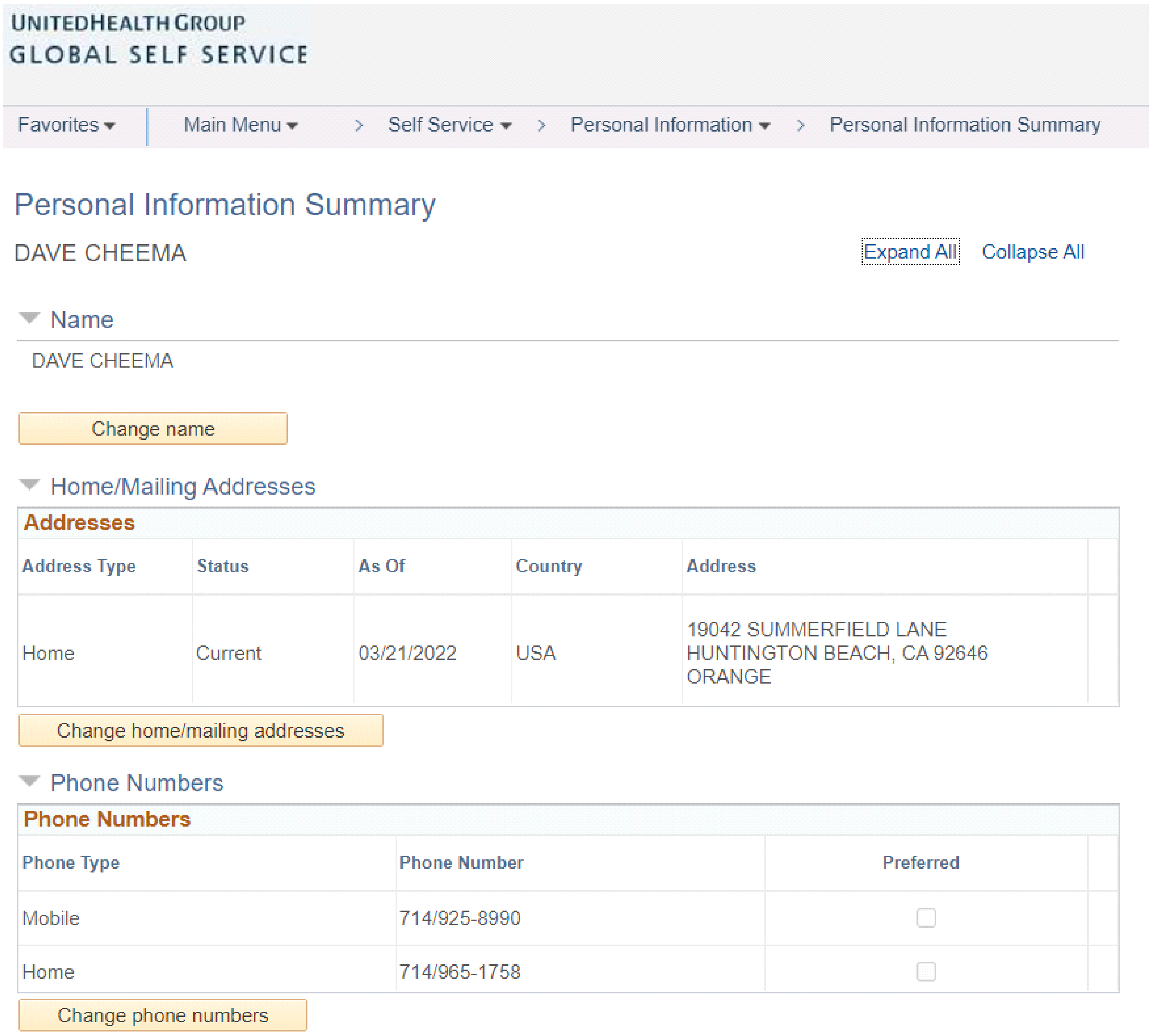
Data Governance
Data Consistency and Integrity
Encrypting data by default
Regular IT risk assessments to know the risks your organization faces and map them to business outcomes

Applying access control
Patching, updates, and network monitoring
Ensuring data protection, retention, and redundancy
Maintaining governance and compliance
Demanding attestations and certifications
Comprehensive Security Posture

Personal

Sunday, April 3, 2022 9:27 PM

Performance evaluation
Contribution Tracker
OAS Training
Career model
I would be invited to some formal meetings
Bob Clemens, John Shin and Mike Haberman are helpful resources
Individual MBOs
Self-assessed utilization
An Excel sheet is created for the Sales Cycle
Stay on top of sales opportunity
Opportunity leads that determined how you would be rewarded
Sheri Dyer is the manager of individual contributions
Practice contribution is the biggest contributor
You work with the opportunity manager to determine what was your contribution
There would be a training on sales contribution
Innovation - such as new offering
Pull through sales
People coaching and mentoring will make you stand out
Career model
++
Allegiance to OAS PTS
Spinning cycle time is an investment
+++



Personal Information Summary

DAVE CHEEMA

Name

DAVE CHEEMA

Home/Mailing Addresses

Addresses

Address Type	Status	As Of	Country	Address
Home	Current	03/21/2022	USA	19042 SUMMERFIELD LANE HUNTINGTON BEACH, CA 92646 ORANGE

Phone Numbers

Phone Numbers

Phone Type	Phone Number	Preferred
Mobile	714/925-8990	☐
Home	714/965-1758	☐

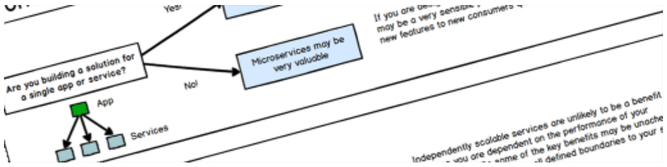
Microservices

Tuesday, April 5, 2022 11:02 AM

The Death of Microservice Madness in 2018

Posted on Jan 12, 2018 | 3090 words | ~15 mins
Microservices Docker Kubernetes CodeProject Devops
En Español | Reddit Thread | Hacker News Thread

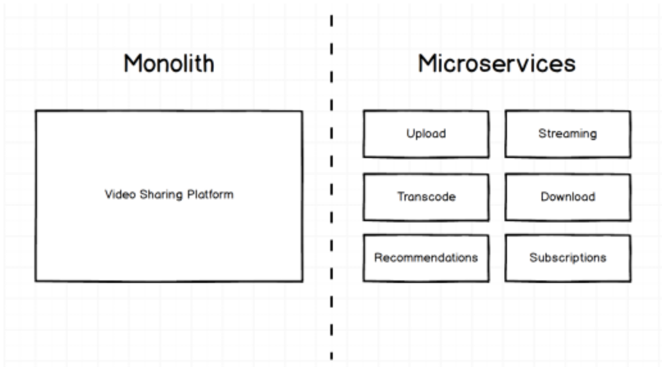
Microservices became a very popular topic over the last couple of years[1]. 'Microservice madness' goes something like this:
Netflix are great at devops. Netflix do microservices. Therefore: If I do microservices, I am great at devops.
There are many cases where great efforts have been made to adopt microservice patterns without necessarily understanding how the costs and benefits will apply to the specifics of the problem at hand.
I'm going to describe in detail what microservices are, why the pattern is so appealing, and also some of the key challenges that they present.
I'll finish with a set of simple questions might be valuable to ask yourself when you are considering whether microservices are the right pattern *for you*. The questions are at the end of the article.



Yes
Are you building a solution for a single app or service?
No!
Microservices may be very valuable
App
Services

What are microservices, and why are they so popular?

Let's start with the basics. Here is how a hypothetical video sharing platform might be implemented, first in the form of a monolith (single large unit) and then in the form of microservices:



The difference between the two systems is that the first is a single large unit; a monolith. The second is a set of small, specific services. Each service has a specific role.
When the diagram is drawn *at this level of detail*, it is easy to see the appeal. There are a whole host of potential benefits:
Independent Development: Small, independent components can be built by small, independent teams. A group can work on a change to the 'Upload' service without interfering with the 'Transcode' service, or even knowing about it. The amount of time to learn about a component is greatly reduced, and it is easier to develop new features.
Independent Deployment: Each individual component can be deployed independently. This allows new features to be released with greater velocity and less risk. Fixes or features for the 'Streaming' component can be deployed without requiring other components to be deployed.
Independent Scalability: Each component can be scaled independently of each other. During busy periods when new shows are released, the 'Download' component can be scaled up to handle the increased load, without having to scale up every component, which makes elastic scaling more feasible and reduces costs.
Reusability: Components fulfil a small, specific function. This means that they can more easily be adapted for use in other systems, services or products. The 'Transcode' component could be used by other business units, or even turned into a new business, perhaps offering transcoding services for other groups.
At this level of detail, the benefits of a microservice model over a monolithic model seem obvious. So if that's the case - why is this pattern only recently in vogue? Where has it been all my life?

If this is so great, why hasn't it been done before?

There are two answers to this question. One is that *it has* - to the best of our technical capabilities, and the other is that more recent technical advances have allowed us to take it to a new level.
When I started writing the answer to this question, it turned into a *long* description, so I'm actually going to separate it into another article and publish it a little later[2]. At this stage, I will skip the journey from single program to many programs, ignore ESBs and Service Orientated Architecture, component design and bounded contexts, and so on.
Those who are interested can read more about the journey separately. Instead I'll say that in many ways we've been doing this for a while, but with the recent explosion in popularity of container technology (Docker in particular) and in orchestration technology (such as Kubernetes, Mesos, Consul and so on) this pattern has become much more viable to implement from a technical standpoint.
So if we take it as a given that we *can* implement a microservice arrangement, we need to think carefully about the *should*. We've seen the high-level theoretical benefits, but what about the challenges?

What's the problem with microservices?

If microservices are so great, what's the big deal? Here are some of the biggest issues I've seen.
Increased complexity for developers
Things *can* get a lot harder for developers. In the case where a developer wants to work on a *journey*, or feature which might span many services, that developer has to run them all on their machine, or connect to them. This is often more complex than simply running a single program.
This challenge can be partially mitigated with tooling[3], but as the number of services which makes up a system increases, the more challenges developers will face when running the system as a whole.
Increased complexity for operators
For teams who don't develop services, but maintain them, there is an explosion in potential complexity. Instead of perhaps managing a few running services, they are managing dozens, hundreds or thousands of running services. There are more services, more communication paths, and more areas of potential failure.
Increased complexity for devops
Reading the two points above, it may grate that operations and development are treated separately, especially given the popularity of devops as a practice (which I am a big proponent of). Doesn't devops mitigate this?

The challenge is that many organisations still run with separated development and operations teams - and a organisation that does is much more likely to struggle with adoption of microservices.
For organisations which have adopted devops, it's still hard. Being both a developer and an operator is already tough (but critical to build good software), but having to also understand the nuances of container orchestration systems, particularly systems which are evolving at a rapid pace, is very hard. Which brings me onto the next point.

It requires serious expertise

When done by experts, the results can be wonderful. But imagine an organisation where perhaps things are not running smoothly with a single monolithic system. What possible reason would there be that things would be any better by increasing the number of systems, which increases the operational complexity?
Yes, with effective automation, monitoring, orchestration and so on, this is all possible. But the challenge is rarely the technology - the challenge is finding people who can use it effectively. These skillsets are currently in very high demand, and may be difficult to find.

Real world systems often have poorly defined boundaries

In all of the examples we used to describe the benefits of microservices, we spoke about *independent* components. However in many cases components are simply not independent. On paper, certain domains may look bounded, but as you get into the muddy details, you may find that they are more challenging to model than you anticipated.
This is where things can get *extremely* complex. If your boundaries are actually not well defined, then what happens is that even though *theoretically* services can be deployed in isolation, you find that due to the inter-dependencies between services, you have to deploy *sets* of services as a group.
This then means that you need to manage coherent versions of services which are proven and tested when working together, you don't actually have an independently deployable system, because to deploy a new feature, you need to carefully orchestrate the simultaneous deployment of many services.

The complexities of state are often ignored

In the previous example, I mentioned that a feature deployment may require the simultaneous rollout of many versions of many services in tandem. It is tempting to assume that sensible deployment techniques will mitigate this, for example blue/green deployments (which most service orchestration platforms handle with little effort), or multiple versions of a service being run in parallel, with consuming channels deciding which version to use.
These techniques mitigate a large number of the challenges *if the services are stateless*. But stateless services are quite frankly, easy to deal with. In fact, if you have stateless services, then I'd be inclined to consider skipping microservices altogether and consider using a serverless model.
In reality, many services require state. An example from our video sharing platform might be the subscription service. A new version of the subscriptions service may store data in the subscriptions database in a different shape. If you are running both services in parallel, you are running the system with two schemas at once. If you do a blue green deployment, and other services depend on data in the new shape, then they must be updated *at the same time*, and if the subscription service deployment fails and rolls back, they might need to roll back too, with cascading consequences.
Again, it might be tempting to think that with NoSQL databases these issues of schema go away, but they don't. Databases which don't enforce schema do not lead to schemaless systems - they just mean that schema tends to be managed at the application level, rather than the database level. The fundamental challenge of understanding the shape of your data, and how it evolves, cannot be eliminated.

The complexitities of communication are often ignored

As you build a large network of services which depend on each other, the liklihood is that there will be a lot of inter-service communication. This leads to a few challenges. Firstly, there are a lot more points at which things can fail. We must expect that network calls will fail, which means when one service calls another, it should expect to have to retry a number of times at the least. Now when a service has to potentially call many services, we end up in a complicated situation.
Imagine a user uploads a video in the video sharing service. We might need to run the upload service, pass data to the transcode service, update subscriptions, update recommendations and so on. All of these calls require a degree of orchestration, if things fail we need to retry.
This retry logic can get hard to manage. Trying to do things synchronously often ends up being untenable, there are too many points of failure. In this case, a more reliable solution is to use asynchronous patterns to handle communication. The challenge here is that asynchronous patterns inherently make a system stateful. As mentioned in the previous point, stateful systems and systems with distributed state are very hard to handle.
When a microservice system uses message queues for intra-service communication, you essentially have a large database (the message queue or broker) glueing the services together. Again, although it might not seem like a challenge at first, schema will come back to bite you. A service at version X might write a message with a certain format, services which depend on this message will also need to be updated when the sending service changes the details of the message it sends.
It is possible to have services which can handle messages in many different formats, but this is hard to manage. Now when deploying new versions of services, you will have times where two different versions of a service may be trying to process messages from the same queue, perhaps even messages sent by different versions of a sending service. This can lead to complicated edge cases. To avoid these edge cases, it may be easier to only allow certain versions of messages to exist, meaning that you need to deploy a set of versions of a set of services as a coherent whole, ensuring messages of older versions are drained appropriately first.
This highlights again that the idea of independent deployments may not hold as expected when you get into the details.

Versioning can be hard

To mitigate the challenges mentioned previously, versioning needs to be very carefully managed. Again, there can be a tendency to assume that following a standard such as semver[4] will solve the problem. It doesn't. Semver is a sensible convention to use, but you will still have to track the versions of services and APIs which can work together.
This can get very challenging very quickly, and may get to the point where you don't know which versions of services will actually work properly together.
Managing dependencies in software systems is notoriously hard, whether it is node modules, Java modules, C libraries or whatever. The challenges of *conflicts between independent components* when consumed by a single entity are very hard to deal with.
These challenges are hard to deal with when the dependencies are static, and can be patched, updated, edited and so on, but if the dependencies are themselves *live services*, then you may not be able to just update them - you may have to run many versions (with the challenges already described) or bring down the system until it is fixed holistically.

Distributed Transactions

In situations where you need transaction integrity across an operation, microservices can be very painful. Distributed state is hard to deal with, many small units which can fail make orchestrating transactions very hard.
It may be tempting to attempt to avoid the problem by making operations idempotent, offering retry mechanisms and so on, and in many cases this might work. But you may have scenarios where you simply need a transaction to fail or succeed, and never be in an intermediate state. The effort involved in working around this or implementing it in a microservice model may be very high.

Microservices can be monoliths in disguise

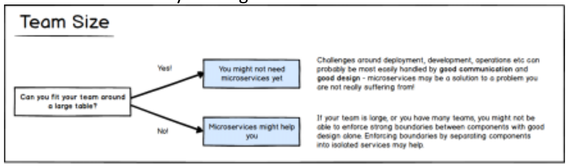
Yes, individual services and components *may* be deployed in isolation, however in most cases you are going to have to be running some kind of orchestration platform, such as Kubernetes. If you are using a managed service, such as Google's GKE4 or Amazon's EKS5, then a large amount of the complexity of managing the cluster is handled for you.
However, if you are managing the cluster yourself, you are managing a large, complicated, mission critical system. Although the individual services may have all of the benefits described earlier, you need to very carefully manage your cluster. Deployments of this system can be hard, updates can be hard, failover can be hard and so on.
In many cases the overall benefits are still there, but it is important not to trivialise or underestimate the additional complexity of managing another big, complex system. Managed services may help, but in many cases these services are nascent (Amazon EKS was only announced at the end of 2017 for example).

Networking Nightmares

A more traditional model of services running on known hosts, with known addresses, has a fairly simple networking setup.
However, when using microservices, generally there will be many services distributed across many nodes, which typically means there's going to be a *much* more complicated networking arrangement. There will be load balancing between services, DNS may be more heavily used, virtual networking layers, etc etc, to attempt to 'hide' the complexity of this networking.
However, as per Tesler's Law (or the Law of Conservation of Compexlity), this networking complexity is inherent - when you are finding real, runtime issues in larger scale clusters, it can often be at a very low networking level. These sorts of issues can be *very* hard to diagnose. I have started tracking some examples at the end of the article, but I think that Tinder's Migration to Kuberenetes shows this challenge very well.
Overall - the transition is still likely to be for the best, but doesn't come without some serious challenges at the networking level, which will require some serious expertise to deal with!

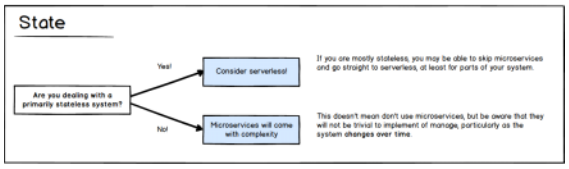
The Death of Microservice Madness!

Avoid the madness by making careful and considered decisions. To help out on this I've noted a few questions you might want to ask yourself, and what the answers might indicate:


Team Size
Can you fit your team around a large table?
Yes!
You might not need microservices yet
No!
Microservices might help you

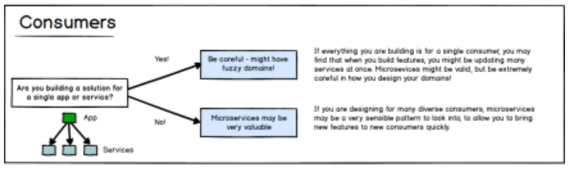
Challenges around deployment, development, operations etc can probably be most easily handled by **good communication** and **good design** - microservices may be a solution to a problem you are not really suffering from!

If your team is large, or you have many teams, you might not be able to enforce strong boundaries between components with good design alone. Enforcing boundaries by separating components into isolated services may help.


State
Are you dealing with a primarily stateless system?
Yes!
Consider serverless!
No!
Microservices will come with complexity

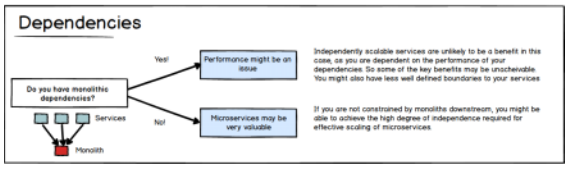
If you are mostly stateless, you may be able to skip microservices and go straight to serverless, at least for parts of your system.

This doesn't mean don't use microservices, but be aware that they will not be trivial to implement of manage, particularly as the system **changes over time**.


Consumers
Are you building a solution for a single app or service?
App
Services
Yes!
Be careful - might have fuzzy domains!
No!
Microservices may be very valuable

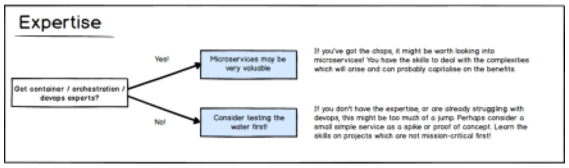
If everything you are building is for a single consumer, you may find that when you build features, you might be updating many services at once. Microsevices might be valid, but be extremely careful in how you design your domains!

If you are designing for many diverse consumers, microservices may be a very sensible pattern to look into, to allow you to bring new features to new consumers quickly.


Dependencies
Do you have monolithic dependencies?
Services
Monolith
Yes!
Performance might be an issue
No!
Microservices may be very valuable

Independently scalable services are unlikely to be a benefit in this case, as you are dependent on the performance of your dependencies. So some of the key benefits may be unacheivable. You might also have less well defined boundaries to your services.

If you are not constrained by monoliths downstream, you might be able to achieve the high degree of independence required for effective scaling of microservices.


Expertise
Got container / orchestration / devops experts?
Yes!
Microservices may be very valuable
No!
Consider testing the water first!

If you've got the chops, it might be worth looking into microservices! You have the skills to deal with the complexities which will arise and can probably capitalise on the benefits.

If you don't have the expertise, or are already struggling with devops, this might be too much of a jump. Perhaps consider a small simple service as a spike or proof of concept. Learn the skills on projects which are not mission-critical first!

You can download a PDF copy here: microservice-questions.pdf

Final Thoughts: Don't Confuse Microservices with Architecture

I've deliberately avoided the 'a' word in this article. But my friend Zoltan made a very good point when proofing this article (which he has contributed to).

There is no microservice architecture. Microservices are just another pattern or implementation of components, nothing more, nothing less. Whether they are present in a system or not does not mean that the architecture of the system is solved.

Microservices relate in many ways more to the technical processes around packaging and operations rather than the intrinsic design of the system. Appropriate boundaries for components continues to be one of the most important challenges in engineering systems.

Regardless of the size of your services, whether they are in Docker containers or not, you will always need to think carefully about how to put a system together. There are no right answers, and there are a *lot* of options.

I hope you found this article interesting! As always, please do comment below if you have any questions or thoughts. You can also follow some lively discussions on:

- Reddit - The Death of Microservice Madness
- Hacker News - The Death of Microservice Madness

Appendix: Further Reading

The following links might be of interest:

- Martin Fowler - Bounded Context - Martin's articles are great, I'd thoroughly recommend this.
- Martin Fowler - Microservices - An often recommended introduction to the pattern.
- Microservices - Good or Bad? - Björn Frantzén's thoughts on microservices, after reading this article.
- When Not To Do Microservices - Excellent post on the topic from Christian Posta
- Sean Hull - 30 questions to ask a serverless fanboy - Interesting thoughts on the challenges of serverless, from a serverless fan!
- Dave Kerr - Monoliths to Microservices - Practical tips for CI/CD and DevOps in the Microservice world - A recent conference presentation I did on devops with microservices.
- Alexander Yermakov - Microservices without fundamentals - A response to this article, with Alex's thoughts and counterpoints to the points raised here (see also Microservices as a self sufficient concept)

Please do share anything else you think makes great reading or watching on the topic!

Thanks

Thanks José from campusmvp.es for having the article translated in Spanish - La muerte de la locura de los microservicios en 2018!

Case Studies

Some interesting examples of experiences I am collecting of larger organisations who have made large scale transitions to microservices:

- Tinder's Move to Kubernetes

References

1. https://trends.google.com/trends/explore?date=today%205-y&q=microservice ↩
2. If you don't want to miss the article, you can subscribe to the RSS Feed, or follow me on LinkedIn or Twitter. ↩
3. Docker Compose is a good solution, Fuge is very clever, and there is also the option of running orchestration locally as is the case with something like MiniKube. ↩
4. Google Kubernetes Engine, a managed service from Google Cloud Platform for Kubernetes: https://cloud.google.com/kubernetes-engine/ ↩

5. Amazon Elastic Container Services for Kubernetes, a managed service from Amazon Web Services for Kubernetes: https://aws.amazon.com/eks/ ↩

From <https://dwmkerr.com/the-death-of-microservice-madness-in-2018/>

Data Security v0.3

Thursday, March 31, 2022 7:39 PM

Enterprise App Security Site: https://appsec.optum.com/blocking/calendar

++
++++++++

Data Security

The cost of a security threat to an information system can have a significant impact on the business.

Data security is a prevention and mitigation asset.

Data security builds trust in customer's mind for a business.
No organization can grow without customer trust and loyalty, and a healthy security posture is a cornerstone of trust.
Data security, beyond good practice and good ethics, is good business.

A recent Cisco study predicted that data security will help fuel (and protect) an estimated $5.3trillion in private sector value in the next 10 years.

Security best practices

- Protect keys, password, security certificates
- Protect data at rest
- Protect data in transit
- Secure email, documents, and sensitive data
- Enterprise grade end-to-end logging

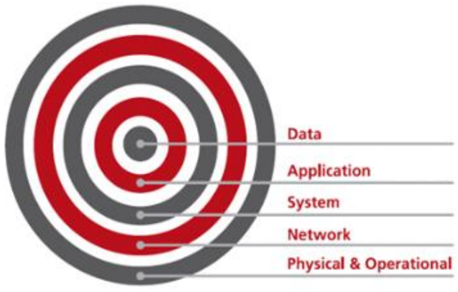
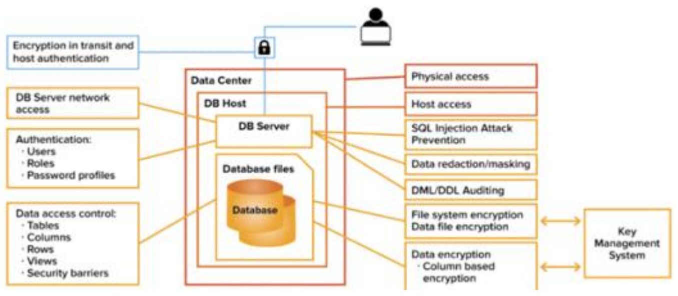
- Choose database that supports: Authentication, Authorization, Trusted Contexts, Auditing, Object Level, Row & Column Access Control, Label-Based Access Control, Encryption controls, and Dynamic Data Masking
- Utilize mature and proven technologies that support data security and data integrity

- Principle of least privilege
- Zero trust policy
- Adaptive security
- Policy based data archive and data Purge

- Physical Security
- Password Policies
- User Account Policies
- Security Incident handling

Layered Defense

Multi-layered defenses—both hardware- and software-based— work together to help protect against, avoid, repel, and withstand any threat.

Multi-level, Defense-in-Depth approach to protect against physical and electronic threats: • Physical & Operational Security • Network Security • System Security • Application Security • Data Security	 Data Application System Network Physical & Operational	 Encryption in transit and host authentication DB Server network access Authentication: · Users · Roles · Password profiles Data access control: · Tables · Columns · Rows · Views · Security barriers Data Center DB Host DB Server Database files Database Physical access Host access SQL Injection Attack Prevention Data redaction/masking DML/DDL Auditing File system encryption Data file encryption Data encryption · Column based encryption Key Management System

Specific data security aspects

Identity and Access management
- Identity Management
  - Federated Identity
  - Identity Provisioning/Deprovisioning
  - Attribute Provisioning
- Authentication services
  - Database Login
  - Azure Active Directory
  - Single Sign-on
  - MFA
  - SAML
  - Password/Key vault
  - Privileged Access Management (PAM)
- Authorization services
  - Rules Management
  - Policy Definition

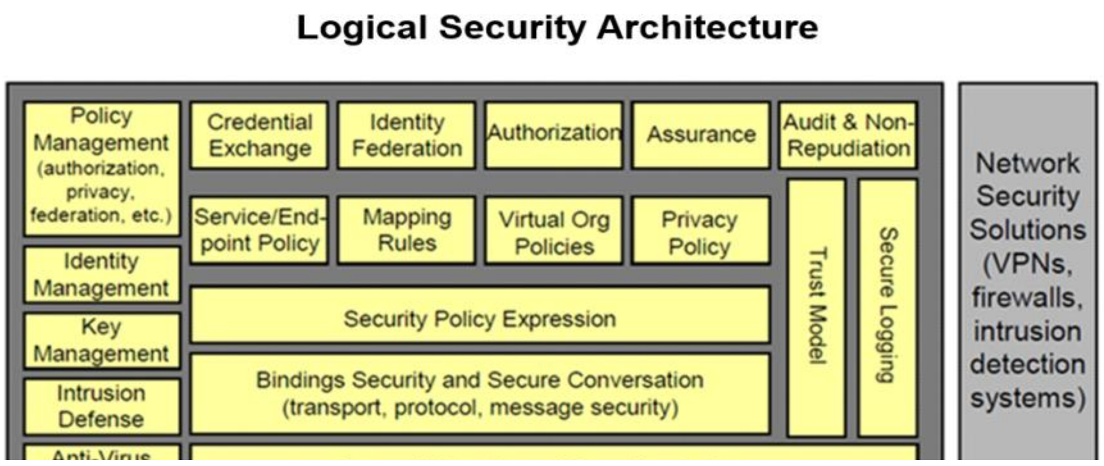
- Policy Distribution
- Policy Contract
- Policy Enforcement

InfoSec. Management
- Risk Portfolio Mgmt.
- Capability Mapping
- Risk Dashboard
- Risk Register

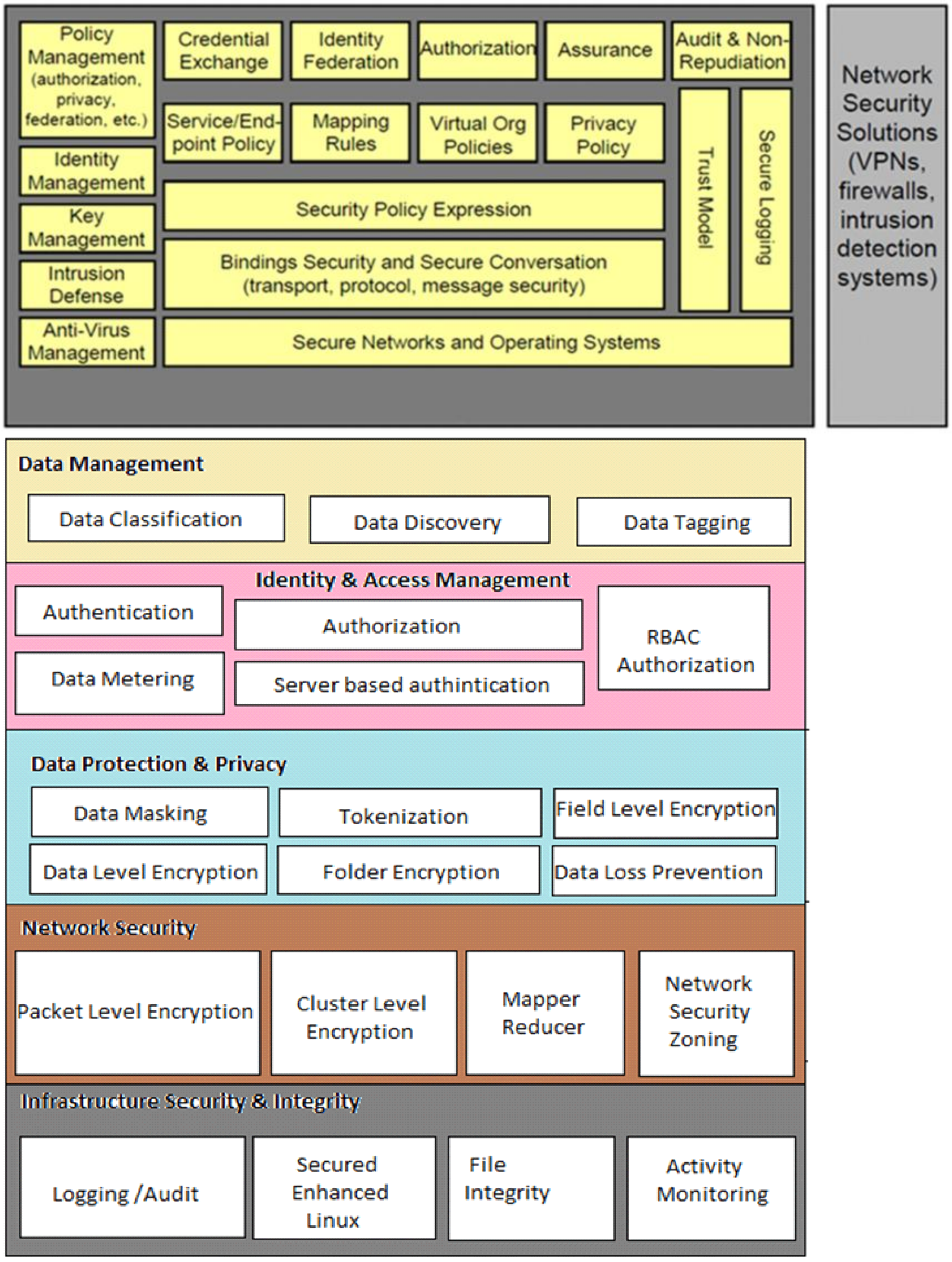
Governance, Risk & Compliance
- Compliance Mgmt.
- Training & Awareness
- Audit Mgmt.
- Policy Mgmt.

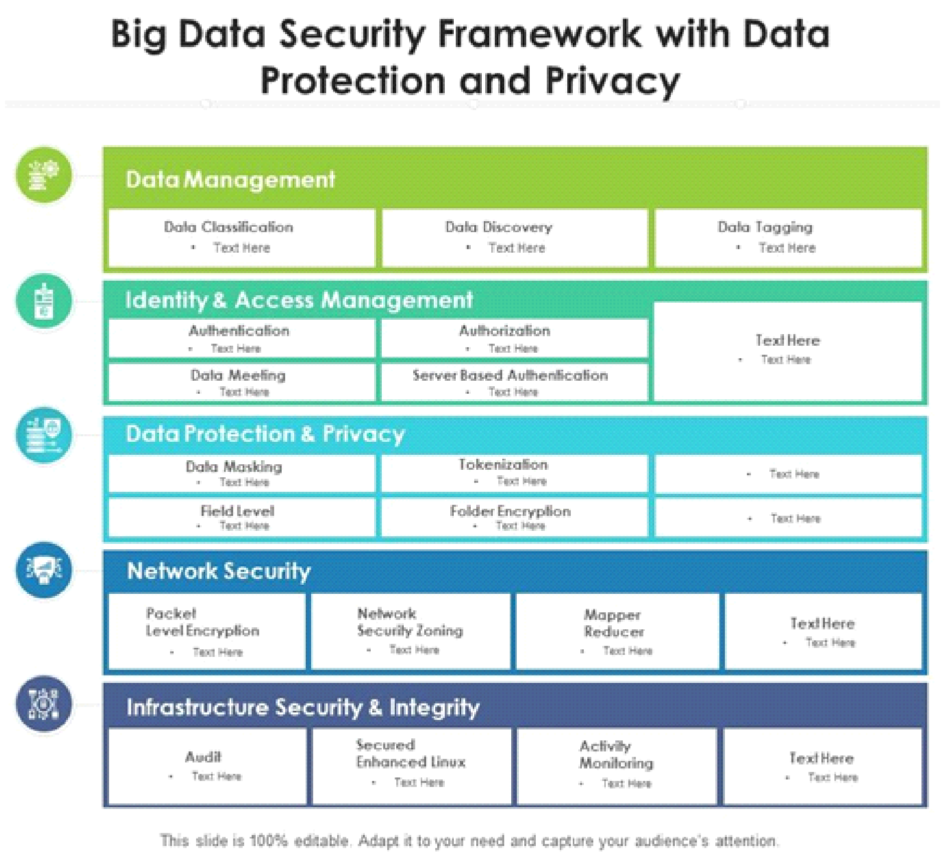
Optimize identity and access management
- Treat identity as the primary security perimeter
- Centralize identity management
- Turn on conditional access
- Enable password management
- Lower exposure of privileged accounts
- Control locations where resources are located

Data Protection
- Data Lifecycle Mgmt.
  - Data Mining
  - Data Tagging
- Data Evaluation
  - Data Loss
- Database Security
  - Database Firewall
  - Database Security
  - Authentication - users to prove their identity
  - Authorization - limit users to specific actions and data
  - Data encryption
- Enable threat protection
  - Implementing secure configurations on database
  - Detect and respond to potential threats as they occur
  - IP protection
- Data Leakage Protection (DLP)
  - Data Dictionary
  - Domain Transfer
  - Domain Use
- Data Governance
  - Data Discovery
  - Data Classification
    - Classify (categorize) stored data by sensitivity and business impact
    - Common classifications for data: Public, Private, Internal, Confidential, and Restricted
    - Organizations with weak data classification and file protection may encounter data leakage or misuse
  - Data Ownership
  - Data Label
  - Leakage Prevention Rules
  - Data Retention Rules
  - Secure Data Disposal
- Enable database auditing
  - Track and log events
  - Review for audits
  - Maintain regulatory compliance, understand database activity, find discrepancies and detect anomalies
- Logging
  - Use logging to analyze a problem in depth
  - Use logging data to trace requests, analyze usage trends, and diagnose storage account issues


Logical Security Architecture
Policy Management (authorization, privacy, federation, etc.)
Credential Exchange
Identity Federation
Authorization
Assurance
Audit & Non-Repudiation
Service/End-point Policy
Mapping Rules
Virtual Org Policies
Privacy Policy
Trust Model
Secure Logging
Identity Management
Key Management
Intrusion Defense
Security Policy Expression
Bindings Security and Secure Conversation (transport, protocol, message security)
Network Security Solutions (VPNs, firewalls, intrusion detection systems)

Logical Security Architecture





Big Data Security Framework with Data Protection and Privacy

Data Management

Data Classification	Data Discovery	Data Tagging
• Text Here	• Text Here	• Text Here

Identity & Access Management

Authentication • Text Here	Authorization • Text Here	Text Here • Text Here
Data Meeting • Text Here	Server Based Authentication • Text Here	

Data Protection & Privacy

Data Masking • Text Here	Tokenization • Text Here	• Text Here
Field Level • Text Here	Folder Encryption • Text Here	• Text Here

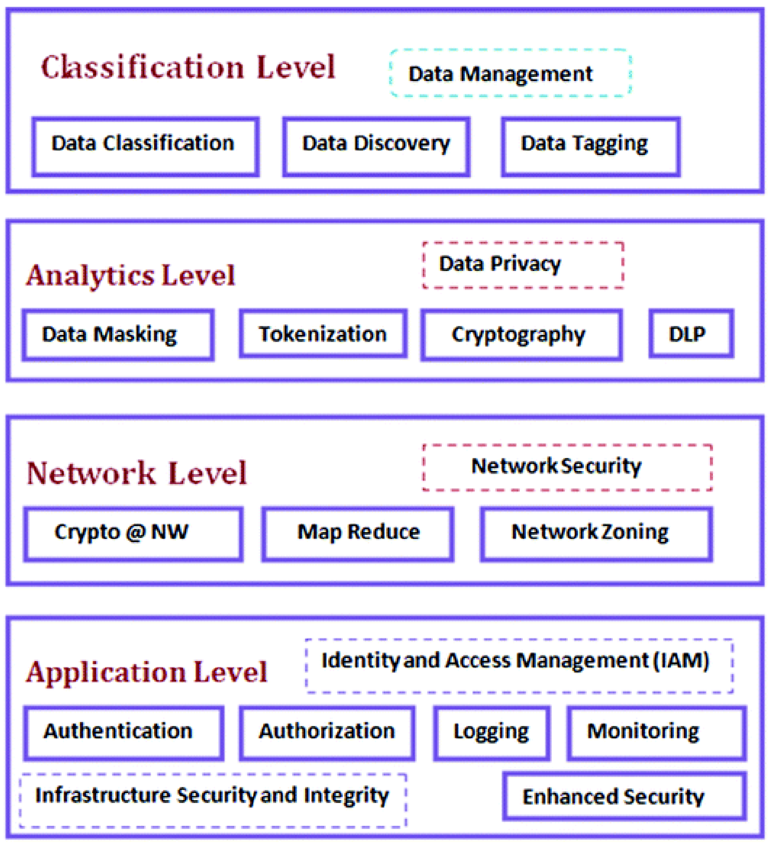
Network Security

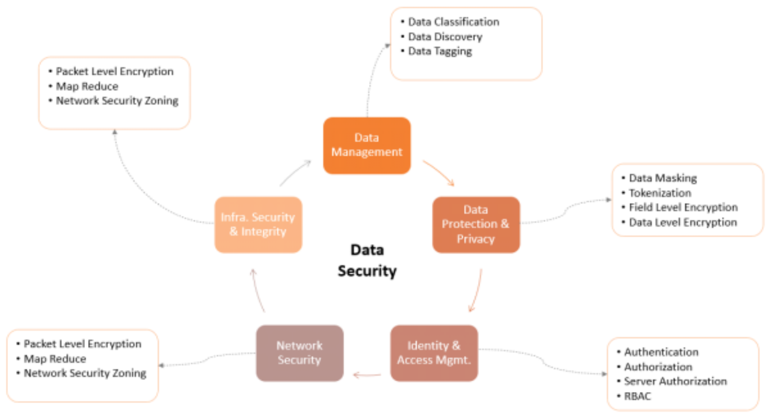
Packet Level Encryption	Network Security Zoning	Mapper Reducer	Text Here
• Text Here	• Text Here	• Text Here	• Text Here

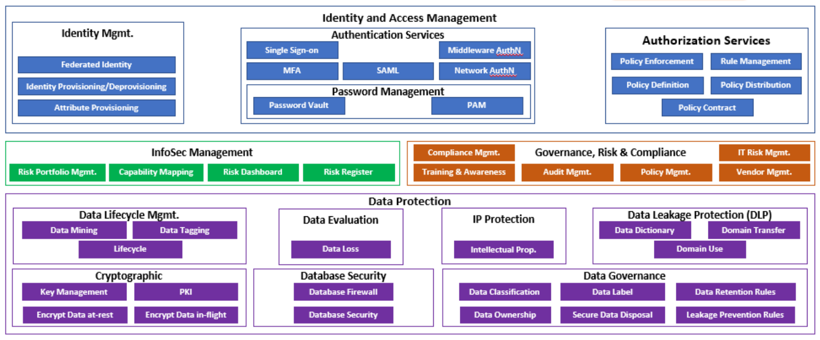
Infrastructure Security & Integrity

Audit	Secured Enhanced Linux	Activity Monitoring	Text Here
• Text Here	• Text Here	• Text Here	• Text Here

This slide is 100% editable. Adapt it to your need and capture your audience's attention.




• Data Classification
• Data Discovery
• Data Tagging
• Packet Level Encryption
• Map Reduce
• Network Security Zoning
Data Management
• Data Masking
• Tokenization
• Field Level Encryption
• Data Level Encryption
Infra. Security & Integrity
Data Protection & Privacy
Data Security
Network Security
Identity & Access Mgmt.
• Packet Level Encryption
• Map Reduce
• Network Security Zoning
• Authentication
• Authorization
• Server Authorization
• RBAC


Identity and Access Management
Identity Mgmt.
Federated Identity
Identity Provisioning/Deprovisioning
Attribute Provisioning
Authentication Services
Single Sign-on
Middleware AuthN
MFA
SAML
Network AuthN
Password Management
Password Vault
PAM
Authorization Services
Policy Enforcement
Rule Management
Policy Definition
Policy Distribution
Policy Contract
InfoSec Management
Risk Portfolio Mgmt.
Capability Mapping
Risk Dashboard
Risk Register
Compliance Mgmt.
Governance, Risk & Compliance
IT Risk Mgmt.
Training & Awareness
Audit Mgmt.
Policy Mgmt.
Vendor Mgmt.
Data Protection
Data Lifecycle Mgmt.
Data Mining
Data Tagging
Lifecycle
Data Evaluation
Data Loss
IP Protection
Intellectual Prop.
Data Leakage Protection (DLP)
Data Dictionary
Domain Transfer
Domain Use
Cryptographic
Key Management
PKI
Encrypt Data at-rest
Encrypt Data in-flight
Database Security
Database Firewall
Database Security
Data Governance
Data Classification
Data Label
Data Retention Rules
Data Ownership
Secure Data Disposal
Leakage Prevention Rules

Dinesh Feedback

Tuesday, April 5, 2022 11:10 PM

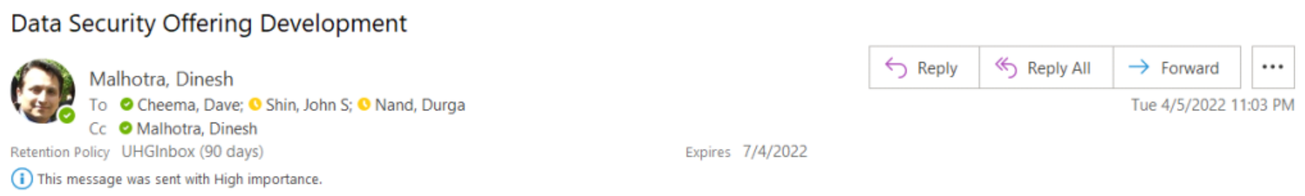
++

Dinesh Feedback:

[2:52 PM] Malhotra, Dinesh

1. Business Context to anchor why Data Security is important
2. What is Data Security
3. What is scope of overall security and how does Data Security fit in the broader context
4. What is the scope of Data Security
5. Data Security as a part of Cloud Enablement – Use Case DW Migration
6. Data Security as a part of Data Democratization (self-service enablement)
7. Data Security as a part of multi-work-load Data Management (for role based data accessibility and authorization)

++



Data Security Offering Development

Malhotra, Dinesh

To Cheema, Dave; Shin, John S; Nand, Durga

Cc Malhotra, Dinesh

Tue 4/5/2022 11:03 PM

Retention Policy UHGInbox (90 days) Expires 7/4/2022

This message was sent with High importance.

Dave – thank you once again for taking the lead in putting your thoughts to paper to help brainstorm baseline content that can be us ed to build a collateral for Data Security offering.

Team – below (scroll down) is slide of DLT GTM offerings we would like to be able to take to the market in 2022. You will notice that one of the offering is specific to Data Security Assessments / Security Architecture.

We need to build an offering to tee-up the Data Security Assessment and offer advisory services for Data Security Architecture.

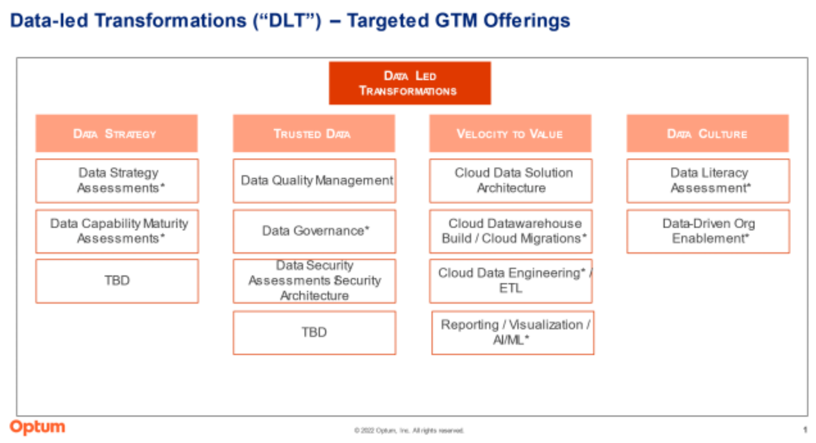
Dave / Durga– can we channelize our energies to quickly tease out how to bring this offering together? Once we have a draft offering defined, the white paper / PoV would become nice marketing collateral to help us Credentialize ourselves.

Here is my thinking for the skeleton outline for this offering – please add to the outline below to make it complete and more robust:

1. Data Security focus in healthcare – why now
    a. Business context, rapid digitalization, cloud adoption etc.
2. Top of the mind data security risks keeping C-suite awake at night – CEO, COO, CIO, CTO, CISO, CDO etc.
    a. Either word cloud or something similar
3. Data Security data points from public research
    a. McKinsey, Gartner, Accenture, PWC, E&Y etc.
4. Data Security Leading practices
    a. Richard Scott should be able to assist with this per today's convo
5. Data Security scope – visual to set the context for what all could be in scope
    a. This can be one of the visual that Dave already has pulled together
6. Optum's Data Security Service offerings
    a. Data Security Assessment
    b. Data Security Architecture
    c. *<<We need to reconcile what is on IT-PS Catalog and align our services nomenclature>>*
7. Data Security Assessment
    a. Framework with specific outputs / deliverables
    b. Highlight on "how" we do data security assessment – this should be a follow-up with Richard Scott
8. Data Security Architecture
    a. Optum's Data Security Reference Architecture with key messages

Reference Links

Data Security Services | IBM
Data protection and privacy services | EY - Global | EY - US
Cognizant—Data Security Services From Cognizant Security
Data Privacy and Protection Services | Infosys
Data Security (techmahindra.com)
Cybersecurity & Data Protection: PwC
Gartner Top Security and Risk Trends for 2021



Data-led Transformations ("DLT") – Targeted GTM Offerings

DATA LED TRANSFORMATIONS

DATA STRATEGY	TRUSTED DATA	VELOCITY TO VALUE	DATA CULTURE
Data Strategy Assessments*	Data Quality Management	Cloud Data Solution Architecture	Data Literacy Assessment*
Data Capability Maturity Assessments*	Data Governance*	Cloud Datawarehouse Build / Cloud Migrations*	Data-Driven Org Enablement*
TBD	Data Security Assessments Security Architecture	Cloud Data Engineering* / ETL	
	TBD	Reporting / Visualization / AI/ML*	

Optum

1

Best,
Dinesh Malhotra
M: +1 773-398-7713

-----Original Appointment-----
From: Malhotra, Dinesh
Sent: Tuesday, March 29, 2022 3:31 PM
To: Malhotra, Dinesh; Cheema, Dave; Shin, John S; Nand, Durga
Subject: Review Data Security PoV Outline
When: Tuesday, April 5, 2022 2:30 PM-3:00 PM (UTC-06:00) Central Time (US & Canada).
Where: Microsoft Teams Meeting

Hi Team – Dave plans to share the outline for Data and Information Security PoV.

Stay tuned!
++

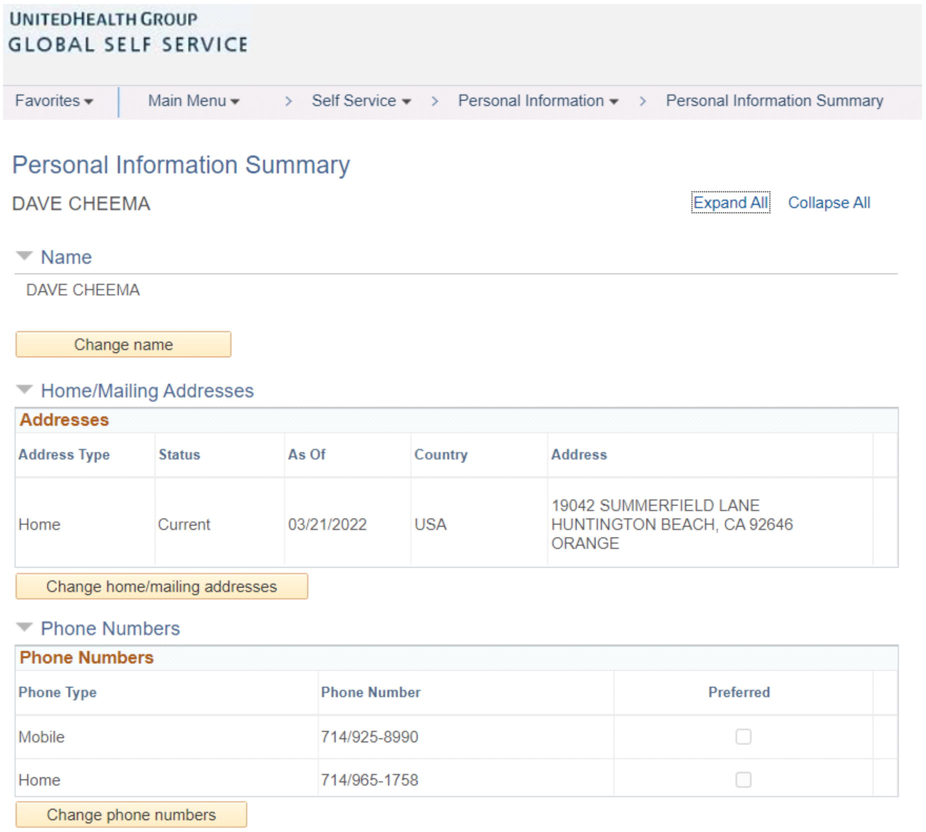
Personal Accomplishments

Saturday, April 9, 2022 3:28 PM

1. Data Security - tangible output 6-8 slides; don't forget the MBOs; make time for the practice
2. Finished all training
3. Provided input and feedback to HAP proposal, I contributed to the collateral
4. Developed Data Security practice - completed the deck; reviewed and revised based on Michael Hill's feedback. He had only one small comment about the password rotation policy
5. Engaged OAS with Yun Xu for the DataStage jobs conversion/migration. Also, provided the initial engagement
6. Interview SaikamalLesh saikamalleshsf@gmail.com
7. Worked on the SMART DW - detail out what exactly did you do
8. Reviewed resumes of Rama Rao Kavuri, Sourabh Gupta
9. Interviewed Rama Rao Kavuri
10. 04/01/2022 - Introduced David Lazar to the OAS
11. 06/22/2022 - reviewed resume of Ramana Swamy and provided feedback
12. 06/22/2022 - Met with John Lavoie on Business Development to integrate CDO into OCDP platform
13. 06/23/2022 - reviewed resumes of SRINIVASULA REDDY ATLA and conducted interview with him
14. 06/28/2022 - worked on the Geisenger EDW Opportunity - provided feedback on how to position our proposal
15. 07/01/2022 - Connected OAS practice with Data Lake data migration team. They are waiting for John Shin's bake off analysis results to be able to make a decision as to which vendor/partner for the data migration to pick.
16. Introduced Niteen Parikh to the OAS practice
17. 07/18/2022 - Dinesh cited me for being aware of the Data Lake data migration initiative and made OAS practice aware of it
18. 08/03/2022 - Made OAS aware of CDOS/COZEVA Data extract re-architect and redesign project
19. 08/05/2022 - shared the Current state documentation with John Shin so that OAS will have some context and background to start the conversation
20. 08/25/2022 - SMART DW Modernization contributed on Kafka Streaming pipeline
21. 09/15/2022 - Interviewed SATEESH KUMAR REDDY AELLA and provided feedback to HR
22. 09/22/2022 - Interviewed SAKETH RAO and provided feedback to HR
23. 08/26/2022 - John S. - Smart Modernization Proposal - Helped complete the Kafka and Streaming pipeline portion of the proposal
24. 08/31/2022 - John S. and Sansdeep Palla - Working session on SMART DW Modernization - Helped with the architecture validation
25. 09/12/2022 - John S. and Yun Xu - OCUDM Migration assumption - Helped Yun validate tools, products and vendors assumptions
26. 09/30/2022 - Sandeep Palla - OAS-SMART Modernization - ADF and KAFKA - Helped Sandeep clarify his understanding of ADF and Kafka stacks at Optum and what he'll have to do to get the infrastructure set up
27. 10/19/2022 - Sandeep Palla - SMART DW ETL Future State Architecture - Educate Sandeep on Infrastructure setup
28. 10/20/2022 - Sandeep Palla - SMART DW - Review Future State ETL Architecture
29. 10/27/2022 - Sandeep Palla - Azure ADF connectivity to On-Prem network
30. 10/30/2022 - Interviewed Robert Proffitt for the DB2 position - DB2 Technical SME Reviewed resume, conducted interview and provided my feedback to the HR team
31. 11/04/2022 - Interviewed John Marshall for the DB2 position - DB2 Technical SME - Reviewed resume, conducted interview and provided my feedback to the HR team
32. Helped recruit Nitin Parkh, Alpesh Dedhia, and John Mei
33. Made Dinesh and John S. aware of the CDO Data migration and automation opportunity
34. Shared OCDP architecture artifacts
35. Shared Data Movement and migration architecture
36. On-prem to Snowflake Data Migration architecture and PoC
37. Move on-prem SSIS package to ADF using Azure-SSIS IR
38. Developed Data Mesh practice
39. Primary interviews for the practice

++ ++++++++++++++++++++++++++
What was value delivered?
++ +++++++++++++++++++++
Need to send to Dinesh:

- Sales credit
- Open review emails
- Send Dinesh contribution summary
- Send a copy of employment letter



UNITEDHEALTH GROUP
GLOBAL SELF SERVICE

Favorites ▾ | Main Menu ▾ > Self Service ▾ > Personal Information ▾ > Personal Information Summary

Personal Information Summary

DAVE CHEEMA

Expand All Collapse All

▾ Name

DAVE CHEEMA

Change name

▾ Home/Mailing Addresses

- **Addresses**

Address Type	Status	As Of	Country	Address
Home	Current	03/21/2022	USA	19042 SUMMERFIELD LANE HUNTINGTON BEACH, CA 92646 ORANGE

Change home/mailing addresses

▾ Phone Numbers

Phone Numbers

Phone Type	Phone Number	Preferred
Mobile	714/925-8990	☐
Home	714/965-1758	☐

Change phone numbers

- Low performance counseling
- How can we build the pipeline targets

Practice

Thursday, April 21, 2022 12:40 PM

Opportunity Pipeline reports:
https://uhgazure.sharepoint.com/sites/consulting/staff/finops/SitePages/Finance%20and%20Ops%20Reporting%20View.aspx?RootFolde r=%2Fsites%2Fconsulting%2Fstaff%2Ffinops%2FPipeline%20And%20Staffing%2FFinance%20and%20Ops%20Reporting%2FPipeline&FolderCTID=0x01200065E0388411F19440932F2CC6 E552CF5E&View=%7B47FD2787-C15F-4F64-931F-FF596DC9374B%7D

Modern Data Warehouses

Friday, July 1, 2022 10:48 AM

[Modern Data Warehouse Architecture: Traditional Vs Cloud Data Warehouse | Talend]
[Modern Data Warehouse explained - James Serra]
[Enterprise data warehouse - Azure Solution Ideas | Microsoft Docs]
[Modern data warehouse for small and medium business - Azure Example Scenarios | Microsoft Docs]
[Data warehousing and analytics - Azure Architecture Center | Microsoft Docs]
Design a Modern Data Warehouse using Azure Synapse Analytics - <https://docs.microsoft.com/en-us/learn/modules/design-modern-data-warehouse-using-azure-synapse-analytics/>

Modern Data W ehouse

James Serra
Data Platform Architecture Lead
EY
jamesserra3@gmail.com
Blog: JamesSerra.com

References

Tuesday, August 16, 2022 12:22 PM

For your reference, here is link to session recording - 081622 EA Community Forum Meeting Recording.mp4

Harvester - link to presentation - 081622 EA Community Forum - HaaS - Harvester as a Service Overview.pdf

Common Review

Thursday, November 3, 2022 10:23 PM

IMPORTANT: Common Review Begins: Complete Your Self-Evaluation

Malhotra, Dinesh

Reply | Reply All | Forward | ...

To Anantha Ramakrishnan, Srinivasan; Shin, John S; Cheema, Dave; Nand, Durga; Hill, Michael O; Walinjom, Ida; Koneti, Rajesh; Siegel, David J; Hanson, Peder; Colladay, Philip; Hagglund, Robert; Tee, Vicky Hui Meng; **+5 others**

Thu 11/3/2022 5:46 PM

Retention Policy UHGInbox (90 days) Expires 2/1/2023

Internal

Team – please make this a priority to get your self-input in the MAP tool within the timelines specified

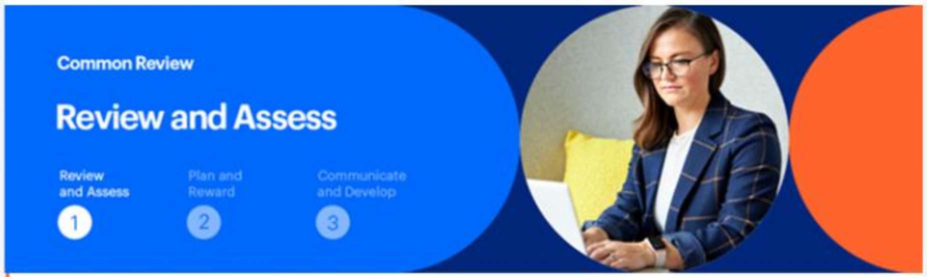
Common Review calendar link attached for your convenience

2022-2023-Common-Review-Manager-Calendar.pdf (sharepoint.com)

Best,
Dinesh Malhotra
M: +1 773-398-7713

From: Common Review <common_review@comms.uhg.com>
Sent: Thursday, November 3, 2022 2:09 PM
To: Malhotra, Dinesh <dinesh.malhotra@optum.com>
Subject: Common Review Begins: Complete Your Self-Evaluation

To view this email in a browser, click here.



It's Time to Complete Your Self-Evaluation

Common Review is your opportunity to highlight your accomplishments and the experiences that enabled you to grow and develop over the past year. Get started on your self-evaluation by taking these actions:

Confirm your self-evaluation deadline with your manager

Provide names to your manager for colleague input

Complete and submit your self-evaluation in MAP

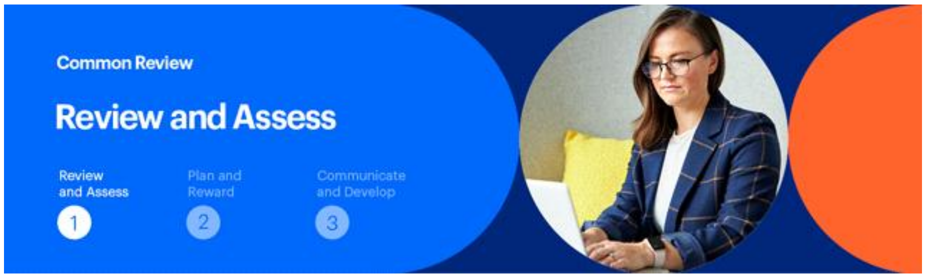
Helpful advice

- **Prioritize providing names for colleague input and completing your self-evaluations.** This is valuable information that your manager can reference when writing performance reviews.
- **Incorporate how you achieved results when describing your accomplishments.** How did you collaborate with partners outside your own team or step in to support your colleagues? How did you manage conflict? How did you influence leaders? Use Common Language of Leadership (CLL) practices to describe these actions in your self-evaluation.

- **Refer to the check-in conversations** you've had with your manager during the year and your Development Action Plan to identify progress and key areas of growth.

Resources

To view this email in a browser, click here.



It's Time to Complete Your Self-Evaluation

Common Review is your opportunity to highlight your accomplishments and the experiences that enabled you to grow and develop over the past year. Get started on your self-evaluation by taking these actions:

Confirm your self-evaluation deadline with your manager

Provide names to your manager for colleague input

Complete and submit your self-evaluation in MAP

Helpful advice

- **Prioritize providing names for colleague input and completing your self-evaluations.** This is valuable information that your manager can reference when writing performance reviews.
- **Incorporate how you achieved results when describing your accomplishments.** How did you collaborate with partners outside your own team or step in to support your colleagues? How did you manage conflict? How did you influence leaders? Use Common Language of Leadership (CLL) practices to describe these actions in your self-evaluation.
- **Refer to the check-in conversations** you've had with your manager during the year and your Development Action Plan to identify progress and key areas of growth.

Resources

Preparing for Common Review – At a Glance: Understand steps to prepare for and write your self-evaluation

MAP WorkCenter: Complete your self-evaluation

Using CLL in Common Review: Learn ways to describe how you achieved your goals in your self-evaluation

UNITEDHEALTH GROUP | Optum | UnitedHealthcare

This email was sent to all integrated employees.
Employees hired after Sept. 30, 2022, do not participate in this year's Common Review process.

Self-input for Open Review

Saturday, November 5, 2022 1:03 PM

Practice Development: could include but not limited to contributions to enhance the strength of the practice, create market visibility and credibility of the practice etc.:

1. New thought leadership / POV
    a. Provide thought leadership by writing whitepapers. For example:
        i. How to debug in live production environments conditionally
        ii. Debug Azure Function App remotely
        iii. CDOS-COZEVA Data Extract - Review and Redesign
        iv. Creating Azure Blob Storage best practices
        v. DevOps Branching Strategy and best practices
2. Lead / support offering development
    a. Developed collateral on Data Security
    b. Created PoC's on Data Movement and migration architecture:
        i. Migrate on-prem data to Snowflake using ADF and Private Link Service-Endpoint
        ii. Move data from On-prem to cloud using ADF and Self-Hosted Integration Runtime
        iii. Execute on-prem SSIS packages in Azure ADF using Azure-SSIS Runtime Integration and Self-Hosted Integration Runtime without moving the code
    c. Developed architecture collateral
        i. Streaming Data Ingestion Pipeline
        ii. OptumCare Data Platform Architecture
        iii. CareData Architecture Overview
        iv. CareData Detailed Dataflow View
        v. Curo to CareData Pipeline
        vi. Facets to Curo Data Pipeline
        vii. Facets Patient data and LDMG EMPI Integration

3. Lead / support reusable asset / accelerator development
    a. How to debug in live production environments conditionally
    b. Debug Azure Function App remotely
    c. CDOS-COZEVA Data Extract - Review and Redesign
    d. Creating Azure Blob Storage best practices
    e. DevOps Branching Strategy and best practices
    f. Developed Data Security practice

4. Publish articles in trade journals or LinkedIn / speaking at conferences

Business Development: could include but not limited to contributions to help grow the business, pipeline and sales:

1. Leads / Opportunities originated and the ones converted to sold work
2. RFP / proposals led / supported with specific role and contribution
    a. Connected DataStage Migration (Yun Xu, HCE) with OAS
    b. Provided input and feedback to HAP proposal, I contributed to the collateral - created slides for Proving Business Benefit Activities Across Migration Lifecycle
    c. Worked on the SMART DW - Timeline of Key Milestones: Reporting & ETL - defined assumptions, activities and deliverables
    d. 06/22/2022 - Met with John Lavoie on Business Development to integrate CDO into OCDP platform, connected OAS with Tracy M.
    e. 06/28/2022 - advised on the Geisenger EDW Opportunity - provided feedback on how to position our proposal
    f. 08/05/2022 - shared the Current state documentation with John Shin so that OAS will have some context and background to start the conversa tion for SMART DW
    g. 08/25/2022 - SMART DW Modernization contributed on Kafka Streaming pipeline
    h. 08/31/2022 - John S. and Sandeep Palla - Working session on SMART DW Modernization - Helped with the architecture validation
    i. 09/12/2022 - John S. and Yun Xu - OCUDM Migration assumption - Helped Yun validate tools, products and vendors assumptions
    j. 10/20/2022 - Sandeep Palla - SMART DW - Review Future State ETL Architecture
    k. 09/30/2022 - Sandeep Palla - OAS-SMART Modernization - ADF and KAFKA - Helped Sandeep clarify his understanding of ADF and Kafka stacks at Optum and what he'll have to do to get the infrastructure set up

3. New client relationships developed with commercial potential
    a. 07/01/2022 - Connected OAS practice with Data Lake data migration team. They are waiting for John Shin's bake off analysis results to be a ble to make a decision as to which vendor/partner for the data migration to pick. (**Note**: 07/18/2022 - Dinesh cited me for being aware of the Data Lake data migration initiative and made OAS practice aware of it)
    b. 08/03/2022 - Made OAS aware of CDOS/COZEVA Data extract re-architect and redesign project
    c. 08/26/2022 - John S. - Smart Modernization Proposal - Helped complete the Kafka and Streaming pipeline portion of the proposal
    d. Made Dinesh and John S. aware of the CDO Data migration and automation opportunity

4. Exploring and building vendor relationships for joint GTM potential
5. # of candidates interviewed / staffed for staffing engagements:
    a. Interview SaikamalLesh saikamalleshsf@gmail.com
    b. Reviewed resumes of Rama Rao Kavuri, Sourabh Gupta
    c. Interviewed Rama Rao Kavuri
    d. 04/01/2022 - Introduced David Lazar
    e. Helped recruit Nitin Parkh, Alpesh Dedhia, and John Mei
    f. 06/22/2022 - reviewed resume of Ramana Swamy and provided feedback
    g. 06/23/2022 - reviewed resumes of SRINIVASULA REDDY ATLA and conducted interview with him
    h. 07/11/2022 - Introduced Niteen Parikh to the OAS practice
    i. 09/15/2022 - Interviewed SATEESH KUMAR REDDY AELLA and provided feedback to HR
    j. 09/22/2022 - Interviewed SAKETH RAO and provided feedback to HR
    k. 10/30/2022 - Interviewed Robert Proffitt for the DB2 position - DB2 Technical SME Reviewed resume, conducted interview and provided my feedback to the HR team
    l. 11/04/2022 - Interviewed John Marshall for the DB2 position - DB2 Technical SME - Reviewed resume, conducted interview and provided my feedback to the HR team

People Development: could include but not limited to contributions to help grow our people and yourself:

1. # of individuals mentored / coached
    a. Sandeep Palla - helped him -
        i. familiarize with the Optum environment
        ii. how and who will setup Kafka
        iii. Azure ADF
        iv. Create and configure storage accounts

        v. on-prem and Azure connectivity

2. Training programs developed / supported
    a. Completed all my OAS, OCDP, Optum, and Healthcare Fundamentals training
3. Brown bags conducted to share your personal knowledge with broader audience
    a. Clearly communicated to the team that I'm always available wherever and whenever I could be of any help
    b. Share knowledge willingly and openly
4. Create a brand for self to become the 'go to' person for specific opportunities/ domains
    a. Go to person for the Azure cloud, Azure Data Factory, Databricks, and enterprise architecture
5. New trainings / certifications accomplished
    a. In addition to completing all required training, I also completed Leadership training, and Healthcare Fundamentals

Organizational Culture: could include but not limited to:

1. Total hours invested in charities and social causes - UHG-sponsored or otherwise
    a. Donated money to Farmers protests in New Delhi - $250
    b. Donated money to Pakistan Flood Relief Fund - $500
2. Living the culture - demonstrated examples of living our core values and culture values
    a. I demonstrated by donating money to people in sufferings and hardships that I care about humanity and help out whenever and w herever possible

++
Sales and Utilization will be provided by HR - I know you are doing good on Utilization.

Going forward, as we plan and prepare for 2023, I would like to understand how you can strike a good balance between your expected Utilization (75%) and the allocation of remaining 25% of time to help grow the business and practice.

Thank you for your great work in 2022 and look forward to partnering with you to build our plans for a better 2023.

Sales Training

Monday, November 7, 2022 12:26 PM

[Watch the replay now]

Dinesh's ask

Thursday, December 15, 2022 1:00 PM

Put together simple documents

- Don't lose track of them
- Put together one pagers
- blind spots
- what can be done to qualify the opportunity