Enterprise Architecture

Georgia-Pacific Application Architecture Standards and Guidelines

GP IT Enterprise Architecture

June 2021

Application Decision Guidelines

- ERP
  - If it is a segment or capability specific need and your ERP already has the functionality you need without significant gaps you should look there first
  - If an ERP module enables it, are we licensed to use it and, if not, what is the licensing cost? If not, is it on the roadmap and you wait?
  - Why would you not use your ERP?
    - Missing required or highly valued functionality
    - Not licensed for the functionality or module and the cost is prohibitive
    - Other alternatives are superior to the ERP offering
    - You need the ability to bake in custom, value added, functionality that would be difficult to enable with the ERP
    - The application needs to be used more broadly across GP and/or Koch than the group using the ERP

Application Decision Guidelines

- SaaS
  - Usually the most cost-effective option, but not always, so be highly aware of licensing model related to usage patterns
  - For non-differentiating applications where the market is mature
  - Why not SaaS?: If there is a SaaS product available, think about why hosting or developing your own would add value
    - Think 80/20 – is that extra 20% (usually less) worth the additional effort and cost of developing and supporting your own application
    - Can the application integrate with our existing applications and identity provider (KochID/PingID)?
      - If not, do they have an on-premise version of the product that allows for that?
    - Many SaaS products now have a PaaS layer that allows you to customize around the core application to fill gaps

Application Decision Guidelines

- 3rd Party internally hosted
  - Often similar in pricing to SaaS but higher TCO due to use of internal infrastructure and IT resources
  - Good choice when there are no SaaS alternatives that meet our needs, but we don't require something custom
  - Must consider internal infrastructure standards like OS (Windows, RHEL, Amazon Linux), identity, authentication and authorization (KochID), and security standards
    - Can our security, monitoring, and logging tools run on their servers/containers?
- Custom
  - If there is no viable SaaS or other 3rd Party alternative that meets your requirements
  - If the software logic requires GP/Koch IP to support an advantaged capability
  - If you need to be highly agile and release frequent enhancements and features
  - If the TCO of a custom application will be cheaper than market alternatives
  - If integration requirements with existing apps and ERPs will be difficult with 3rd party options

Identity and Access Management

- Custom apps
  - Integrate KOCHID into your application for internal employee access.
  - If a custom app is internet facing and there is a requirement for external users to access the application, integration with an external IDP is allowed if it meets the GP Cyber Security Identity and Access Management Standard.
- 3rd party apps
  - Verify they can utilize KOCHID or integrate it with their provider
- For questions or more information please visit https://kochid.com/ or reach out to the KGS AIS Team

Cloud Platforms

- Amazon Web Services is our primary cloud platform for custom and 3rd party hosted IaaS, serverless, and PaaS solutions
  - IaaS should only be implemented in AWS. There is little differentiation in running VMs or containers on another platform.
  - Koch.link/aws
- Microsoft Azure is our secondary cloud platform alternative for serverless and PaaS
  - Azure should only be an option if AWS does not have a service that meets your needs or there is a capability within Azure that we believe adds significant value vs AWS (not just incremental)
  - portal.azure.com
- ERP and SaaS provider PaaS offerings may be used for work specific to those applications (e.g. SAP Cloud Platform)
  - Although these platforms typically have the capability to run non-platform related applications, that should not be done in our environment
- For questions or more information reach out to Enterprise Architecture or GP Cloud Optimization

Cloud Compute

- New Internal & Vendor Applications must leverage any combination of:
  - Containers
  - Serverless compute
  - Platform as a Service (PaaS)
- Considerations:
  - Containers are the most portable option
    - Enables deployments that span Cloud to Edge
  - Serverless generally has the lowest cost
  - PaaS generally has the lowest maintenance
- For questions or more information reach out to Enterprise Architecture

Cloud Optimization

- Koch Ind. has negotiated our Enterprise Discount Plan (EDP) with AWS, making AWS our go to cloud platform.
  - EDP ~ 30% off all major services
- Koch has purchased Savings Plans 3 years no up front for compute resources (EC2, Lambda, Fargate) and SageMaker.
- For RDS and Redshift RIs purchases, please reach out to Carlos Wiley.
  - These are managed at the Koch level and not at the account level.
- Cloudability is GP's source of truth for cloud costs. Access is granted here. You can log in at Koch.link/cloudability.
- Cloudability has rightsizing recommendations for EC2 instances, EC2 ASG, EBS, S3, RDS, Redshift, and Container Workloads.
  - For an optimization consultation please enter a ticket here
- Cloud Optimization Tech Fluency
  - Here you will learn about Cost Optimization Design Patterns and Cloudability "how to"
- Cost allocation standard tags are here
- The org, segment, application, and cost center composite key reference can be found here.
  - For new segment requests, please reach out to Carlos Wiley here

Edge Compute

- New onsite applications should
  - Mirror Cloud Compute Standards
  - Follow DevOps standards
- Data transfer should leverage Pub/Sub model
  - Utilize MQTT & follow Enterprise Standard
  - Extremely large (50GB+) transfers may utilize HTTP
- KOCHedge is the target platform for new deployments
  - Built-in MQTT Network
  - Container-centric deployments
  - Automated Management
- For questions or more information reach out to Enterprise Architecture

Edge Compute Deployments

- Use VMs before Industrial Edge Devices
- Edge Compute Must:
  - Connect to network via the Edge DMZ (Purdue Layer 3.5)
  - Be a standard Hardware Offering
  - Leverage KOCHedge OS (preinstalled)
  - Be managed via Canopy
- Non-Compute Hardware (sensors, radios, etc…) can only connect to the internal network at the Edge DMZ (Purdue Layer 3.5) or below (ie. PCN Network).
  - Alternatively, it may connect directly to an edge device
- For questions or more information reach out to Enterprise Architecture

Containers

- Container images must conform to OCI standards
- Container deployments must utilize industry standards toolset:
  - Kubernetes
  - AWS ECS
- Container images must be stored in a central registry:
  - Jfrog **Pending Deploy & Supporting Services*
- Container lifecycle must follow DevOps, Security, and other enterprise standards
  - GP Cyber Security POV: Container Vulnerabilities
- Shared clusters must use Cloudability's YAML file for cost allocation labels
  - Reach out to the Cloud Optimization Team for more details on how to create your own specific YAML for your application

Mobile

- Application Decision Guidelines
  - When considering 3rd party solutions for internal use consider the following before choosing custom development:
    - Citizen Development Platforms
    - Connected Worker Platforms
    - Rapid Applications Development Platforms (e.g., OutSystems)
- Development
  - Mobile applications should follow all other guidelines and standards in this document
  - Mobile applications should not require a GP network connections to work, but instead connect via the internet
- Manufacturing
  - Please review the following if deploying/developing mobile solutions for manufacturing users:
    - OpsConnect Manufacturing Mobile App Standards
    - OpsConnect Mobile Device Information
- Please review the Mobile Device Policies & Guidelines to ensure your use case meets the guidelines

Databases

- For custom developed applications requiring a relational database our standard is AWS RDS Aurora (MySQL or Postgres)
- For custom developed applications requiring NoSQL our standard is Amazon DynamoDB
- Edge applications or those hosted in Azure or ERP clouds will require different options
  - Reach out to the ERP team, Database Services Team, or Enterprise Architecture for guidance
- For 3rd party application databases that require SQL Server, Oracle, and other non-Aurora offerings, use Amazon RDS instead of IaaS when at all possible
  - Certain licensing or functionality restrictions may make IaaS necessary. Talk to Database Services and Enterprise Architecture to vet exceptions
- There is growing momentum around alternatives to traditional SQL and NoSQL databases and guidance will be published as standards come into place
  - Examples are time series databases, graph databases, and distributed ledger databases'
  - Please reach out to Enterprise Architecture, Database Services, and/or the Enterprise Data and Analytics team if you have a need for an alternative database
- For questions or more information please reach out to Enterprise Architecture or Database Services

Integration and APIs

- API Standards
  - Expose application data and interfaces through RESTful APIs
  - Design your integrations so that your application is decoupled from interfacing applications
  - Keep re-use in mind both within your organization and across GP when designing new APIs and integrations
  - All APIs, regardless of where developed, should be cataloged in MuleSoft
- When choosing 3rd party applications, APIs available for required GP interfaces should be part of the evaluation criteria
- For questions or more information reach out to Enterprise Architecture or Integration Platform Services
- Best practices for securing APIs
- Standards for integrating files from Manufacturing Facilities to AWS - Continuous File Based Integration Standards
- Event Broker user guide

Integration Tool Standards

Attributes	Technologies				
	Enterprise	BP	CPG	MFG (CSC)	PKG
API Management/Governance	AWS API Gateway Mulesoft	AWS API Gateway Mulesoft	SAP Gateway SAP Cloud Connector	AWS API Gateway Mulesoft	AWS API Gateway Mulesoft
Broker/Queue	AWS EventBridge AWS SQS	AWS EventBridge	AWS EventBridge	AWS EventBridge AWS SQS	AWS EventBridge
EDI/B2B	Axway Sterling	Axway Sterling	Axway Sterling	Axway Sterling	Axway Sterling
ETL/ELT/Big Data	AWS Glue Talend	AWS Glue	SAP DS SCP-DS	AWS Glue	AWS Glue
Replication	Mimix		SAP SLT		Clik Replicate
Streaming	AWS Kinesis AWS MKS	AWS Kinesis AWS MKS	AWS Kinesis AWS MKS	AWS Kinesis AWS MKS Ignition Kepware VerneMQ AWS IoT Core	AWS Kinesis AWS MKS
Transactional	Mulesoft Sterling	Infor ION Mulesoft Sterling	SAP PO SCP-CPI	Mulesoft	Infor ION Mulesoft Sterling
Virtualization	Denodo	Denodo	Denodo	Denodo	Denodo

Testing and Quality

- Test driven development – define test scenarios and code to pass those tests
- Automate testing as much as possible
  - Mitigates risk of breaking existing functionality
  - More accurate and faster than humans; Increase speed of delivery
  - Opportunity to save a lot of time and money spent on manual testing and use those resources elsewhere
- Tooling and standards
  - KGSI Quality Engineering provides a variety of tools and services to meet your testing and quality needs for various use cases. KGSI QE will provide best practices when it comes to standards for all of Koch Industries
- For questions and more information reach out to Enterprise Architecture

Logging

- Aggregate logs across your workload/application using Splunk
  - Koch Splunk
  - Learn about Splunk
  - Learn how to use Koch's Splunk with your app
  - Ask GP Integration Services about existing logging APIs
- For questions or more information reach out to Enterprise Architecture

Security - Encryption

- Enable encryption wherever possible and whenever possible
  - For most PaaS and SaaS solutions encryption is just a check box
  - Performance overhead is minimal in most modern applications
  - Encrypt confidential data at rest.
  - Encrypt all data in transport.
  - If a 3rd party solution does not support end-to-end encryption, we need to look at alternatives
  - If there is a blocker to encryption reach out to GP Cybersecurity Engineering

Security – Secrets Management

Provisional Standard - deployment pending

- HashiCorp Vault is our standard secrets management platform
  - Use Vault to store passwords, keys, and other secrets
  - Use Vault to rotate your keys when possible
  - AWS Secrets Manger and KMS may be approved for niche cases – must discuss with GP Cybersecurity and/or Enterprise Architecture
  - vaultproject.io/
  - Learn Vault
- For questions or more information reach out to Enterprise Architecture, GP Cybersecurity Engineering, or GP Cloud Optimization

Disaster Recovery and HA

Minimum Expectations	Tier 1	Tier 2	Tier 3
RTO	Up to 24 Hours	Up to 7 days	Up to 30 days
RPO	< 4 hours	< 4 hours	< 24 hours
Min # AZ	2 (or more)	2 (or more)	1 (or more)
Capacity Reservation	Required	Required	Optional
Replication Technology	Cloud Endure	Cloud Endure	Optional
Backup Technology	CPM	CPM	CPM

Disaster Recovery and HA

AWS Services	Tier 1	Tier 2	Tier 3
S3	Multi-AZ and Versioning	Multi-AZ and Versioning	Versioning
Lambda	Multi-AZ and backups	Multi-AZ and backups	Backups
RDS	Multi-AZ and backups	Multi-AZ and backups	Backups
API Gateway	Multi-AZ and backups	Multi-AZ and backups	Backups

- All other AWS Services will need to have Multi-AZ and backups enabled for Tier 1 and 2 applications.
- DR testing is required at a minimum yearly cadence for Tier 1. For Tier 2 and Tier 3 a yearly tabletop is required.
- A DR plan is required for all Tier 1 and Tier 2 applications and must be published on the GP DR SharePoint
- For additional DR information click here.

Links to Domain Specific Standards

- Koch Cloud
- GP Mobility
- Mulesoft Standards – TBD
- Koch Edge Standards – TBD
- Security
  - GP Cyber Security Sharepoint
  - GTE – Koch enterprise tool for assessing compliance and security risk.
    - High Level Workflow
    - GTE Yammer
  - Web Application Security Program
    - Web Application Security Program Overview
      - **Security ScoreCard** – Used to report on security vulnerabilities in SAAS providers. By going through GTE process vendor will be scanned.
      - **Netsparker** – for scanning custom externally facing web applications.
    - Web Application Security Documentation

DevSecOps

- HashiCorp Terraform is our standard for infrastructure as code
  - IaC POV
  - Terraform – Tech Fluency Track
  - GP Infrastructure as Code Consulting Compass Form
- The expectation is that you script out your infrastructure using Terraform and automate the creation of additional environments
- At minimum, separate development, QA/test, and production environments are required
- No development work, including bug fixes, should be done outside of the development environment
- Application and infrastructure code will be moved to post development environments using automated CI/CD pipelines
- For questions or more information reach out to Enterprise Architecture or GP Cloud Optimization

DevSecOps

- Use automated CI/CD pipelines to integrate and deploy your code.
- Environments above Development should be locked down from changes being made outside the CI/CD pipeline.
- GitLab/KochSource is our standard source code repository and CI/CD platform
    - Kochsource
    - Learn GitLab
- Azure DevOps is acceptable for teams already using it, but the same level of GP enterprise and KBS support will not be available
    - KGS and GP Cloud Optimization will provide updates, enhance GitLab functionality, and provide operational support
- For questions or more information reach out to Enterprise Architecture or GP Cloud Optimization

Change Log

Modifications	Author	Date
Created one slide to cover Cloud Optimization. Updated containers slide to include the labeling strategy for container labels with shared clusters, also updated the link to Koch.link/aws in the cloud platforms slide.	Laila Majidi	6/2/2022
Created two slides to cover DevSecOps, encompassing Environments/IaC/Deployment Source Control, removed slides for those topics.	Carlos Wiley	6/24/2021
Added link to best practices for securing APIs to Integrations	Ryan Hopf	6/24/2021
Slide 21 (Domain Specific Links) added GTE Link, security scorecard, RSAM and Netsparker info	Ryan Hopf	6/24/21
Updated Integration Tools Standards	Brian Dobash	7/7/2021
Updated Mobile Slide to reference Compliance Mobile Device Policies & Guidelines	Angie Pappas	9/2/2021
Updated Integration and APIs to reference Continuous File Based Integration Standards	Dave Nettuno	9/2/2021
Updated encryption section to reflect current standards. Updated Security section to detail what tools are used when and updated links to other info.	Ryan Hopf	9/15/2021
Update to testing & quality section tools and standards to work with Koch Global Services Quality Engineering	Brian Dobash	12/16/2021
Add API standards reference, remove reference to old API naming standards	Ryan Filpi	2/28/2023