IE Cheatsheet - MAP2

June 2, 2025

Contents

1 Containers & Cloud

1.1 Cloud services properties

- Broadband access - Consume the services from anywhere
- On-demand self-service - Consume the services when you want
- Resource pooling and virtualization - Pool the infrastructure, virtual platforms and applications
- Rapid elasticity - Pooled resources with horizontal scalability
- Measured service - Pay only for what you consume when you consume

1.2 Cloud services

1.2.1 PaaS

A cloud computing model that provides a ready-to-use development and deployment environment. It includes infrastructure (servers, storage, networking) and platform tools (databases, runtime, development frameworks), allowing developers to build and run applications without managing the underlying hardware or software layers. An example is Azure.

1.2.2 SaaS

A cloud delivery model where users access fully functional software applications over the internet. The provider manages everything (infrastructure, platform, and software), and users typically interact through a web browser. An example is Youtube.

1.2.3 IaaS

A cloud computing model that provides virtualized computing resources (servers, storage, networking) over the internet. Users manage the OS, middleware, and applications, while the provider handles the infrastructure. An example is AWS.

1.2.4 FaaS

A Serverless computing platform where the unit of computation is a function that is executed in response to triggers such as events or HTTP requests. The cloud provider handles the infrastructure, scaling, and execution, charging only for actual usage time. Examples are Cloudflare workers, AWS Lambdas

1.2.5 IaC

A DevOps practice where infrastructure (servers, networks, etc.) is provisioned and managed using code and automation rather than manual processes. This enables version control, testing, and consistent environments. An example is Terraform.

1.2.6 Cloud styles

Clouds may be hosted and employed in different styles depending on the use case, respectively the business model of the provider: **Private cloud** (A cloud environment dedicated to a single organization, hosted either on-premises or by a third party. Used for enhanced security and control over data.); **Community cloud** (A cloud infrastructure shared by several organizations with common concerns, such as security or compliance. Ideal for groups with similar needs, like government agencies or healthcare institutions.); **Public cloud** (A cloud service offered by third-party providers over the internet and shared among multiple customers. Cost-effective and scalable, but less control over infrastructure.); **Hybrid cloud** (A combination of two or more cloud types (private, public, or community) that remain distinct but are integrated. Flexible approach that balances security and scalability.); **Special purpose clouds** (Clouds designed for specific tasks or industries, such as high-performance computing or scientific simulations. Optimized for niche or specialized workloads.).

1.3 Physical Servers

Slow-iteration and slow-deployment. Single tenancy. Unfriendly for friendly for multi programming languages. Deploy in weeks. Typically, alive for years.

1.4 Virtual Machines

VMs work by operating on top of a hypervisor, which is stacked on top of a host machine. A VM monitor (VMM) or hypervisor intermediates between the host and guest VM. By isolating individual guest VMs from each other, the VMM enables a host to support multiple guests running different OSes. Each VM carries their own virtualized hardware stack

that comprises network adapters, storage, applications, binaries, libraries and its own CPU. **Advantages:** VMs allow to consolidate applications onto a single server, Faster-iteration and deployment, Multi-tenancy, Somewhat friendly for multi programming languages, Deploy in minutes, Typically, alive for weeks. **Disadvantages:** Having multiple VMs with their owned OS adds substantial overheads in terms of RAM, CPU, I/O and storage.

1.5 Containers

A container is a self-contained execution environment that shares the kernel of the host system and which is (optionally) isolated from other containers in the system. One of the major advantages of containers is resource efficiency, because you don't need a whole operating system instance for each isolated workload. When a process is running inside a container, there is only a little bit of code that sits inside the kernel managing the container. Contrast this with a virtual machine where there would be a second layer running. In a VM, calls by the process to the hardware or hypervisor would require bouncing in and out of privileged mode on the processor twice, thereby noticeably slowing down many calls.
Containers are an abstraction at the app layer that packages code and dependencies together. Multiple containers can run on the same machine and share the OS kernel with other containers, each running as isolated processes in user space. Containers take up less space than VMs (container images are typically tens of MBs in size), can handle more applications and require fewer VMs and Operating systems. **Advantage**: more lightweight than VM's

1.5.1 Docker image

An image is a read-only template with instructions for creating a Docker container. Often, an image is based on another image, with some additional customization. For example, you may build an image which is based on the ubuntu image, but installs the Apache web server and your application, as well as the configuration details needed to make your application run. You might create your own images or you might only use those created by others and published in a registry. To build your own image, you create a Dockerfile with a simple syntax for defining the steps needed to create the image and run it. Each instruction in a Dockerfile creates a layer in the image. When you change the Dockerfile and rebuild the image, only those layers which have changed are rebuilt. This is part of what makes images so lightweight, small, and fast, when compared to other virtualization technologies.

1.5.2 Docker container

A container is a runnable instance of an image. You can create, start, stop, move, or delete a container using the Docker API or CLI. You can connect a container to one or more networks, attach storage to it, or even create a new image based on its current state. By default, a container is relatively well isolated from other containers and its host machine. You can control how isolated a container's network, storage, or other underlying subsystems are from other containers or from the host machine. A container is defined by its image as well as any configuration options you provide to it when you create or start it. When a container is removed, any changes to its state that are not stored in persistent storage disappear.

1.5.3 Docker Hub

It is a service provided by Docker for finding and sharing container images with others. It's the world's largest repository of container images with an array of content sources including container community developers, open source projects and independent software vendors (ISV) building and distributing their code in containers.
Docker Hub provides the following major features:

- **Repositories:** Push and pull container images.
- **Teams & Organizations:** Manage access to private repositories of container images.
- **Docker Official Images:** Pull and use high-quality container images provided by Docker.
- **Docker Verified Publisher Images:** Pull and use high-quality container images provided by external vendors.
- **Docker-Sponsored Open Source Images:** Pull and use high-quality container images from non-commercial open source projects.
- **Builds:** Automatically build container images from GitHub and Bitbucket and push them to Docker Hub.
- **Webhooks:** Trigger actions after a successful push to a repository to integrate Docker Hub with other services.

1.5.4 Docker compose

It is a tool for defining and running multi-container Docker applications. A YAML file is used to configure the application's services. Then, with a command, you create and start all the services from your configuration. Compose works in all environments: production, staging, development, testing, as well as CI workflows. It also has commands for managing the whole lifecycle of applications:
• Start, stop, and rebuild services
• View the status of running services
• Stream the log output of running services
• Run a one-off command on a service

1.6 Kubernetes

It is an open source orchestrator for deploying, scaling, and management of containerized applications (different from terraform which is applicable to any cloud resource). It allows to run Docker containers and workloads and helps tackling some of the operating complexities when moving to scale multiple containers, deployed across multiple servers.

- The service delivery velocity founded on
  - **Immutability:** rather than incremental updates and changes, an entirely new, complete image is built, where the update simply replaces the entire image with the newer image in a single operation.
  - **Declarative configuration:** describing the state of the desired world, instead of specifying the series of instructions.
  - **Online self-healing systems:** e.g., if you assert a desired state of 3 replicas, Kubernetes creates exactly 3 replicas. If a fourth is manually created, Kubernetes destroys it.
- Scaling (software and teams)
  - Decoupling
  - Clusters
  - Microservices
  - Separation of concerns
- Abstracting the infrastructure
- Resource efficiency usage

1.6.1 Kubernetes Architecture

A **node** is a machine where containers (workloads) are deployed. Every node in the cluster must run a container runtime such as Docker, as well as the below-mentioned components, for communication with the primary for network configuration of these containers. A **Kubelet** is responsible for the running state of each node, ensuring that all containers on the node are healthy. It takes care of starting, stopping, and maintaining application containers organized into pods as directed by the control plane. A **Kube-proxy** is an implementation of a network proxy and a load balancer, and it supports the service abstraction along with other networking operation. It is responsible for routing traffic to the appropriate container based on IP and port number of the incoming request.

1.6.2 Kubernetes Pods

A Pod represents a collection of application containers and volumes running in the same execution environment. A Pod is the smallest deployable artifact in a Kuberneted cluster. All of the containers in a Pod always land on the same machine. Applications running in the same Pod share the same IP address and port space (network namespace), have the same hostname, and can communicate using native interprocess ccommunication channels. On the opposite, applications in different Pods are isolated from each other; they have different IP addresses, different hostnames,... Containers in different Pods running on the same node might as well be on different servers. In general, "Will these containers work correctly if they land on different machines?"
No - use a Pod to group the containers
Yes - use multiple Pods

1.7 Terraform (IaC)

Terraform is a solution to create cloud environments using code instead of using the cloud providers User Interfaces. Therefore, the management of the cloud resources takes less effort and the creation, or update, process is faster. Terraform state can be shared through cloud environments like S3 buckets in AWS. For example, I can have 2 different terraform projects that use the same bucket, meaning I could get the hostnames of machines in other projects.

1.8 Serverless Computing

Serverless computing is a platform that hides server usage from developers and runs code on-demand automatically scaled and billed only for the time the code is running. Cloud Native Computing Foundation (CNCF) defines serverless computing as "the concept of building and running applications that do not require server management. It describes a finer grained deployment model where applications, bundled as one or more functions, are uploaded to a platform and then executed, scaled, and billed in response to the exact demand needed at the moment." **Serverless essential qualities:**

1. Providing an abstraction that hides the servers and the complexity of programming and operating them.
2. Offering a pay-as-you-go cost model instead of a reservation-based model, so there is no charge for idle resources.
3. Elasticity - automatic, rapid, and unlimited scaling resources up and down to match demand closely, from zero to practically infinite.

1.8.1 AWS Lambda Functions

- **Function**: is a resource that you can invoke to run your code in AWS Lambda. A function has code that processes events, and a runtime that passes requests and responses between Lambda and the function code. You provide the code, and you can use the provided runtimes or create your own.
- **Runtime**: Lambda runtimes allow functions in different languages to run in the same base execution environment. You configure your function to use a runtime that matches your programming language. The runtime sits in between the Lambda service and your function code, relaying invocation events, context information, and responses between the two. You can use runtimes provided by Lambda or build your own.
- **Event**: is a JSON formatted document that contains data for a function to process. The Lambda runtime converts the event to an object and passes it to your function code. When you invoke a function, you determine the structure and contents of the event. When an AWS service invokes your function, the service defines the event.
- **Concurrency**: is the number of requests that your function is serving at any given time. When your function is invoked, Lambda provisions an instance of it to process the event. When the function code finishes running, it can handle another request. If the function is invoked again while a request is still being processed, another instance is provisioned, increasing the function's concurrency.
- **Trigger**: is a resource or configuration that invokes a Lambda function. This includes AWS services that can be configured to invoke a function, applications that you develop, and event source mappings. An event source mapping is a resource in Lambda that reads items from a stream or queue and invokes a function.

1.8.2 Serverless Drawbacks

Not suitable in terms of cost and execution platform for long-running processes. Vendor lock-in (becoming heavily dependent on a specific cloud provider's proprietary services and technologies, making it difficult and expensive to switch to a different provider later). Cold starts can cause an overhead that is unacceptable on low-latency applications. Monitoring and debugging is more complex when compared with other architectures.

2 Business Process Management

Business Process Management (BPM) is a method for analyzing, improving, and automating business processes to make them more efficient and effective. It helps organizations streamline operations and adapt to change.

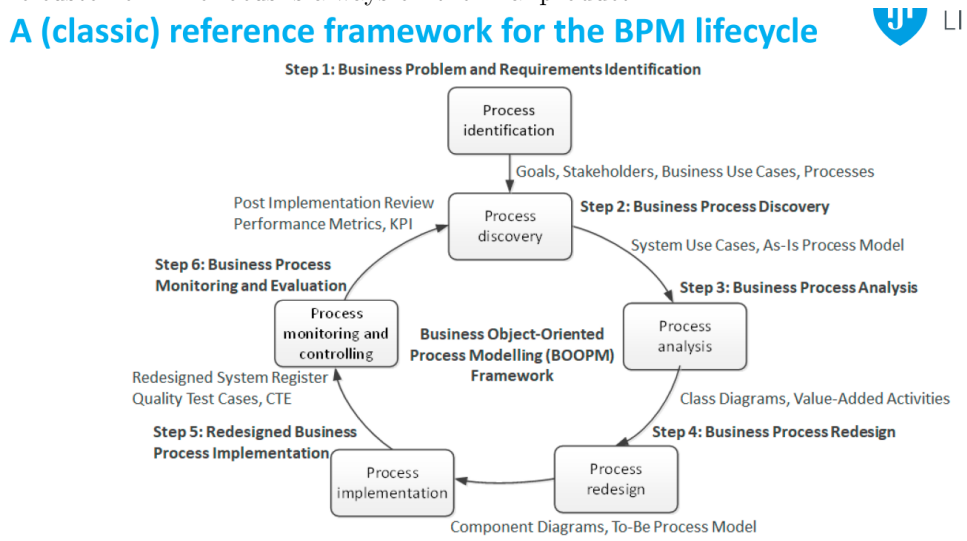
Camunda Engine is the business process executor that consumes the available microservices in the enterprise. The goal is to enable the integration with all the remaining enterprise systems and to enable the representation and execution of the sequence of business behaviours in an easy way. The process-oriented nature allows a closer approach to the business development of the enterprise.

2.1 Workflow Systems

Workflow Management System is a software platform that supports the design, development, implementation and analysis of workflows. Create new applications as an exercise of composition (existing functions) rather them the traditional development of a new application by conventional programming. Programming based on models, represented as straight forward visual constructs (visual programming). Workflows were considered, since the 90's also as a strategic approach for application integration. For all of the above reasons considered as: programming in the large

2.2 Business Process

Archimate: A business process represents a sequence of business behaviors that achieves a specific result such as a defined set of products or business services. A business process describes the internal behavior performed by a business role that is required to produce a set of products and services. For a consumer, the products and services are relevant and the required behavior is merely a black box, hence the designation "internal".
Slides: Set of interrelated activities that transform inputs into outputs in order to produce a service or product to a specific customer. The focus is always on the final product!!!



2.3 Process vs Business Process

Process:
• "A set of interrelated and cooperative activities that transform inputs into outputs".
Business Process:
• "A collection of activities that takes one or more kinds of input and creates an output that is of value to the customer."

2.4 BPMN (Business Process Model and notation)

BPMN (Business Process Model and Notation) is a standardized graphical language used to model and visualize business processes. It helps stakeholders understand and communicate how processes work using flowchart-like diagrams.

2.4.1 Process types

- **Descriptive**: Concerned with visible elements and attributes used in high-level modeling.
- **Analytic**: Contains all of Descriptive and in total about half of the constructs in the full Process Modeling Conformance Class.
- **Common Executable**: Focuses on what is needed for executable process models.

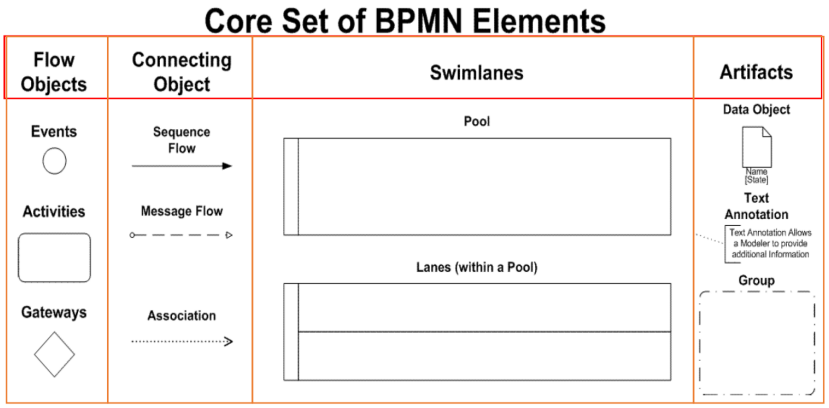
2.4.2 Types of BPMN Diagrams

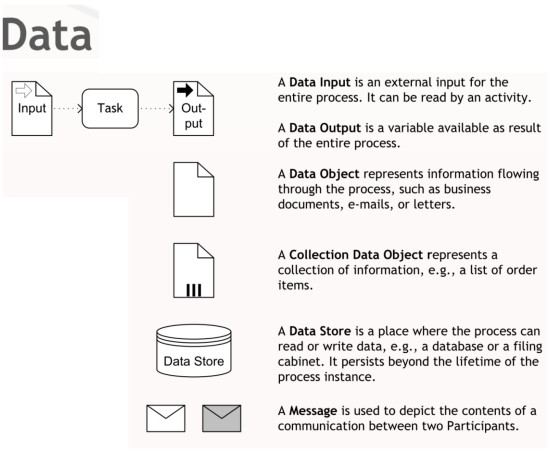
- **Process**
  - Represents the public or private processes of a participant.
  - Focus on representing the (internal) orchestration of a process.
  - The participant can be subdivided into multiple Lanes.
  - All external pools (if any) must be black-box.

- A Process focuses on a single Participant.
- A Private Process focuses on a Participant internal to the organization (a single Participant with multiple lanes is a private process).
- A Public process means more than one participant in it.

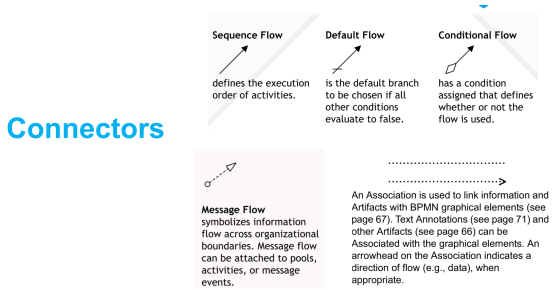
- **Collaboration**
  - Represents the message exchange between two or more participants.
  - Focus on representing the orchestration of a process across multiple participants.
- **Choreography**
  - Represent the information pertaining to each participant in the choreography.
  - The focus is not on orchestrations of the work performed within these Participants, but rather on the exchange of information between Participants.
- **Conversation**
  - Conversation diagrams visualize messages exchange between pools.
  - Design workflow with business process diagram and visualize communications with BPMN conversation diagrams.

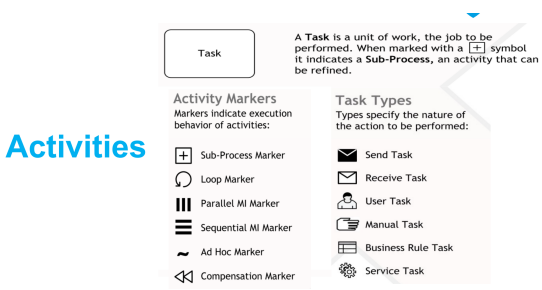
2.4.3 Core BPMN Elements





Pool: represents a process Participant. Sequence flows cannot cross Pool boundaries. Message flows can cross Pool boundaries.
Lane: a sub-division of a Pool. Used to organize and categorize the activities of a Participant. Sequence flows can cross Lane boundaries.
Activity: a unit of work.
Event: an occurrence during a business process (Like start, one line, intermediate, 2 lines, end, bold line).
Gateway: controls the flow of activities.





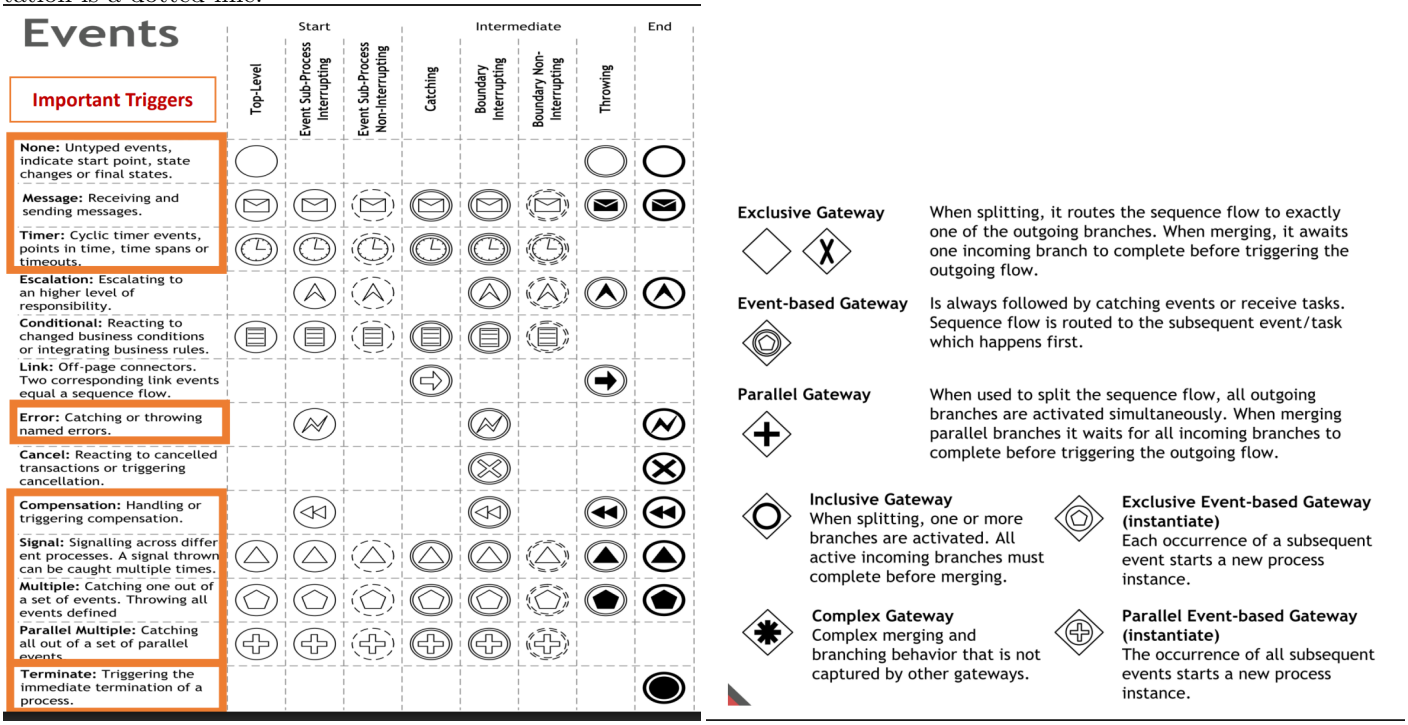
2.4.4 Event Triggers/Behaviour

A Trigger specifies what causes the Event. The Trigger is shown as an icon inside the Event symbol. BPMN defines several types of Triggers: None (i.e. no Trigger) and 12 other (Message, Timer, Error, Signal,...)
A Trigger may have two different behaviours:
Throw a Trigger (throw/send a message) (Black)
Catch a Trigger (White)

• When throwing a Trigger the Event waits for a token and then produces the Trigger. The notation for throw is a filled Trigger.
• When catching a Trigger the Event waits for a token and then waits for the Trigger. The notation for catch is an outlined Trigger. "Catch" is blocking while it waits for the Trigger and the Token.

Start events, can only catch, intermediate events, can catch and throw, end events can only throw.

Interrupting Event: when the event is thrown or caught the corresponding activity is interrupted and is not completed. Notation is a solid line.
Non-Interrupting Event: when the event is thrown or caught the corresponding activity continues its execution. Notation is a dotted line.



2.4.5 Compensation

Sometimes you need to undo the effects of a business process. You do this by **rolling it backwards**, one completed Activity at a time

There are three options for undoing each completed Activity:

1. **Do nothing** - there are no data changes to undo
2. **Overwrite** - restore all data to its original state
3. **Undo** - perform a specific Activity to undo the data changes - this is known as *compensation*

2.5 Gateways

Photo above.

2.5.1 Exclusive Gateway (XOR-split/merge)

XOR-split selects one and only one of the 2..* output flows. The conditions are evaluated top-to-bottom; the output flow associated to first condition evaluated true is selected. Optionally, a default flow (–/–) may be included. The default flow is unconditional and is selected whenever all the other conditions are evaluated false. The output flows of a XOR-split may be merged using a XOR-merge that continues as soon as one input flow arrives.

2.5.2 Parallel (AND-split/merge)

AND-split forks one input flow into 2..* parallel (concurrent in time) output flows. AND-merge waits for all input flows before joining them into a single output flow.

2.5.3 Event-Based Gateway

Follow the flow of the corresponding event that happenened.

2.5.4 Complex Gateway

These have no default semantics!

- Splitting - modeller provides an IncomingCondition
- Merging - modeller provides an OutgoingCondition

They *must* be supported by Text Annotations that describe their semantics, otherwise the BPD is unreadable!

2.6 Modelling an executable BPMN

Process automation is about automating tasks within a process as well as the automation of the control flow between these tasks. Three different combinations possible which define a kind of maturity levels of process automation:
1. The human controls the process, often passing paper around. You're probably familiar with this from physical inbox folders on your desk in an office environment. Software and office tools can, of course, make this process more efficient.
2. The computer controls the process and involves people whenever necessary, for example using task list user interfaces.
3. The whole process is fully automated and only requires manual intervention if something happens beyond the expected normal operations.

Two types of automation:
1. Automation of the control flow: The interactions between tasks are automated, but the activities itself might not. In the previous example, this was the humans cooking the food. A process might not be fully automated as it cannot run without human interaction. This is often known as human task management.
2. Automation of the tasks: The task itself is automated. In the previous example, this would be the robots who cook the food. Automating the tasks leads to fully automated processes, which is typically named STP (straight through processing). Very often this is the most ideal path, where everything runs smoothly and is fully automated. Humans are involved in case any unforeseen exceptions or special cases occur. This approach is actually quite powerful, as you can invest the effort on automation on the majority of cases and save additional (manual) effort only on the rare cases.

2.7 Business Process Execution Engine (Camunda)

2.7.1 Camunda Architecture

• Process Engine Public API: Service-oriented API allowing Java applications to interact with the process engine. The different responsibilities of the process engine (i.e., Process Repository, Runtime Process Interaction, Task Management, ...) are separated into individual services. The public API features a command-style access pattern.
• BPMN 2.0 Core Engine: this is the core of the process engine. It features a lightweight execution engine for graph structures (PVM - Process Virtual Machine), a BPMN 2.0 parser which transforms BPMN 2.0 XML files into Java Objects and a set of BPMN Behavior implementations (providing the implementation for BPMN 2.0 constructs such as Gateways or Service Tasks).
• Job Executor: the Job Executor is responsible for processing asynchronous background work such as Timers or asynchronous continuations in a process.
• The Persistence Layer: the process engine features a persistence layer responsible for persisting process instance state to a relational database.

2.7.2 Camunda Deployment & Operation environment

- Clustering – active/ative, with shared database for process execution
- Kubernetes for dynamic installation
- Separation between execution data and historical data
- Optimize available with Enterprise Edition

2.7.3 Asynchronous Continuations in Camunda BPM

Asynchronous continuations are break-points in the process execution. They are used as transaction boundaries and allow another thread than the currently active thread to continue execution.
• Async is used for placing a safe-point before an activity such that the execution state is committed. If the activity then fails to execute, the transaction is rolled back only up to the safe point.

• Async also comes in handy if you have longer-running computations and do not want to block the calling thread (eg. HTTP Thread) but instead want to delegate the heavy lifting to a background thread.
• Finally, due to the fact that asynchronous continuations are executed by the job executor, the retry mechanism can be used in order to retry a failed activity execution.

2.7.4 Handling data in process

When using Camunda, you have access to a dynamic map of process variables, which lets you associate data to every single process instance (and local scopes in case of user tasks or parallel flows).
• Input mappings can be used to create new variables. They can be defined on service tasks and subprocesses. When an input mapping is applied, it creates a new local variable in the scope where the mapping is defined.
• Output mappings can be used to customize how job/message variables are merged into the process instance. They can be defined on service tasks, receive tasks, message catch events, and subprocesses.
• Can be used to create new variables or customize how variables are merged into the process instance.

2.7.5 Camunda Authorization

• Assignee a specific user who must perform the task
• Candidate users a list of specific users who can perform a task
• Candidate groups a list of user groups who can perform the task

3 Application Programming Interfaces (API) Management

3.1 API

APIs are by definition interfaces to be used as entry points to reusable software entities with well-defined contracts. They are not independent software entities; they are instead packaged with the software libraries, frameworks, or Web services, that offer them.

Second definition: An API represents an abstraction of the underlying implementation. An API is represented by a specification that introduces types. Developers can understand the specifications and use tooling to generate code in multiple languages to implement an API consumer (software that consumes an API). An API has defined semantics or behavior to effectively model the exchange of information. Effective API design enables extension to customers or third parties for a business integration. In process API invocation: e.g., a java RMI call is handled by the same process from which the call was made. Out of process API invocation: e.g., a .NET application invocating an external REST-like API using an HTTP library is handled by an additional external process other than the process from which the call was made.

Due to their omnipresence and evolution, APIs greatly impact software development. Understanding, mitigating, and leveraging the impact of APIs and API evolution on software development is necessary to design and use software APIs APIs evolve for various reasons, such as increasing complexity, and continuous change. However, due to their nature as a connection point between software modules, API evolution is not without side effects On the one hand, as predicted by Lehman, continuing change means that API developers must determine ways to keep their APIs useful, cutting edge, and competitive with other pieces of software and API users must adapt to these API changes and new API releases. On the other hand, conservation of familiarity, or existing API usages, constrain the evolution of an API to avoid breaking changes while improving the API (i.e., security or performance improvements). The evolution of APIs therefore involves a balancing act of constant improvement and maintaining existing functionality. Maintaining existing functionality requires in-depth knowledge of use cases and architectural foresight and flexibility, while keeping up with rapid release cycles requires modifications to user applications as well as learning about new APIs and changes to existing APIs.

3.2 Differences from SOA

From an architectural perspective they are similar: “a logical representation of a repeatable activity that has a specific outcome, the usual notion of a service” But the focus is different:
• APIs were focused in simplifying the consumption, developer centric, humanreadable contract
• SOA focus in shielding the client from back-office applications changes

3.3 API trends

New tools and techniques typically seek to help with API evolution by resolving problems that it can cause for API users (e.g., API migration tools) or to help reduce the development burden on API developer (e.g., automatic API documentation tools). Empirical studies related to API evolution typically employ large data, case studies, or user studies

to provide evidence of existing problems, the impacts of API evolution, or potential solutions to existing problems. These problems typically centre around the impacts of API evolution on API usability and API maintainability.

3.4 API Management

It is a set of tools and services that enable developers and companies to build, analyze, operate, and scale APIs in secure environments. API management can be delivered on-premises, through the cloud, or using a hybrid on-premises – SaaS.

3.4.1 Important features of API management tools

- **API ACCESS CONTROL:** APIs should be built using access controls, commonly known as authentication and authorization, that grant users permission to access certain systems, resources, or information.
- **API PROTECTION:** API protections include API keys for identification, API secrets, and application authorization tokens that can be verified.
- **API CREATION AND DESIGN:** APIs allow web applications to interact with other applications. You can create and define different types of APIs such as RESTful APIs and WebSocket APIs.
- **SUPPORT FOR HYBRID MODELS:** A RESTful API is a group of resources and methods, or endpoints, that leverage an HTTP request type. A WebSocket API maintains a persistent connection between connected clients.
- **HIGH PERFORMANCE:** Highly performant APIs depend on code, the separation of functionalities, and on underlying data structure and data architecture.
- **CUSTOMIZABLE DEVELOPER PORTAL:** API developer portals connect API publishers with API subscribers. They enable self-service API publishing and allow potential API customers to easily discover APIs they can use.

3.5 Representation State Transfer (REST)

It is a set of architectural contraints, most commonly applied using HTTP as the underlying transport protocol. To be considered RESTful your API must ensure that:
1. A producer-to-consumer interaction is modeled where the producer models resources the consumer can interact with.
2. Requests from producer to consumer are stateless, meaning that the producer doesn't cache details of a previous request. In order to build up a chain of requests on a given resource, the consumer must send any required information to the producer for processing.
3. Request are cachable, meaning the producer can provide hints to the consumer where this is appropriate. In HTTP this is often provided in information contained in the header.
4. A uniform interface is transmitted to the consumer.
5. It is a layered system, abstracting away the complexity of systems sitting behind the REST interface. For exemple, the consumer should not know or care if they are interacting with a database or other services.

3.5.1 REST data elements

The key abstraction of information in REST is a resource. Any information that can be named can be a resource (document, image, etc.) In other words, any concept that might be the target of an author's hypertext reference must fit within the definition of a resource. A resource is a conceptual mapping to a set of entities, not the entity that corresponds to the mapping at any particular point in time.

REST components perform actions on a resource by using a representation to capture the current or intended state of that resource and transferring that representation between components. A representation is a sequence of bytes, plus representation metadata to describe those bytes. Other commonly used but less precise names for a representation include: document, file, and HTTP message entity, instance, or variant.

A representation is a sequence of bytes, plus representation metadata to describe those bytes. The data format of a representation is known as a media type. Some media types are intended for automated processing, some are intended to be rendered for viewing by a user, and a few are capable of both. Composite media types can be used to enclose multiple representations in a single message. Response messages may include both representation metadata and resource metadata: information about the resource that is not specific to the supplied representation.

Control data defines the purpose of a message between components, such as the action being requested or the meaning of a response. It is also used to parameterize requests and override the default behavior of some connecting elements. For example, cache behavior can be modified by control data included in the request or response message. A representation

can be included in a message and processed by the recipient according to the control data of the message and the nature of the media type.

3.5.2 REST over HTTP

An HTTP request is:
• A verb (aka method), most of the time one of GET, POST, PUT, DELETE or PATCH
• A URL
• Headers (key-value pairs)
• Optionally a body (aka payload, data)
An HTTP response is:
• A status, most of the time one of 2xx (successful), 4xx (client error) or 5xx (server error)
• Headers (key-value pairs)
• A body (aka payload, data)
HTTP verbs characteristics:
• Verbs that have a body: POST, PUT, PATCH
• Verbs that must be safe (i.e. that mustn't modify resources): GET
• Verbs that must be idempotent (i.e. that mustn't affect resources again when run multiple times): GET (nullipotent), PUT, DELETE

3.5.3 Richardson maturity heuristics

• Level 0: The starting point for the model is using HTTP as a transport system for remote interactions, but without using any of the mechanisms of the web. Essentially, using HTTP as a tunneling mechanism for remote interaction mechanism, usually based on Remote Procedure Invocation.
• Level 1 – introduce Resources: rather than making all our requests to a singular service endpoint, start talking to individual resources. Tackles the question of handling complexity by using divide and conquer, breaking a large service endpoint down into multiple resources.
• Level 2 - using the HTTP verbs: as closely as possible to how they are used in HTTP itself. Introduces a standard set of verbs so that we handle similar situations in the same way, removing unnecessary variation.
• Level 3 - Hypermedia Controls introduces HATEOAS (Hypertext As The Engine Of Application State).
• Level 3 introduces discoverability, providing a way of making a protocol more self-documenting.

3.6 Open API

REST APIs are technological implementation of services and do not account with contracting issues. Usually an additional document, or wiki documents the API usage. However, those are hard to maintain and testing is not automating. "The OpenAPI Specification (OAS) defines a standard, languageagnostic interface to HTTP APIs which allows both humans and computers to discover and understand the capabilities of the service without access to source code, documentation, or through network traffic inspection. When properly defined, a consumer can understand and interact with the remote service with a minimal amount of implementation logic".

Swagger has evolved into one of the most widely used open source tool sets for developing APIs with rich support for the OpenAPI Specification, AsyncAPI specification, JSON Schema and more.

The contract of an API encompasses:
• Title
• Endpoint
• Method
• URL parameters
• Message payload
• Header parameters
• Response code
• Error code
• A sample request and response
• Tutorials and walkthrough
• Service-level agreement

3.7 GraphQL

It is an API technology developed by Facebook to address some of the challenges faced with RESTful APIs, particularly in complex applications where multiple data sources need to be queried. Allows the client to request only the specific data it needs, using a declarative query language, reducing over-fetching and under fetching issues common with RESTful APIs. Provides a flexible and efficient way for front-end applications, making it a choice for applications with complex data requirements and a variety of front-end interfaces. It allows developers to define their queries precisely, resulting in fewer network requests and less data transfer. However, comes with additional complexity compared to RESTful APIs and requires more careful management of server-side schema

3.8 gRemote Procedure Call (gRPC)

Developed by Google, is a high-performance, open-source API framework that uses HTTP2 for transport and protocol buffers as data format. gRPC is designed to provide efficient communication between microservices, making it highly suitable for blockchain backends that require fast and reliable communication with front-end clients. One of the advantage is its ability to support bi-directional streaming, which is particularly useful for real-time applications where low latency is critical. Unlike RESTful APIs, gRPC allows the server to push updates to the client, making it suitable for applications that require continuous data streams. gRPC's performance and efficiency make it an excellent option for projects that demand low latency and high data throughput, such as real-time trading platforms or blockchain monitoring services. However, gRPC is more complex to implement than REST or GraphQL and may require more setup, particularly for handling serialization and managing HTTP2 connections. Despite this, its performance benefits are invaluable for projects with stringent speed and reliability requirements.

3.9 API Gateway Systems (KONG)

According to Gartner, a gateway in computer networking: "gateway converts information, data, or other communications from one protocol or format to another".
Moreover, it must allow communication in both directions and maintain the connections. A gateway can also be seen as a "supervised entry point" through which messages (carries of information/knowledge) can enter a particular environment undergiven conditions and rules applied.

Provides or integrates with third-party gateways for runtime management, security, policy enforcement, throttling, operational control and usage monitoring for APIs.

Specific:
• Kong Gateway, is a commercial version of its open-source API gateway based on NGINX and OpenResty.
• Kong Gateway works as a reverse proxy that manage, configure, and route requests to other APIs.
• Kong Gateway runs in front of any RESTful API and can be extended through modules and plugins. It's designed to run on decentralized architectures, including hybrid-cloud and multi-cloud deployments.

Advantages of an API Gateway System
• Enable new consumers without coding or configuration (Interface and Volume Scoping, Routing)
• Keep unwanted people & robots out of your systems(Authorization and Authentication, Threat Protection)
• Understand what is happening with your APIs (Discovery, Usage, and Concerns, History)

3.9.1 Kong main concepts

• Service: is the name Kong uses to refer to the upstream APIs and microservices it manages
• Route: specify how (and if) requests are sent to their Services after reaching Kong
• A single Service can have multiple Routes.
• Plugin: extension to the Kong Gateway, written in Lua or Go
• Port 8001 is used for managing APIs
• Port 8000 for service invocation

3.9.2 Full lifecyle of API management

• Design APIs – solutions such as swagger that are able to facilitate the design, build and documentation
• Run APIs – solutions such as Kong that are able to connect to endpoints and return the responses
• Secure APIs – solutions such as Kong plug-ins that are able to apply fine-grained security and traffic policies to services
• Govern APIs – solutions such as Konga that are able to gain real-time visibility of the services

3.10 Identity Management

3.11 AAA (authentication, authorization and accountability) framework

• Authentication (A) - It is the challenge process by which identity claims are tested and validated. The purpose of the authentication is ensuring that a particular user is really who he or she claims to be. Then access is granted to a system if granted by the authorization' process execution
• Authorization (A) - After authentication, the authorization process enforces the system' policies, granular access control, and user privileges. It also establishes the tasks and activities that users can perform within those authorized resources
• Accountability (A) - is about measuring what's happening within the system, collecting and logging data on user sessions, e.g., length of time, type of session, and resource usage. It offers a clear audit trail for compliance and business purposes.

3.11.1 Authentication (A)

It is the challenge process by which identity claims are tested and validated, where challenge is secret and could be:
• Password
• Physical identifies: card, physical key
• Biometric data: face, iris, fingerprint
• Cypher/decipher challenge with keys
Authentication in applications/data stores within an organization:
• Typically, single sign-on using LDAP to interact with Active Directory, Kerberos

But, on the Cloud, multiple options possible:
• Each organization does its authentication leads to multiple identities
• One organization authenticates all participants
• For each business partnership, an organization (s) is chosen to authenticate
• Allow each organization to use its authentication framework and create a loosely coupled mechanism allowing the reuse of identities and authentication

3.11.2 Authorization (A) (Não acho isto necessário?)

Today, countless access control models (ACM) solutions are available in the academy and industry. Some examples:
• Discretionary access control (DAC)
• Mandatory access control (MAC)
• Role-based access control (RBAC)
• Time-role-based access control (TRBAC)
• Attribute-based access control (ABAC)
• Orcon or Chinese wall
• Nevertheless, in the majority of situations, the recognized development of ACM, these solutions specifies and implements the structural security access concerns of a single organizational silo.

3.12 eXtensible Access Control Markup Language (XACML)

XACML is an XML-based standard markup language for specifying access control policies. The standard, published by OASIS defines a declarative fine-grained, attribute-based access control policy language and a processing model describing how to evaluate access requests according to the rules defined in policies.
XACML is an attribute-based access control system:
• Input, e.g., the information about the subject accessing a resource, the resource to be addressed, and the environment
• Output, the decision of whether access is granted or not

• Policy - A set of rules, an identifier for the rule-combining algorithm and (optionally) a set of obligations or advice. May be a component of a policy set
• PAP - Policy Administration Point is the system entity that creates a policy or policy set
• PEP - Policy Enforcement Point is the system entity that performs access control, by making decision requests and enforcing authorization decisions.
• Obligation - An operation specified in a rule, policy or policy set that should be performed by the PEP in conjunction with the enforcement of an authorization decision
• PDP - Policy Decision Point is the system entity that evaluates applicable policy and renders an authorization decision
• PIP - Policy Information Point is the system entity that acts as a source of attribute values

3.13 SAML

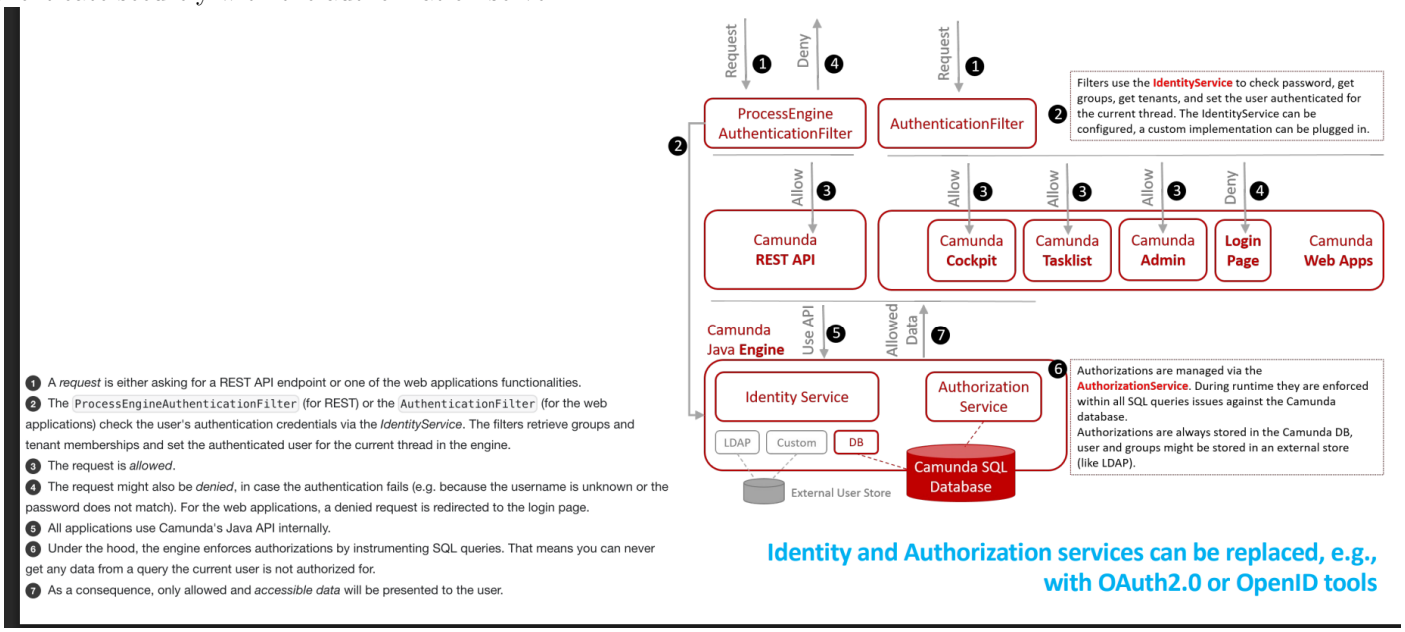
SAML is a well-established standard developed by the OASIS consortium for authentication and authorization. Developed during early 2000s, now in the version 2.0, it is an XML-based standard heavily influenced by the enterprise technologies popular at the time, especially the WS- stack. Similar to some other XML-based standards, it defines a hierarchy of basic concepts - assertions, protocols, bindings and profiles. The most common SAML profile (simplified, profiles are essentially use-cases) is multi-domain web single sign-on and includes interaction between three parties - a user, an Identity provider, and a Service Provider. In this scenario, the user already has an established session with one web site, during which the user is redirected to a new web site. The original website acts as an IdP and relays information to the redirected website that acts as a Service provider. The relayed information effectively authenticates the user through a SAML message allowing for a session between the user and the redirected website to be established. In SAML terms, the first website is generally referred to as the asserting party and the second as the relying party.

3.14 OpenID

OpenID Connect is an authentication protocol specified and maintained by the OpenID Foundation. The foundation's members are mostly international corporations including well-known names like Google, Microsoft, Oracle, PayPal, Verizon, RSA, VMWare, Deutsche Telekom. The protocol is defined through a set of OpenID specifications including the core specification (Sakimura, 2014) and accompanying specifications detailing additional services (like dynamic provider discovery, dynamic registration with providers, response types, etc.). Unlike the previous versions of OpenID, the current one (final specification launched in 2014) is based on the previously described OAuth 2.0 protocol. The specification extends and additionally specifies parts of the OAuth specification that have been left open by OAuth, so OAuth-based mechanisms could be used in authentication scenarios

3.15 OAuth 2.0

OAuth 2.0 standard is published and maintained by IETF through a set of RFC documents, the core consisting of RFC 6749 (Hardt, 2012 (1)), RFC 6750 (Hardt, 2012 (2)) and RFC 6819 (McGloin, 2013). OAuth 2.0 is foremost an delegation protocol. The user provides permission to a third party (a client in OAuth terms) to access some of user's data at the identity. For example, the user allows a site like fit4life.com read-only access the user's fitness data stored at google.com (an authorization server and resource server in OAuth terms), without necessarily divulging any of the user's other confidential data. Being a more modern protocol that targets not only web applications and services but also handheld devices, OAuth makes a clear distinction between public and confidential clients based on their ability to authenticate securely with the authorization server.



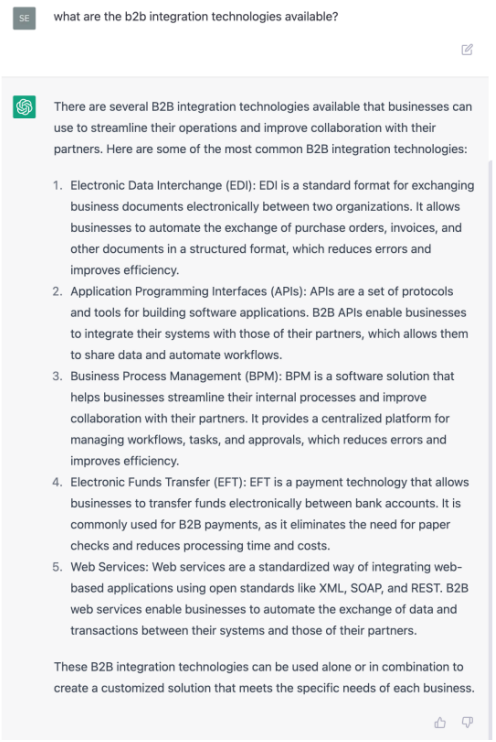
	OAuth2	OpenID	SAML
Token (or assertion) format	JSON or SAML2	JSON	XML
Authorization	Delegation	No	Yes
Authentication	Pseudo-authentication	Yes	Yes
Security risks	Phishing OAuth 2.0 does not support signature, encryption, channel binding, or client verification. Instead, it relies completely on TLS for confidentiality	Phishing Identity providers have a log of OpenID logins, making a compromised account a bigger privacy breach	XML Signature Wrapping to impersonate any user
Best suited for	API authorization	Single sign-on for consumer apps	Single sign-on for enterprise Note: not well suited for mobile

3.16 Consent Management

Consent Management refers to the process and system by which an organization collects, manages, and maintains user consent for the collection and processing of personal data. It ensures compliance with privacy laws and regulations, such as the GDPR (General Data Protection Regulation) and CCPA (California Consumer Privacy Act), by allowing users to make informed decisions about what personal data they are willing to share. The goal is to give users control over their data while also providing transparency about how it is being used. It involves obtaining clear consent, documenting it, and ensuring that it can be easily modified or withdrawn by the user at any time.

4 B2B

'chat.openai.com/chat



- Point to point integration - Increasing cost, Hard to maintain and scale (Different protocols, messages, and security)
- Centralized hub integration - Who implement the bus? Who pays for it? (Trustability problem (maybe solved by blockchain?), Data privacy problem, Cost too high, only applicable to big companies)

- Internet integration - Each company is responsible for his own EAI (Enterprise Application Integration), including all protocol layers, security and audit, Standard EAI connectors simplify interoperability and reduce the deployment cost
- Marketplaces (Like amazon business) - Transaction costs is higher, but companies invest less in IS, Trust is increased, Value chain observability.

5 Perguntas

5.1 Being informed, and an expert, about the following main key terms

5.1.1 DMN (Decision Model and Notation)

DMN (Decision Model and Notation) is a standardized modeling language used to represent and automate business decisions. It separates decision logic from process flow, allowing organizations to define rules in a clear, structured way. DMN models typically use decision tables and diagrams to capture business rules, making them understandable to both technical and non-technical stakeholders. This helps improve consistency, transparency, and flexibility in decision-making across systems and teams.

5.1.2 Camunda business key

In Camunda, the business key is a unique, human-readable identifier assigned to a process instance, often representing a business entity like an order or customer ID. It helps correlate the process with external systems and makes querying and tracking easier. Once set, it cannot be changed.

5.1.3 Docker

Docker is a platform that enables developers to package applications and their dependencies into lightweight, portable containers. These containers run consistently across different environments, making deployment faster and more reliable.

5.2 What is it and explain in detail how does it work?

5.2.1 Business process engine

A business process engine is software that executes and manages business process models, typically defined in BPMN. It controls the flow of tasks, handles user interactions, manages rules, and integrates with systems to automate business workflows.

5.2.2 Authorization of a business process engine

Authorization in a business process engine controls who can perform specific actions within processes. It ensures that users or systems have the correct permissions to start, view, complete, or manage process instances, tasks, and resources. This helps enforce security, compliance, and role- based access within workflows.

5.2.3 Identity management

Identity management is the process of creating, managing, and verifying digital identities within an organization. It ensures that the right individuals have access to the right resources at the right times by handling user authentication, authorization, roles, and lifecycle management. This is essential for security, compliance, and efficient access control.

5.2.4 Camunda form

In Camunda, a form is a user interface element used to collect input from users during a workflow. Forms can be embedded in tasks to capture data needed to proceed, such as approval decisions or details entry

5.2.5 Camunda http-connector

An http-connector in Camunda is able to make requests to endpoints through http. As definitons, you need to define the method used (POST, GET, etc.), the payload in the body of the request and the url itself to connect to. This is for input, for output, you can use JavaScript, for example, to parse the response and create variables that are outputted. It is ine type of camudna service task.

5.2.6 Camunda user interaction task

A Camunda user task is a step in a business process where human interaction is required. It pauses the automated workflow until a user completes the task, such as filling out a form or approving a request. User tasks enable collaboration between people and automated processes.

5.2.7 Camunda service task

A Camunda service task is an automated step in a business process that executes predefined backend logic without human intervention. It can call external services, run scripts, or execute code to perform tasks like data processing, system integration, or API calls.

5.2.8 Serverless API invocation process. What is cold start and warm execuction?

Cold start happens if the function isn't currently running. The cloud provider must allocate resources and initialize the function environment before execution, causing a delay (latency).

Warm execution occurs when the function is already initialized and ready from a recent invocation, so it runs immediately with minimal delay.

5.2.9 What type of computational offer from cloud providers is depicted when referring to serverful computing?

Serverful computing refers to traditional cloud offerings where you manage and provision servers or virtual machines yourself. You're responsible for configuring, scaling, and maintaining the underlying infrastructure. Examples include virtual machines (VMs), dedicated servers, or managed Kubernetes clusters.

5.2.10 What does autoscaling means?

Autoscaling is the cloud capability to automatically adjust the number of running resources—like servers or containers—based on current demand. It helps maintain performance during high load and reduce costs during low usage.

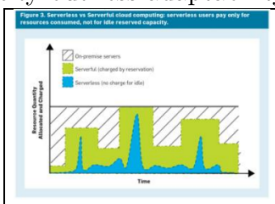
5.2.11 Compare autoscaling and the "premium upgrades" in serverful computing what the main difference between them for the end user is?

The main difference between autoscaling and premium upgrades in serverful computing lies in flexibility and automation:

Autoscaling automatically adjusts resources (e.g., CPU, memory, instances) based on real-time demand, with no manual intervention.

Premium upgrades are manual or static increases in resource capacity (like choosing a larger VM type), requiring user action and often restarts.

For the end user, autoscaling means smoother performance and cost-efficiency, while premium upgrades offer fixed capacity but less adaptability to changing workloads.



Considering the technological dependencies imposed by the following three distinct environments: on-premises servers, serverful and serverless, which were the changes that you need to do if you want to migrate JAVA code:

a) From on-premise to serverful? Adapt to the container operating system and environment + network dependencies

b) From serverful to serverless? Comply to serverless libraries and methods + change to short living processing

5.3 What are the advantages and pitfalls of?

DMN Advantages - Clear, reusable decision logic. Business-friendly and easier to maintain.
DMN Pitfalls - Adds complexity and requires extra learning.

BPMN Gateways Advantages - Simple for basic decisions. No separate tools needed.

BPMN Pitfalls - Hard to manage complex logic. Logic is less reusable and harder to update.

5.4 Pull and push for Camunda task execution

Pull (External Tasks) Advantages - Decoupled and scalable. Good for microservices.

Pull (External Tasks) Pitfalls - Needs polling. Slight latency.

Push (Java Delegates) Advantages - Fast, runs inside engine. Simple setup.

Push (Java Delegates) Pitfalls - Tightly coupled. Harder to scale or externalize.

5.5 What are the differences between the concepts of?

5.5.1 BPMN descriptive process and BPMN executable process

BPMN Descriptive Process is used to visually document and communicate business workflows without technical details. BPMN Executable Process includes all technical details needed to run the process automatically in a BPM engine.

5.5.2 Pull and push for Camunda task execution

Pull (External Tasks) means workers actively fetch tasks from the Camunda engine when they are ready to execute them. This allows better scalability, loose coupling, and easier integration with distributed systems or microservices. However, it may introduce some delay due to polling.

Push (Java Delegates) means the Camunda engine directly invokes the task's code as part of the process execution. This offers faster response and simpler setup but creates tighter coupling between the process engine and the task logic, making scaling and external integration harder.

5.6 How do you? Specify the most relevant steps to perform the following task:

To expose an AWS Lambda function to the internet:
Deploy your Lambda function.
Create an API Gateway and set up an HTTP method linked to your Lambda.
Ensure API Gateway has permission to invoke the Lambda.
Deploy the API to a stage, which provides a public URL.
Use the API Gateway URL to access your Lambda from the internet.

5.7 Multiple Choices

Some examples of "What is the correct answer?

An application built with a microServices framework:
a) Can communicate with other microServices using REST which is very well suited to a time decoupled pattern of communication
b) Can communicate with other microServices using events which are very well suited to a time decoupled pattern of communication
c) Can communicate with other microServices using shared databases
d) The programming model using service synchronous invocation is more complex than event invocation

From the point of view of an API that is exposing services:
a) API's are focused are focused on the governance of services
b) They must be defined in REST
c) SOA has exactly the same objective
d) API's expose a business asset that has value for the owner

Serverless Functions:
a) There is no server executing the function

b) The main objective is to reduce function administration to a minimum
c) It is a model of execution that existed on premises and migrated to the cloud
d) The main objective is speed of execution

Pitfalls related with Serverless functions:
a) More difficult to have high availability
b) Latency on cold starts
c) Can only be used for synchronous invocations
d) Long time execution functions are allowed

Benefits of a Business Process oriented approach:
a) Automatically builds a service hierarchy
b) It produces applications which are more performant than with traditional development
c) Business analysts model the Business Processes in BPMN and then IT people need to create the executable counterparts
d) It creates a complete application which can be integrated with legacy systems and external services

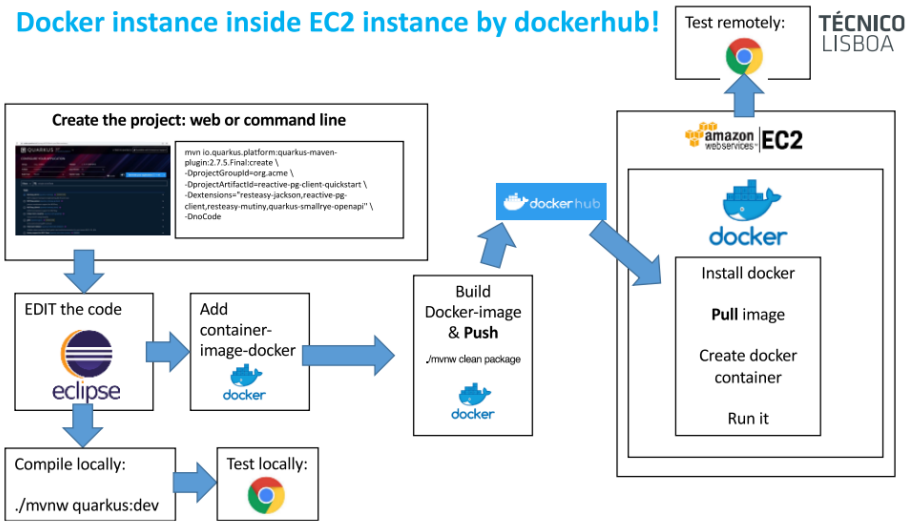
A microservice framework scope:
a) Microservices are based on the principle that they can be orchestrated by a controller service
b) Microservices in opposite to SOA do not have to be high granularity services
c) An application based on microservices defines a choreography using its interfaces
d) Microservices are highly dependent on an Enterprise Service Bus

Considerer a business service of "Selling a product" on an E-commerce application. The interface of the service is specified in JSON and uses the REST protocol. The first time a user purchases something the services requires authentication and register that internally. After that, on a second invocation, the service already has the user identity and follows for the purchase. From this simple description chose the best answer:

a) Loosely coupled and connection oriented
b) Tightly coupled and connection oriented
c) Loosely coupled and connectionless
d) Tightly coupled and connectionless

Camunda authentication and authorization. Which sentence is false?
a) Camunda can use an external identity provider
b) Camunda doesn't need to have an authenticated user
c) Camunda has an internal authorization service that enforced authorization based on the role defined in BPMN
d) Camunda can invoke external services providing authentication credentials

5.8 Images (Business process, etc.)



Considering the process depicted in the above figure to deploy a new Quarkus microservice in the AWS cloud environment.

a) Why is Docker used? Explain the reasons referring to at least 2 advantages.

b) Without Docker, what are the other alternatives to achieve the same deployment?

c) What is the technology that could be used to automate the Quarkus microservices unit tests (both locally and remotely)?

a)

Ensures consistency across environments (local and cloud).
Simplifies deployment by packaging the app with its dependencies.

b)

Manual setup with EC2 user data scripts.
Use Elastic Beanstalk or build native binaries and upload them.

c)

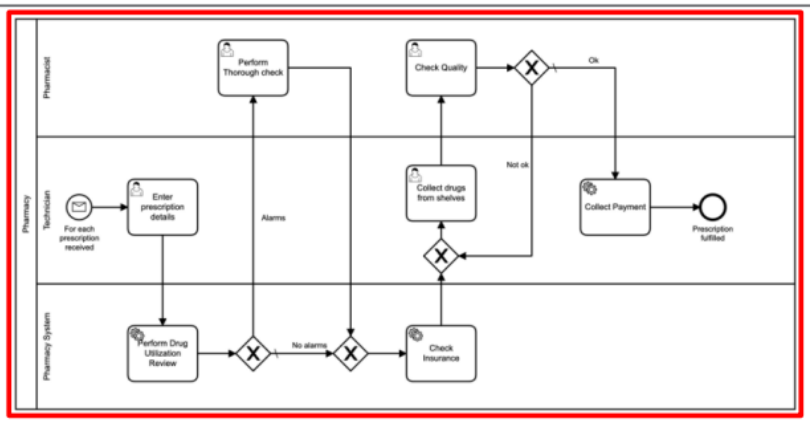
Use CI/CD tools like GitHub Actions, GitLab CI, or Jenkins for running unit tests locally and remotely.

Business processes

Consider the following process model description that the **PharmacyComp** company follows when a client submits a drug prescription.

The process starts when a technician receives a new prescription. The process interest involves three participants: Technician, Pharmacist and Pharmacy System. First, the technician enters the prescription details. Afterwards, the pharmacy system performs a drug utilization review. If an alarm is triggered, then the Pharmacist Perform a Thorough check. Otherwise, the pharmacy system checks the insurance coverage (3rd party company) to verify credit.
If drugs are covered by insurance, then the technician collect the drugs from shelves and the Pharmacist check its quality.
If drugs quality is OK the technician collects the payment and the process ends. Otherwise, technician repeats the drugs collection from shelves and the Pharmacist check its quality again.

1) Design the **PharmacyComp** process using BPMN notation, for a non-executable process, and reusing the existing elements in the following pool:



2) Now, consider that the company wants to automate this process to deal with drug prescription in a more efficient manner.
   a) Considering the CAMUNDA engine capabilities, explain how this part of the previous universe of discourse could be implemented?
   "…the technician enters the prescription details …"
   Explain, in detail, the required steps to implement this part of the process.

   b) Considering the CAMUNDA engine capabilities, explain how this part of the previous universe of discourse could be implemented?
   "…the pharmacy system checks the insurance coverage (3rd party company) to verify credit …"
   Explain, in detail, the required steps to implement this part of the process.

a)

To implement this with Camunda:

- Model a User Task in BPMN (e.g., "Enter Prescription Details").
- Assign the task to a user group (e.g., technicians) via task candidate groups.
- Use Camunda Tasklist to display the task to the technician.
- Technician logs in, fills the form (via embedded or external form), and submits it.
- Data is passed to the next BPMN task via process variables.

b)

To implement this as a service task:

- Create a Service Task in BPMN (e.g., "Check Insurance").
- Configure it as an external task or use a Java/REST connector.
- The pharmacy system (or a worker) polls for this task (if using external task pattern).
- It then calls the insurance API (3rd party system).
- The response (e.g., coverage approved/rejected) is stored as a process variable.
- The workflow proceeds based on the response using a gateway.

Business processes

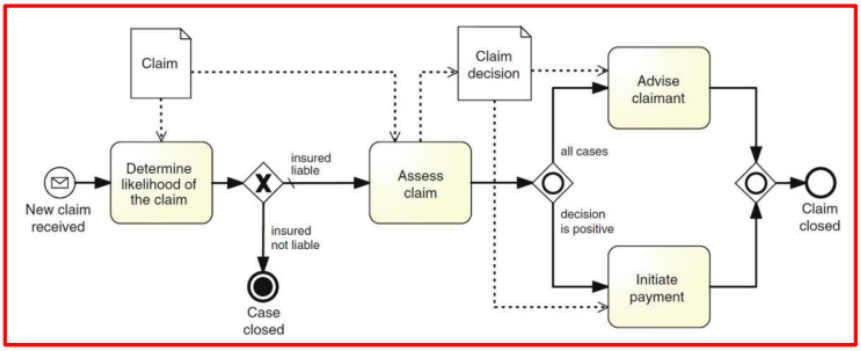
Consider the following process model description that the **InsuranceComp** company follows when a client submits an insurance claim.

```
The process starts when a customer submits a new insurance claim.
Each insurance claim goes through a two-stage evaluation process.
```

[redacted]

```
First of all, the liability of the customer is determined. Secondly, the claim is
assessed in order to determine if the insurance company has to cover this liability and
to what extent.
If the claim is accepted, payment is initiated, and the customer is advised of the
amount to be paid. All tasks except "Initiate Payment" are performed by claim handlers.
There are three claim handlers.
The task "Initiate Payment" is performed by a financial officer.
There are two financial officers.
```

3) Design the **InsuranceComp** process using BPMN notation, for a non-executable process, and reusing the existing elements in the following pool:



4) Now, consider that the company wants to automate this process to deal with claims in a more efficient manner.

1) Considering the CAMUNDA engine capabilities, explain how this part of the previous universe of discourse could be implemented?

```
"…There are three claim handlers…"
```

Explain, in detail, the required steps to implement this part of the process.

2) Considering the CAMUNDA engine capabilities, explain how can the

```
"…the liability of the customer is determined …"
```

be implemented?
Explain, in detail, the required steps to implement this part of the process.

[redacted]

3) Considering the CAMUNDA engine capabilities, propose two different implementation options to inform the client about the **InsuranceComp'** decision?
Explain, in detail, the required steps to implement both options.

1. Configure identity service with three user accounts for claim handlers, Create "claim-handlers" group and assign the three users to it, Set the "Claim decision" task's candidate group to "claim-handlers", Deploy the process and use Camunda Tasklist for task management
2. Several ways: Model the service task in BPMN Create DMN decision table with liability rules, Configure external task worker or REST connector, Define input/output variable mappings, Handle exceptional cases with boundary events
3. Option 1: Automated Email Notification Service Implementation:

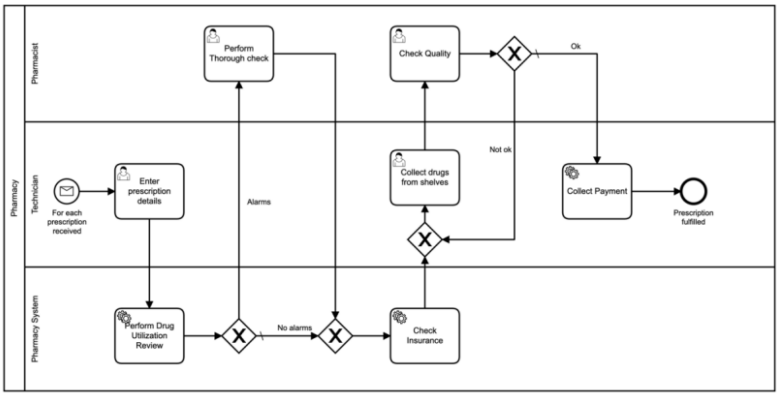
   Create "Send Decision Notification" service task after claim decision Use Camunda's email connector with SMTP configuration Create email templates for approved/rejected claims using process variables Configure as async task with retry mechanism for failed deliveries

Option 2: Manual User Task Communication Implementation:

Create "Notify Customer" user task assigned to customer service group Design form showing claim details and decision rationale Provide communication method options (email, SMS, phone, postal mail) Include documentation fields for communication tracking

Executable BPMN in Camunda

Consider the following process model description that the **PharmacyComp** company follows when a client submits a drug prescription.



Consider that this company wants to automate this process to deal with prescriptions in a more efficient manner using the CAMUNDA engine capabilities.

4) Explain and discuss, in detail, the two alternative solutions (Push and Pull) to implement the *"Collect Payment"* Task?

5) Describe, in detail, two technological alternatives that are available to trigger the instantiation of this process model, as depicted in the next figure.

6) Propose, in detail, a change in the process model to inform the client about the **PharmacyComp'** process result execution. You can design the change directly in the business process model and/or explain it textually.

4) Push: The process engine assigns the task directly to a user or system when it reaches that point in the workflow. The assignee is notified via Tasklist or other means.

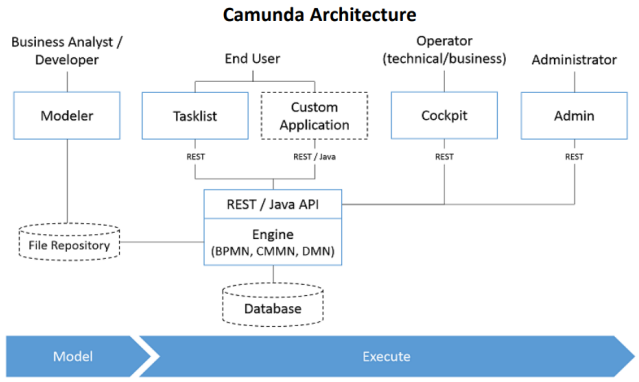
Pull: A worker (e.g., POS system or external task client) polls Camunda for available tasks and "pulls" the Collect Payment task when ready to process it.

5) REST API: An external system sends a POST request to Camunda's /process-definition/key/key/start endpoint when a new prescription is received.

Message Event: A BPMN message start event is used to trigger the process when a message (e.g., PrescriptionReceived) is sent by another system.

6)Model Change: Add a new Service Task (e.g., Notify Client) after the Collect Payment task, using an external system or message to inform the client.

Alternative: Use a Send Task or Message End Event to trigger an email, SMS, or app notification informing the client their prescription is ready or processed.



1) Considering the CAMUNDA architecture depicted in the previous Figure, identify the component (or the components) that is (or are) responsible to execute the instances of a business process?

2) Consider that multiple instances of a given business process, at the same time, are required to be executed. This is a functionality supported by CAMUNDA. What is the CAMUNDA mechanism that can differentiate each instance of the given business process? Explain with an example how it works.

3) Considering the Camunda architecture, what is the difference between an *"assignee"* and a *"candidate groups"* defined within the context of a BPMN task? In which situation should you use one or the other?

4) Considering the following figure, where task B is being implemented as a http-connector, what are the mandatory configurations to enable such connectivity?

---

1)The Engine component (BPMN, CMMN, DMN) is responsible for executing instances of business processes. It interprets the process models and manages the execution flow.

2)Camunda uses Process Instance IDs (unique system-generated) and optionally Business Keys (user-defined identifiers). For example, when starting an "Insurance Claim" process, you can set a business key like "CLAIM-2024-001" for John's claim and "CLAIM-2024-002" for Mary's claim, making instances easily identifiable and searchable by business-meaningful identifiers

3)Assignee: Assigns a task to a specific individual user (e.g., assignee="john.doe")
Candidate Groups: Assigns a task to a group of users who can claim it (e.g., candidateGroups="sales-team")

When to use:
Use assignee when you know exactly who should do the task
Use candidate groups when any member of a team can handle the task (load balancing)

4) For a task implemented as an HTTP connector, the mandatory configurations are:

URL: The endpoint to call
HTTP Method: GET, POST, PUT, DELETE, etc.
Headers: Required HTTP headers (e.g., Content-Type, Authorization)
Input/Output Variable Mapping: How to pass data to/from the HTTP call

BPMN versus DMN

Consider the following DMN decision table:

Meal — Hit Policy: Unique

	When Season (string)	And Number of guests (string)	Then Meal (string)	Annotations
1	"Spring"	<= 4	"Green asparagus"	
2	"Spring"	5	"White asparagus"	
3	"Spring"	[6..8]	"Spinach"	
4	"Spring"	>= 9	"Pasta"	
5	not("Spring")	-	"Lasagne"	
+				

1) Design an equivalent BPMN model using gateways, that is able to perform exactly the same behavior.
2) Discuss advantages and disadvantages of using a DMN decision table instead of using a BPMN model with gateways.
3) How can a DMN decision table be linked with a BPMN process using CAMUNDA? Give an example.

1)Start event, Exclusive gateway checking Season == "Spring", If Spring: Second exclusive gateway checking Number of guests (less or equal 4, =5, [6,8], more or equal 9), Each path leads to a service task setting the meal variable ("Green asparagus", "White asparagus", "Spinach", "Pasta"), If not Spring: Direct path to service task setting meal to "Lasagne" All paths converge to end event

2)DMN decision tables offer several advantages over BPMN gateways: they are business readable allowing non-technical users to understand and modify rules, highly maintainable since you can add or remove rules without changing the process structure, provide centralized logic with all decision rules in one place, and support independent version control of decision tables. However, DMN also has disadvantages including additional complexity requiring understanding of DMN notation, tool dependency needing DMN-capable tools, and less visual flow since decision logic is separated from the process flow.

3)Add Business Rule Task to BPMN process, Set implementation to "DMN", Configure Decision Reference to point to DMN table ID (e.g., "meal-decision"), Map input variables (Season, Number of guests), Map output variable (Meal)