

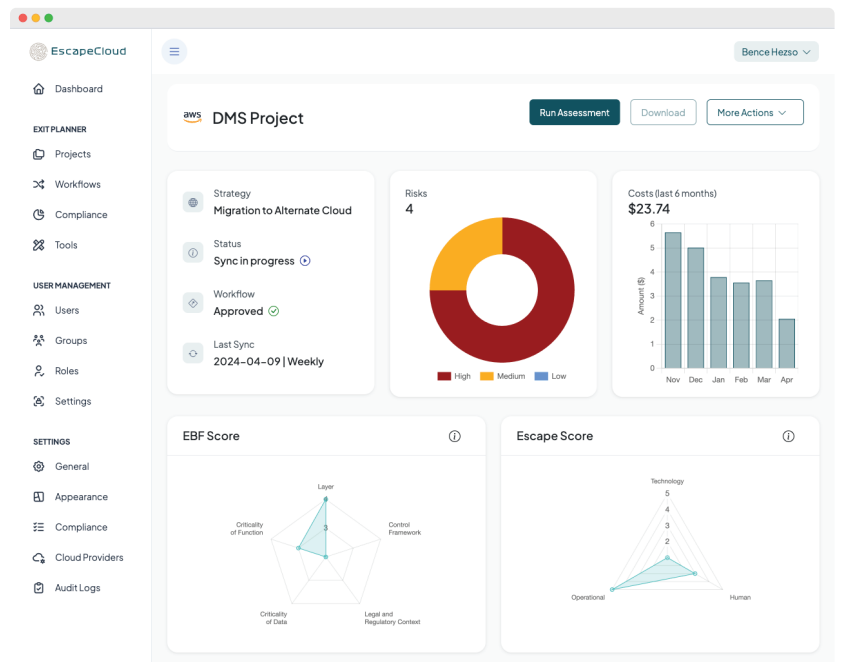
EscapeCloud - Unified Cloud Exit Assessment Solution

Seamlessly Navigate the Cloud with Regulatory Confidence

EscapeCloud is an autonomous cloud exit assessment solution specifically designed to revolutionize how financial institutions prepare cloud exit strategies and plans.

Key use cases

- Develop cloud exit strategies and plans for your cloud workloads
- Identify and mitigate the risks associated with your cloud workloads
- Ensure continuous compliance for your organization
- Assess infrastructure-as-code for risks associated with your cloud provider dependencies



What makes EscapeCloud different



You don't deploy it, you just connect it

EscapeCloud performs assessments using the cloud service providers' API, eliminating the need to deploy agents or sidecars.



Patented technology

EscapeCloud cloud exit assessment solution has been filed for patenting with the US Patent and Trademark Office and is currently under review.

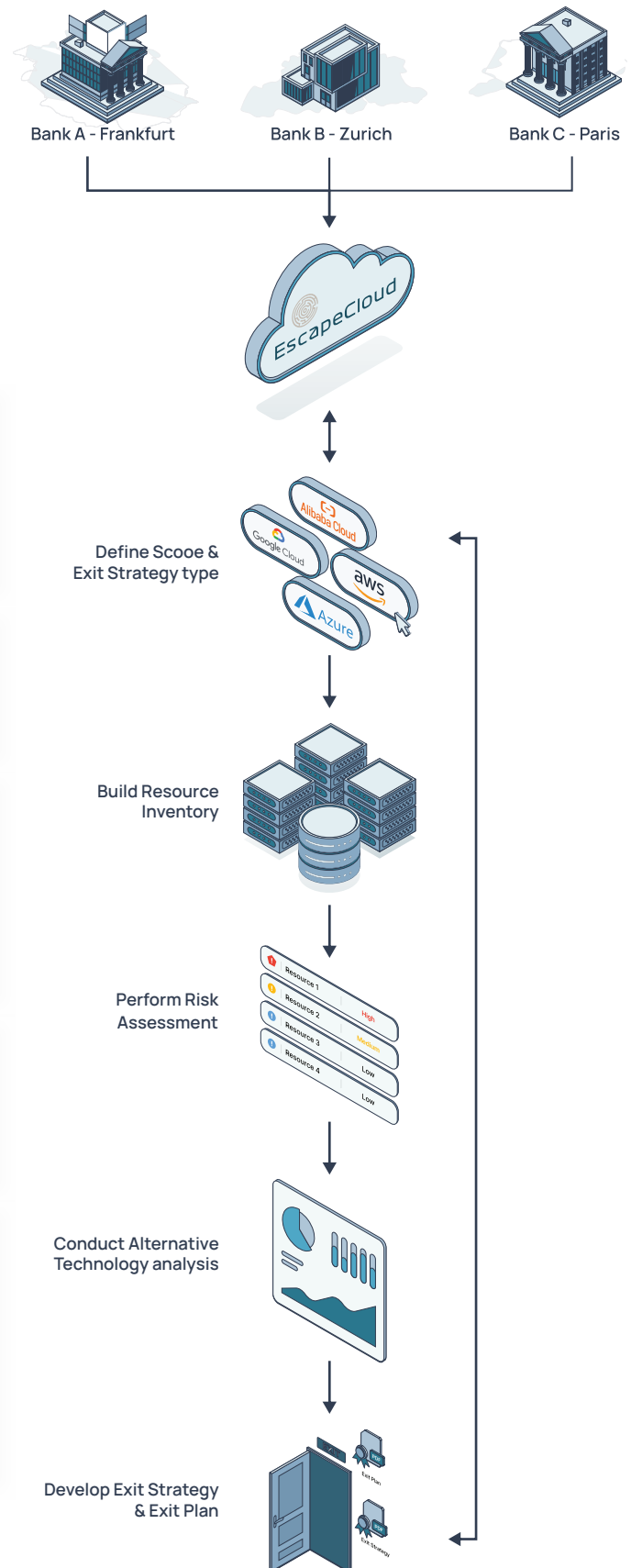


Total coverage of your cloud landscape

EscapeCloud is designed to support organizations adopting a multi-cloud approach, ensuring comprehensive coverage across various cloud platforms.

The first cloud exit assessment solution in the world

EscapeCloud is a sophisticated Software-as-a-Service (SaaS) solution specifically tailored for financial institutions, providing seamless and automated cloud exit assessment compliant with European Banking Authority (EBA) and national regulatory bodies requirements. Our solution empowers financial institutions to effectively leverage cloud service provider outsourcing while ensuring robust development of cloud exit strategies and plans.



01 Define Scope and Exit Strategy Type: Users are required to determine the assessment's scope, which involves selecting the cloud service provider in use (such as AWS, Azure, etc.) and setting the cloud connect credentials. Additionally, they must choose the appropriate type of exit strategy and specify the frequency of the assessment.

02 Build Resource Inventory: Based on the defined scope and frequency, the worker nodes iterate through the resources and services in use, collecting metadata to construct a Resource Inventory.

03 Perform Risk Assessment: Utilizing the Resource Inventory, the worker nodes conduct a risk assessment with a predefined rule set. This process categorizes the associated risks of the utilized resources and services into three levels: High, Medium, and Low. The baseline rule sets are continuously fine-tuned and updated to reflect market best practices.

04 Conduct Alternative Technology Analysis: Utilizing the Resource Inventory and the defined exit strategy type, the worker nodes query the alternative technologies dataset. This supports the selection of potential alternatives and aids in planning the transition.

05 Develop Exit Strategy and Exit Plan: Based on the assessment results, users have the option to download various reports, such as the Executive Summary, Exit Strategy, and Exit Plan. These reports are designed to assist different stakeholders in understanding the project's cloud exit process. Additionally, the reports can be customized to align with the organization's branding and are furnished with a digital signature and timestamp for authentication.

i It's important to note that the Cloud Exit Assessment only gathers metadata from the cloud service provider, without storing, replicating, or utilizing any client data on the cloud infrastructure.