

FINANCIAL SERVICES**CASE STUDY****CREDIT EUROPE BANK**

Mitigating the risk of insider threats
with IAM

OVERVIEW

- ▶ **Challenge:** Credit Europe Bank needed control over who had access to what in their system, and visibility of this for audit.
- ▶ **Process:** Inragen implemented an identity management solution to improve the bank's governance.
- ▶ **Outcome:** Implementation of an IAM system, including automatic access provisioning and segregation of duties.
- ▶ **Future:** Ongoing partnership between Credit Europe Bank and Inragen for training and upskilling and a future-proof system.

**ABOUT CREDIT EUROPE BANK**

Headquartered in the Netherlands, Credit Europe Bank is trusted by global customers to provide financial services such as international trade and commodity finance. Established in 1994, the Bank operates in nine countries with over one thousand employees and 36 branches.



“

For me there are two items that are very important: trust and relationship. Inragen deliver them both.

Head of Operational Risk Management and Information Security, Credit Europe Bank

”

WHY DID CREDIT EUROPE BANK WANT TO IMPLEMENT AN IAM SOLUTION?

Banks and other financial services organisations are always a **target for hackers** due to the nature of the data and assets held within the IT systems.

Credit Europe Bank were particularly concerned about controlling access to their systems to **mitigate the risk of a breach**.

Access control can be **simplified** and **automated** with an IAM solution, eliminating the **risks associated with manual tasks**, and providing a **clear overview** for internal requirements and external **audit** reports.

User experience does not have to be compromised either. Intragen implements leading identity security solutions to achieve **secure IT architecture** while maintaining a **smooth end-user experience**.

- Reduce the risk of insider threat**
- End-user experience**
- Good governance**
- Overview of access rights**
- Access control**
- Audit reporting**

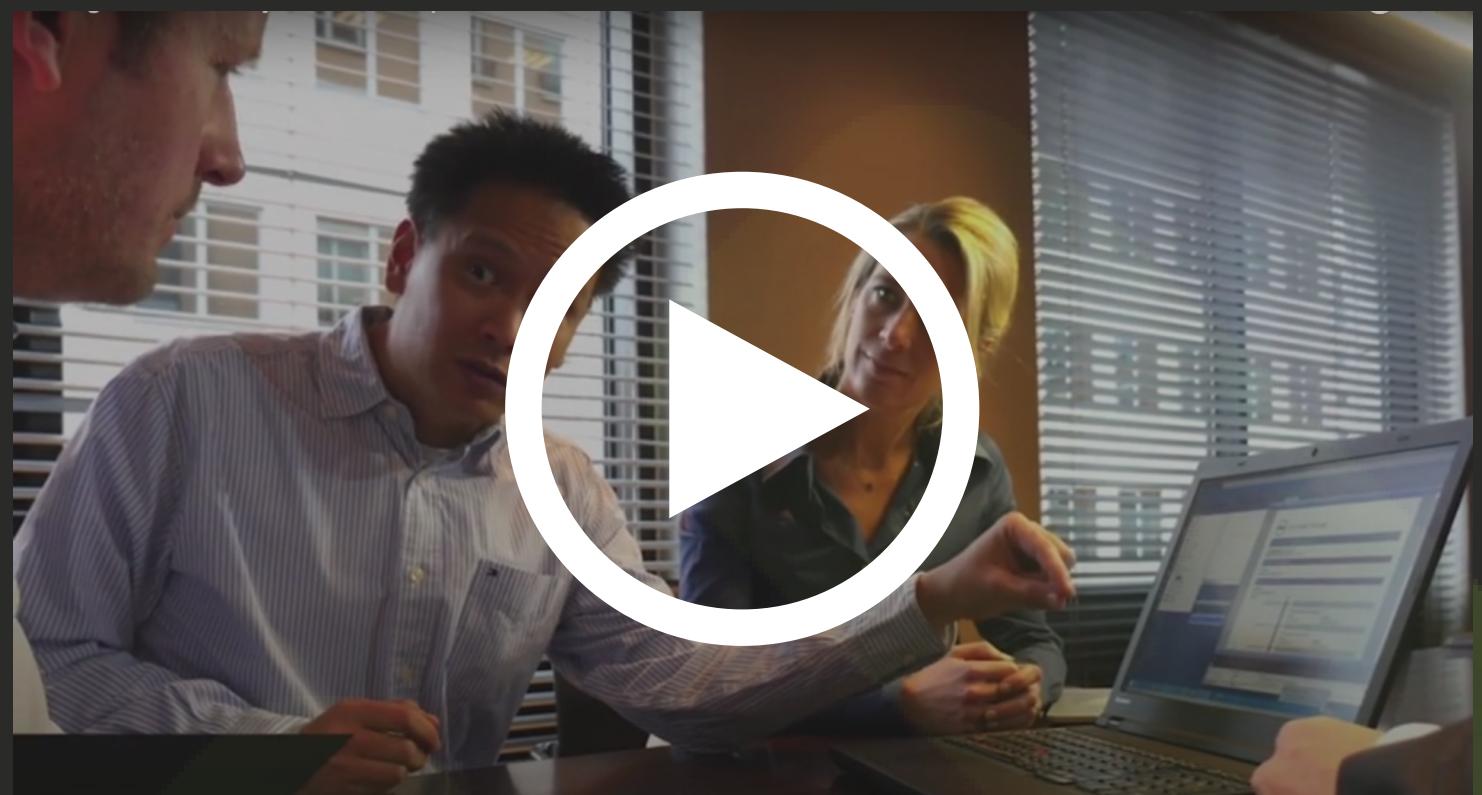
ACCESS CONTROL FOR FINANCIAL SERVICES ORGANISATIONS

Access, Request and Approval

One of the biggest challenges for Credit Europe Bank was **access control** and **visibility** of who had access to what in their IT systems.

Defining and structuring access is fundamental for both internal **security** and external **audit** and **regulation**. Once access groups have been defined in a security store such as **Active Directory**, the access structure is based off group membership.

An Identity Governance system provides additional metadata so that the people requesting and approving access can both have clarity on the access request. Define your application and its access rights (which will be provisioned as groups) with **clear ownership, descriptions and risk information**. Then you can specify the **approval workflow** and who the **approvers** should be.



Watch the case study with Credit Europe Bank

Role-Based Access Control

Financial services organisations can have **thousands of access rights** to their applications and infrastructure. For an end-user trying to request access or an approver reviewing requests, such high volume can lead to **error** or **over-approving**.

Defining a collection of access rights based on roles (such as Financial Advisor) **reduces the volume of requests** that require approval, facilitating a more **diligent decision** from approvers.

To find out more about Intragen's offerings and how we could help your organisation with identity and access governance and security, [contact one of our team today](#).