CYBERFORT FINANCE PILOT

PILOT STORY

From Compliance to Continuous Cyber Resilience

How Dealio used CYBERFORT to transform Cyber Resilience Act readiness, cybersecurity governance and risk management into a continuous operational process for a fintech / finance-sector environment.

Fintech / Finance Pilot Context

Dealio participated in the CYBERFORT Finance Pilot to evaluate how integrated cybersecurity, governance and compliance capabilities can support a fintech organisation operating in a regulated financial-services environment.

As a finance-sector pilot partner, Dealio focused on practical CRA readiness activities that connect assets, risks, controls, policies, assessments and evidence into a coherent operational workflow.

The pilot demonstrated how CYBERFORT can support fintech SMEs in moving from periodic compliance preparation towards continuous cyber resilience, structured risk governance and stronger visibility across security and compliance activities.

Finance-sector relevance: the pilot validated CYBERFORT capabilities in a fintech context where regulatory readiness, secure operations and evidence-based governance are essential.

FINANCE-SECTOR VALUE

- CRA readiness
- Governance visibility
- Risk prioritisation
- Evidence traceability
- Continuous monitoring

CHALLENGE

Balancing innovation, cybersecurity, regulatory duties, operational resilience and CRA readiness.

SOLUTION

An integrated GRC workflow for assessments, risks, controls, policies and evidence management.

IMPACT

A practical move from periodic compliance to continuous cyber resilience for finance-sector SMEs.

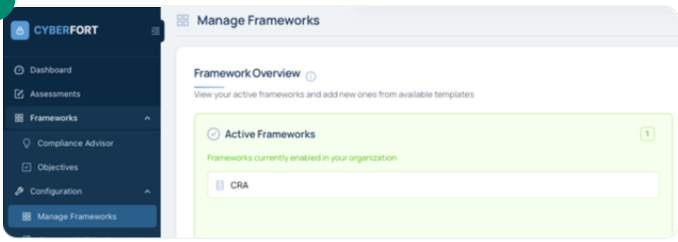
> CYBERFORT demonstrated how cybersecurity governance, technical validation and regulatory readiness can be managed through a single operational framework.
>
> **Dealio Pilot Team**

CYBERFORT IN ACTION

Governance, Risk and CRA Readiness

CRA Framework → Asset Registration → Risk Management → Controls Management → CRA Assessment → Continuous Monitoring

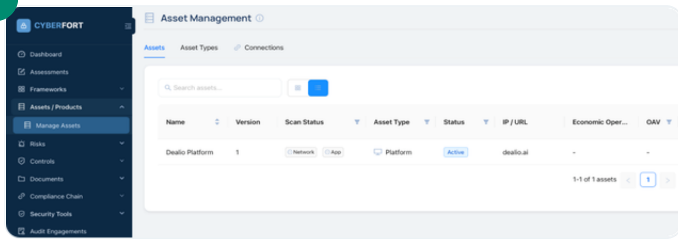
1



CRA Framework

Define and structure CRA obligations, requirements and compliance scope.

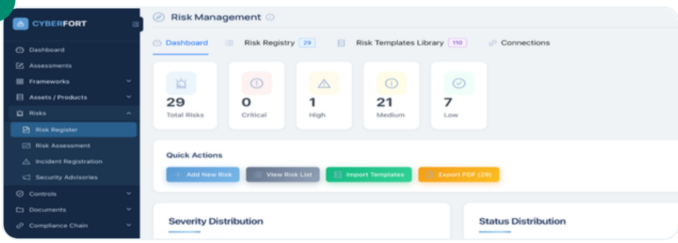
2



Asset Registration

Maintain a complete inventory of assets, systems and third-party components.

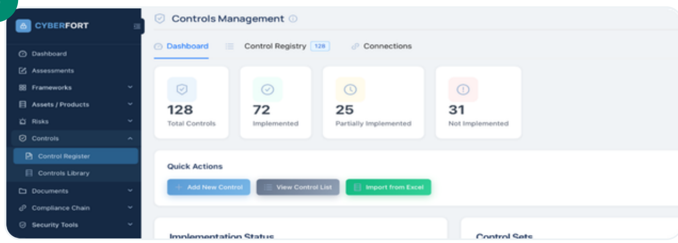
3



Risk Management

Assess, prioritise and track risks with clear ownership and mitigation planning.

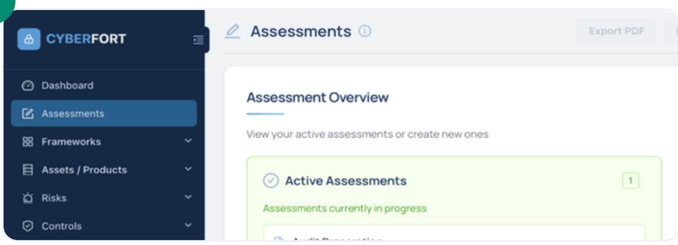
4



Controls Management

Implement and monitor controls to strengthen governance and security maturity.

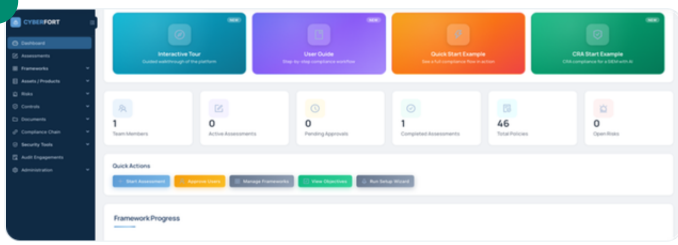
5



CRA Assessment

Run structured assessments and measure CRA readiness across the organisation.

6



Continuous Monitoring

Central visibility across assessments, policies and compliance status.

KEY ACHIEVEMENTS

- CRA readiness assessment completed.
- Centralized visibility across assets, risks and controls.
- Governance and compliance workflows operationalized.
- Improved traceability and evidence management.
- Secure-by-design awareness strengthened.

LOOKING AHEAD

- Continuous monitoring and recurring assessments.
- Automated compliance evidence collection.
- Integration of validation into development workflows.
- Further evaluation of selected CYBERFORT capabilities.

For SMEs in regulated sectors, the Dealio pilot shows how cybersecurity, compliance and resilience can become part of everyday operations instead of isolated audit exercises.