CHARLI

THE ANCAEUS CONTROL PLANE

PEOPLE / DATA / CONTROLS / PROOF

SENSITIVE DATA
CONTROL
ACCOUNTABILITY
REGULATORY
CONFIDENCE

OSFI CAPABILITY BRIEF

Operationalizing Data Control and Evidence for OSFI

How CharliAI helps federally regulated financial institutions move from policy statements to enforceable controls, accountable workflows, and defensible proof.

> **Trust is forensic proof.**

FROM
POLICY
TO PROOF



OSFI scrutiny around sensitive data is increasing, especially where legacy production data remains in UAT, test and other enterprise environments, where approvals and exception handling are manual, and where institutions cannot easily demonstrate operational evidence. CharliAI helps institutions turn governance into execution by applying runtime controls, monitoring data handling, and producing evidence that controls actually operated.

Why institutions are feeling pressure now

- Sensitive data remains in UAT, test and other enterprise environments longer than intended
- Data handling approvals and exceptions are often managed manually
- Control execution is fragmented across teams, systems and vendors
- Institutions can describe policy, but struggle to prove operational evidence
- Supervisory findings increasingly focus on governance, protection and remediation

What OSFI is signaling

B-13

Institutions should identify, classify and protect structured and unstructured data, and perform periodic discovery scans to detect deviations from standards and controls.

E-21

Effective data risk management requires governance, lineage, classification, protection, and response processes throughout the data lifecycle.

Integrity & Security

Sensitive data should be protected at rest, in transit and in use, with controls and escalation mechanisms for unauthorized access.

Where CharliAI creates immediate value

Discover and classify

Surface sensitive information and apply policy-driven handling requirements across workflows and environments.

Protect and remediate

Support anonymization, masking or tokenization, encryption, and protected handling patterns to reduce sensitive-data exposure across production and non-production environments.

Authorize and control

Apply delegated approvals, conditional access, and human checkpoints where policy requires them.

Trace and prove

Capture forensic traces, evidence of decisions, exceptions, and auditable records that support regulatory reporting documentation.

Ideal for enterprise data remediation, sensitive data governance, protection controls, exception management, and regulatory evidence programs.

Aligned to OSFI Guideline B-13, Guideline E-21, Integrity and Security, and supports preparation for Guideline E-23 where data and model governance intersect.

CHARLI AI

THE ANCAEUS CONTROL PLANE

PEOPLE / DATA / CONTROLS / PROOF

SENSITIVE DATA CONTROL ACCOUNTABILITY REGULATORY CONFIDENCE

OSFI CAPABILITY BRIEF

Turning OSFI Expectations into Operating Control

A practical control-plane approach for sensitive data governance, enterprise data remediation, deep enterprise integration, and defensible regulatory evidence.

FROM POLICY TO PROOF

Many institutions already have policies, tools and review processes in place. The challenge is operational consistency. CharliAI connects approvals, policy conditions, runtime control, exception handling, protection workflows, and evidence into a single accountable operating layer.

Capability alignment

OSFI pressure point	CharliAI capability	Operational outcome
Identify, classify and protect sensitive data	Policy-driven data controls, protected data handling, runtime enforcement, and integration with existing protection technologies	Consistent control of sensitive information across business processes and environments.
Sensitive data across production, UAT and test environments	Conditional access, anonymization and remediation workflows, exception tracking, and accountable approvals	Reduced exposure and clearer governance across enterprise data use.
Limited lineage and weak evidence of process	Forensic traces, audit replay, evidence packages, and regulatory reporting documentation	Demonstrable proof that controls operated and exceptions were governed.
Manual exception handling and fragmented accountability	Delegated authorization, human-in-the-loop checkpoints, and role-based decision control	Clear ownership, governed overrides, and traceable accountability.
Slow detection of deviations or risky handling	Active surveillance, alerts, behavioral monitoring, and intervention triggers	Faster remediation and stronger operational resilience.

High-priority use cases

- Non-production environment remediation
- Sensitive data handling across AI and workflow automation
- Exception approval and evidence management
- Legacy data minimization and controlled access

Deep integration with the enterprise stack

CharliAI works with existing security, data, workflow, and oversight investments rather than replacing them. CharliAI complements DLP, masking/tokenization, encryption, IAM, workflow, and audit processes.

Microsoft Azure & Fabric	Microsoft Purview	Snowflake
Databricks & Unity Catalog	SIEM / SOC / GRC tooling	Regulatory reporting & documentation

A focused engagement path

1 Assess
Identify pressure points, sensitive data exposure, approval gaps, integration points, and evidence weaknesses.

→

2 Instrument
Apply control points, approval logic, protection workflows, monitoring, and traceability in the target workflow.

→

3 Prove
Produce defensible evidence, accelerate remediation, support reporting, and expand to adjacent use cases.

Start with a targeted OSFI Data Control & Evidence Workshop. CharliAI helps Canadian institutions bridge the gap from written policy to controlled execution, sovereign data & AI handling, and defensible proof. [charliai.com]

Aligned to OSFI Guideline B-13, Guideline E-21, Integrity and Security, and supports preparation for Guideline E-23 where data and model governance intersect.