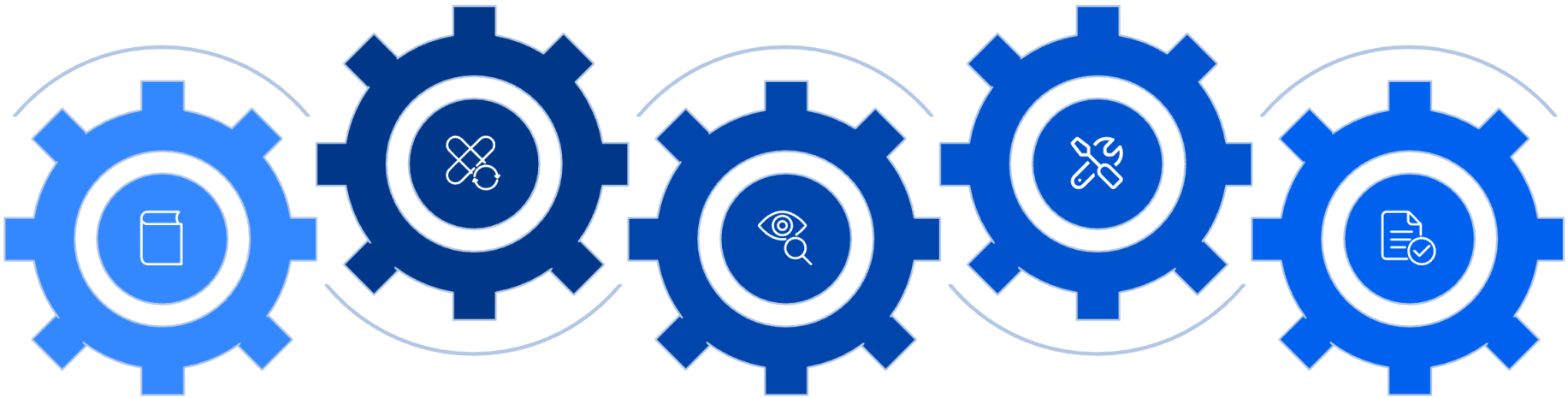
IBM Z Security and Compliance Center (zSCC)

Audit Readiness Challenges

Mapping regulatory requirements to IBM Z controls can be complex

Limited Z skills to understand and fix compliance gaps



Regulatory compliance requirements are evolving rapidly

Discovering and classifying sensitive data in alignment with regulatory standards

System modifications can make previously extracted compliance evidence obsolete.

IBM Z Security and Compliance Center Key Features

Reduce the audit preparation time

Pre-built Profiles

Easily manage audit and regulatory frameworks with pre-configured profiles mapped to leading industry standards like PCI-DSS, NIST, DORA & STIG

Interactive Dashboards

Gain real-time insights into your Z Systems' compliance and security posture through dynamic and customizable dashboards.

Audit Reporting

Generate detailed, exportable reports (PDF/XLS) aligned with industry standards and organizational requirements, significantly reducing audit preparation time.

Custom Goals

Define unique technical checks specific to your organization's requirements, integrating them into profiles for tailored validation scans.

Continuous Compliance

Move beyond point-in-time assessments with historical score tracking, trend visualization, and early warning systems for compliance drift.

IBM Concert Integration

Seamlessly provide zSCC compliance scan results to IBM Concert, providing a unified operational view across mainframe and distributed environments.

Supported Profiles

Payment Card Industry Data Security Standard (PCI-DSS)

Typical industries:

- Banking
- Financial
- Insurance
- Retail

DISA Security Technical Implementation Guides (STIGs)

Typical industries:

- Federal Government
- Local Government
- Banking
- Financial

Center of Internet Security (CIS) Benchmarks

Typical industries:

- Banking
- Financial
- Insurance
- Retail

Digital Operations Resilience Act (DORA)

Typical industries:

- Banking
- Financial
- Insurance
- Retail

National Institute of Standards & Technology (NIST)

Typical industries:

- Federal Government
- Local Government

Custom

ZSCC allows the client to create their own custom profiles leveraging existing goals that come with the product.

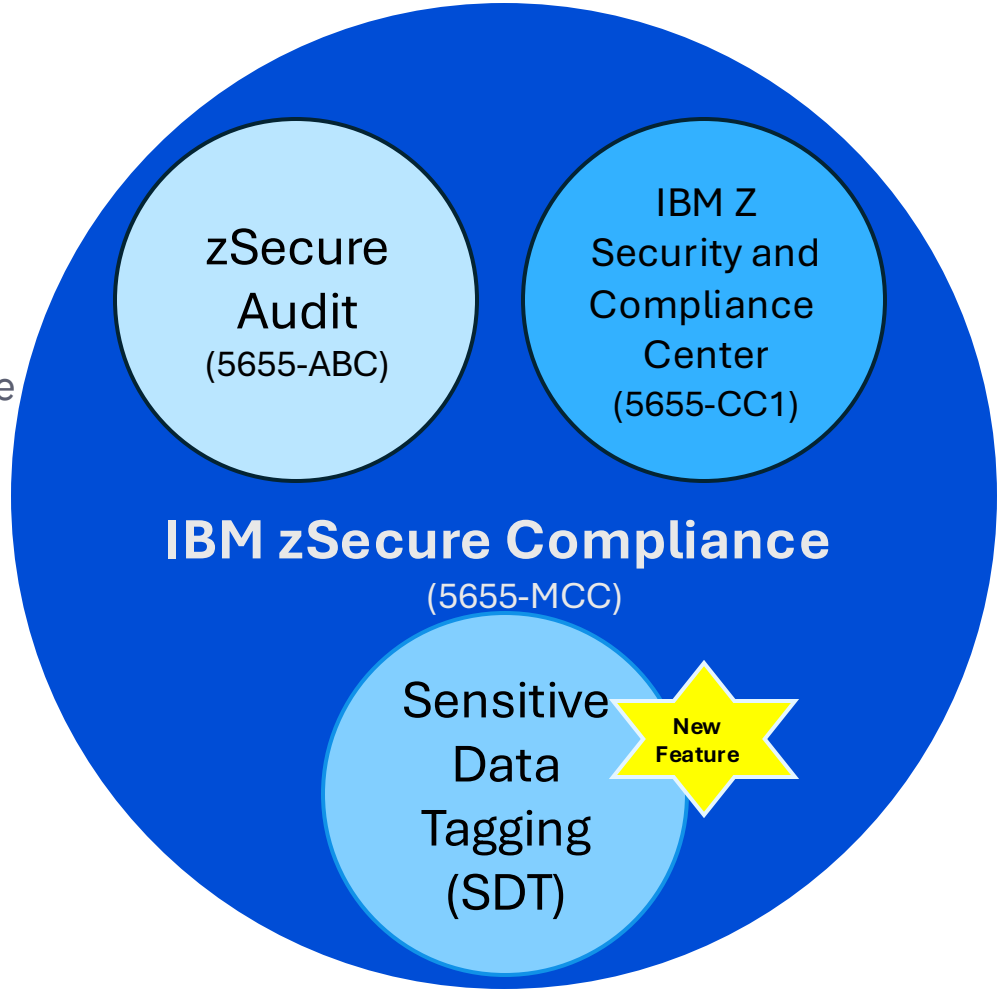
Typical industries:

- Any

IBM zSecure Compliance

Introducing IBM zSecure Compliance 3.2
(PID – 5655MCC)

- ✓ Converges compliance elements of IBM zSW Security portfolio
  - All features of IBM zSecure Audit and IBM Z Security and Compliance Center (zSCC) are included
- ✓ Includes new AI-Powered feature for the discovery and classification of sensitive data called Sensitive Data Tagging (SDT)*
  - leverages the z17/z16 Telum AI Accelerator and Watson Natural Language Processing for enhanced performance and precision
- ✓ Single Entitlement
- ✓ Seamless Transition with little need for process re-engineering
- ✓ Trade-up option for existing zSecure Audit and zSCC customers
- ✓ IBM zSecure Audit and IBM Z Security and Compliance Center EOM 1Q2026
  - Future compliance enhancements will be made available via the IBM zSecure Compliance offering



* Initial release supports DB2; Future enhancements will include support for other datasets including IMS and VSAM.

DEMO

Sensitive Data Tagging (SDT)

IBM Z Telum AI Accelerator

Hardware-accelerated, faster classification.

Watson Natural Language Processing Capabilities

Context-aware, multi-language, continuous learning for high accuracy.

All data remains securely on the mainframe

Complete processing occurs within the z/OS security boundary, including metadata. SDT Scan results are encrypted and access controlled

Uniquely combines the unmatched performance of the mainframe with the intelligence of AI to deliver exceptional accuracy. It's the only approach that enables automated compliance — without ever compromising data security.

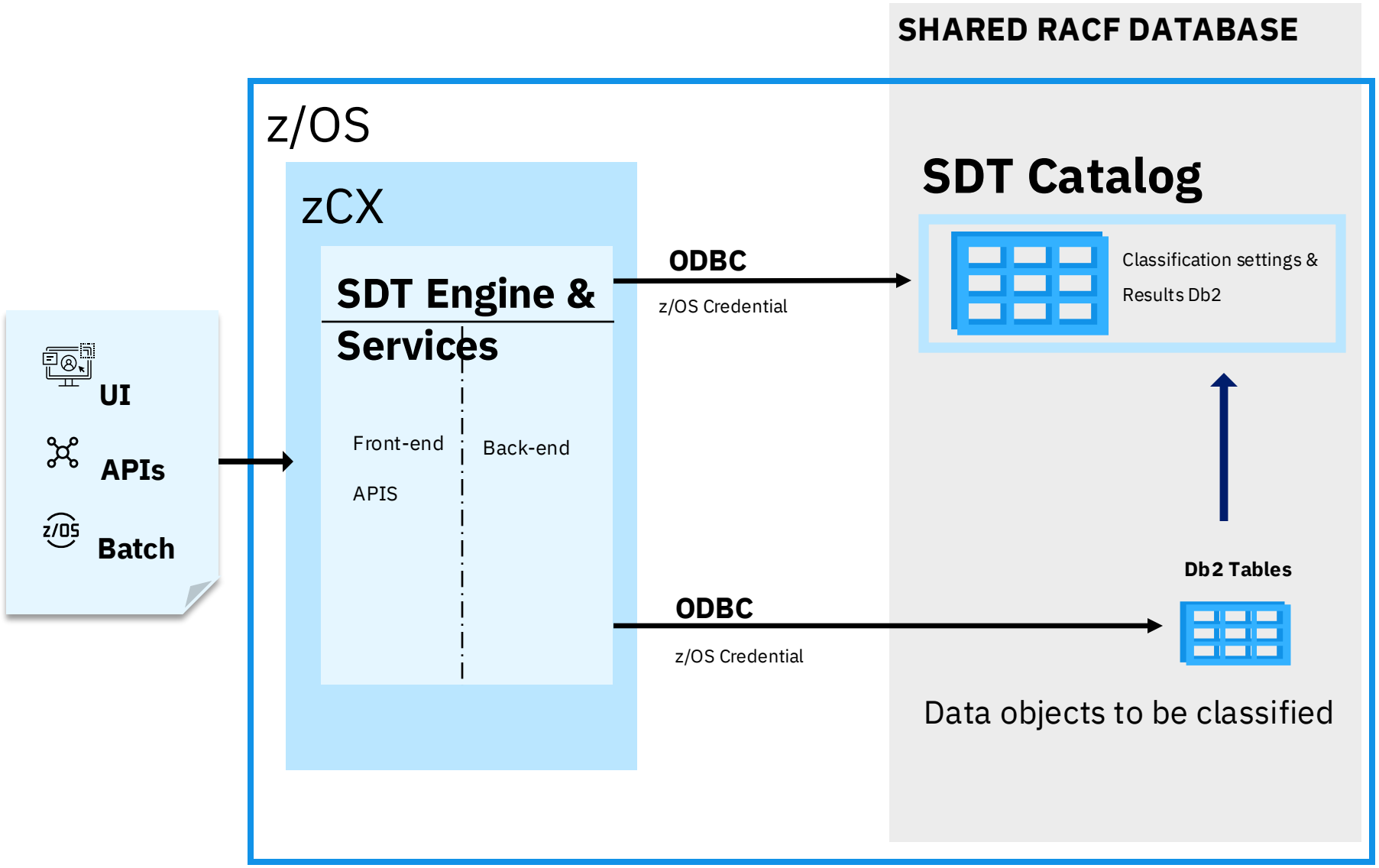
Note – At GA release SDT supports DB2 dataset only; Future enhancements will include support for other datasets including IMS and VSAM.

SDT:

Security Consideration

Preference:

Centralized authentication and authorization management via z/OS - Centralized Audit and Monitoring



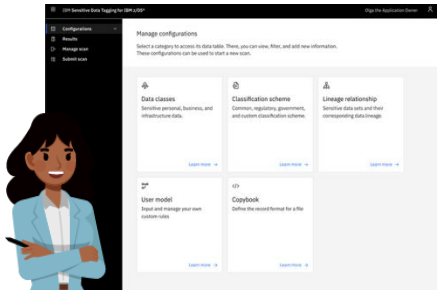
SDT User Flow

Olga –Line of Business Owner

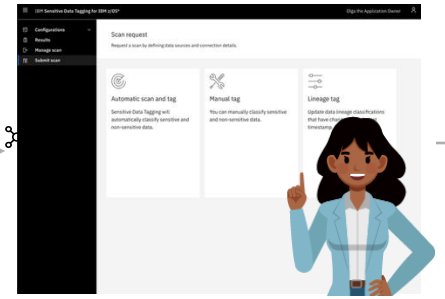
Olga owns the application that handles customer credit card information and is preparing for an upcoming compliance audit. She wants to ensure that all cardholder data within her application is correctly classified according to PCI-DSS standards.

To achieve this, she:

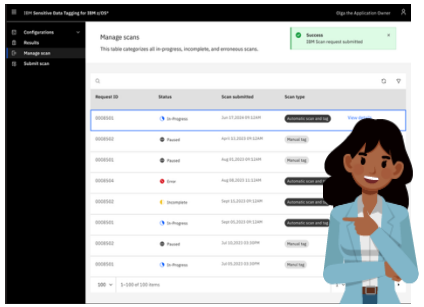
- Reviews the pre-defined data classes and classification Scheme PCI-DSS
- Submits an SDT scan to identify any unclassified sensitive data that needs protection.



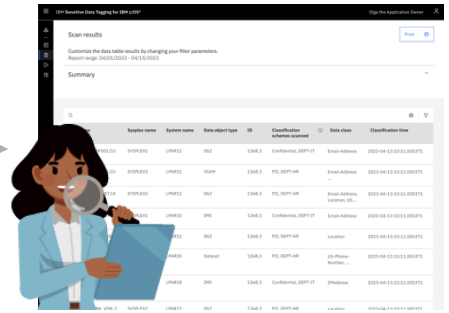
Reviews pre-defines data classes and classification schemes to be identified



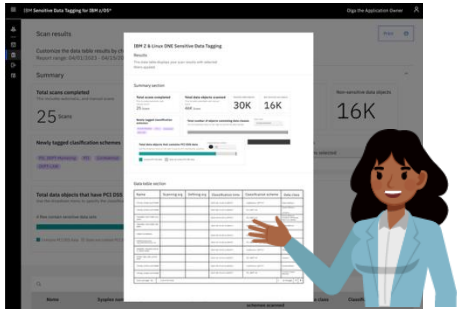
A scan request is submitted - sensitive data is automatically identified



Scan results and evidence are stored in the SDTz catalog



Reports are generated to identify where sensitive data resides. Reports are distributed to security admins.



Security Admin quickly understands where sensitive data resides. Results in SDTz catalog can be viewed and extracted for compliance auditing.

DEMO