Auditing and Protecting your z/OS environment

Guardium for IMS with IMS Encryption

Roy Panting
Guardium for System z Technical Sales Engineer
March 17, 2015

IMS Technical Symposium 2015

Agenda

Audit requirements are evolving

How to protect sensitive data

Database Activity Monitoring for IMS

Encryption for IMS

Summary

Audit requirements are changing

Auditing is evolving

Auditing is advancing from nice to have to must have

Many factors are driving the evolution

The requirement for encryption is also advancing

How can you stay ahead of the compliance curve

How to protect sensitive data

Protecting sensitive data is easy….

We use RACF or a similar access control program

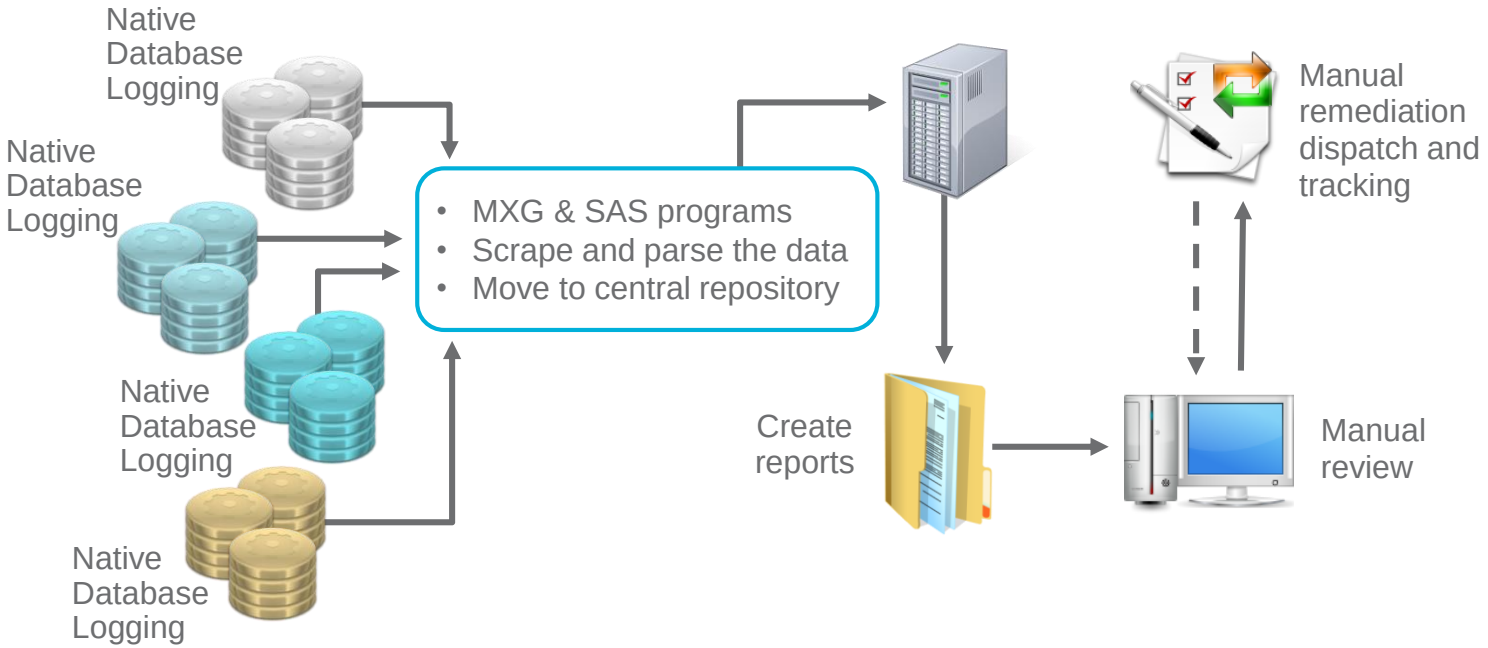
Only authorized people can access applications and data

There are logs generated for security reviews

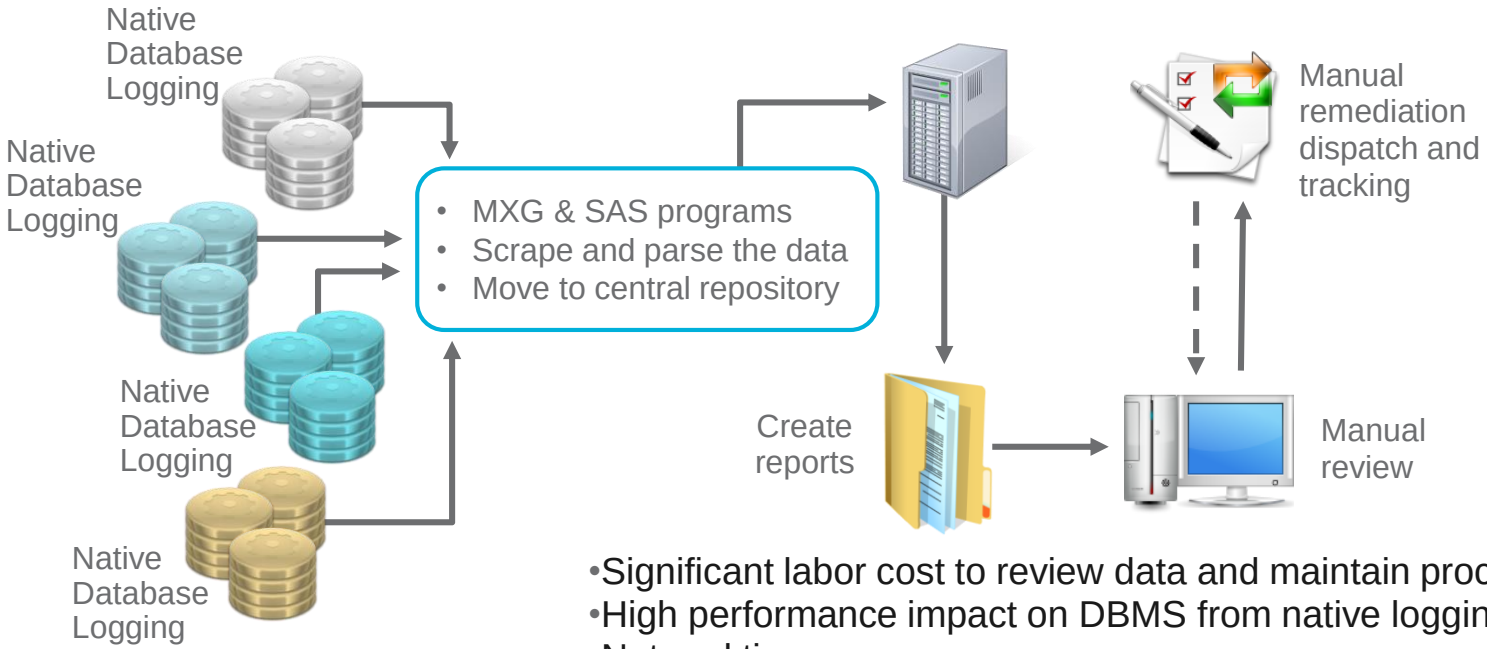
We have trust in our staff

We have never had a problem

Custom built auditing solution



Custom built auditing solutions – are costly

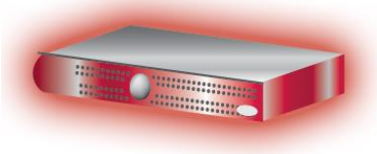


- Significant labor cost to review data and maintain process
- High performance impact on DBMS from native logging
- Not real time
- Does not meet auditor requirements for Separation of Duties
- Audit trail is not secure
- Inconsistent policies enterprise-wide

Database Activity Monitoring for IMS

IMS Technical Symposium 2015

Guardium for System z - Components



- **Guardium Collector appliance for System z**
  - Securely stores audit data collected by mainframe S-TAP
  - Provides analytics, reporting & compliance workflow automation
  - Integrated with Guardium enterprise architecture
- **S-TAP (for DB2, IMS or Data Sets) on z/OS event capture**
  - Mainframe Software Tap (STAP)
  - Collects audit data for Guardium collector
  - Collection profiles managed on the Guardium collector
  - Enabled for zIIP processing
  - Audit data streamed to the collector

Guardium Database Activity Monitoring Overview

- Helps to lower the costs and risks of compliance, security and audit — using proven z/OS technology.
- Monitors and audits IMS, DB2 on z/OS, VSAM and Non-VSAM activity by privileged users, objects, and many more fields.
- Provides visibility at a granular level into critical operations, including reads, data and structural changes.
- Performs all analysis, reporting and storage of audit data off-mainframe in a secure environment.
- Can be used for mainframe environments only, or deployed enterprise-wide to provide a unified security and compliance solution for both mainframe and distributed database environments.

Guardium IMS audit data sources

1. IMS Online regions (DLI Online and DLI Batch)
   - Accesses to databases and segments including INSERT, UPDATE, DELETE, and GET
   - Obtain concatenated key and segment data
   - Links Get Hold and Replace calls which enables before and after images of UPDATED segments
2. IMS DLI/DBB batch jobs
   - Accesses to databases and segments including INSERT, UPDATE, DELETE, and GET
   - Obtain concatenated key and segment data
   - Links Get Hold and Replace calls which enables before and after images of UPDATED segments

Guardium IMS audit data sources

3. System Management Facility (SMF) collector (*)
   - Access to database, image copy and RECON data sets and security violations
4. IMS (SLDS) Archived Log data set (*)
   - IMS Online region START and STOP, database and PSB change of state activity and USER sign-on and sign-off

(*) Using this collector is optional

Guardium S-TAP for IMS Collection Activity

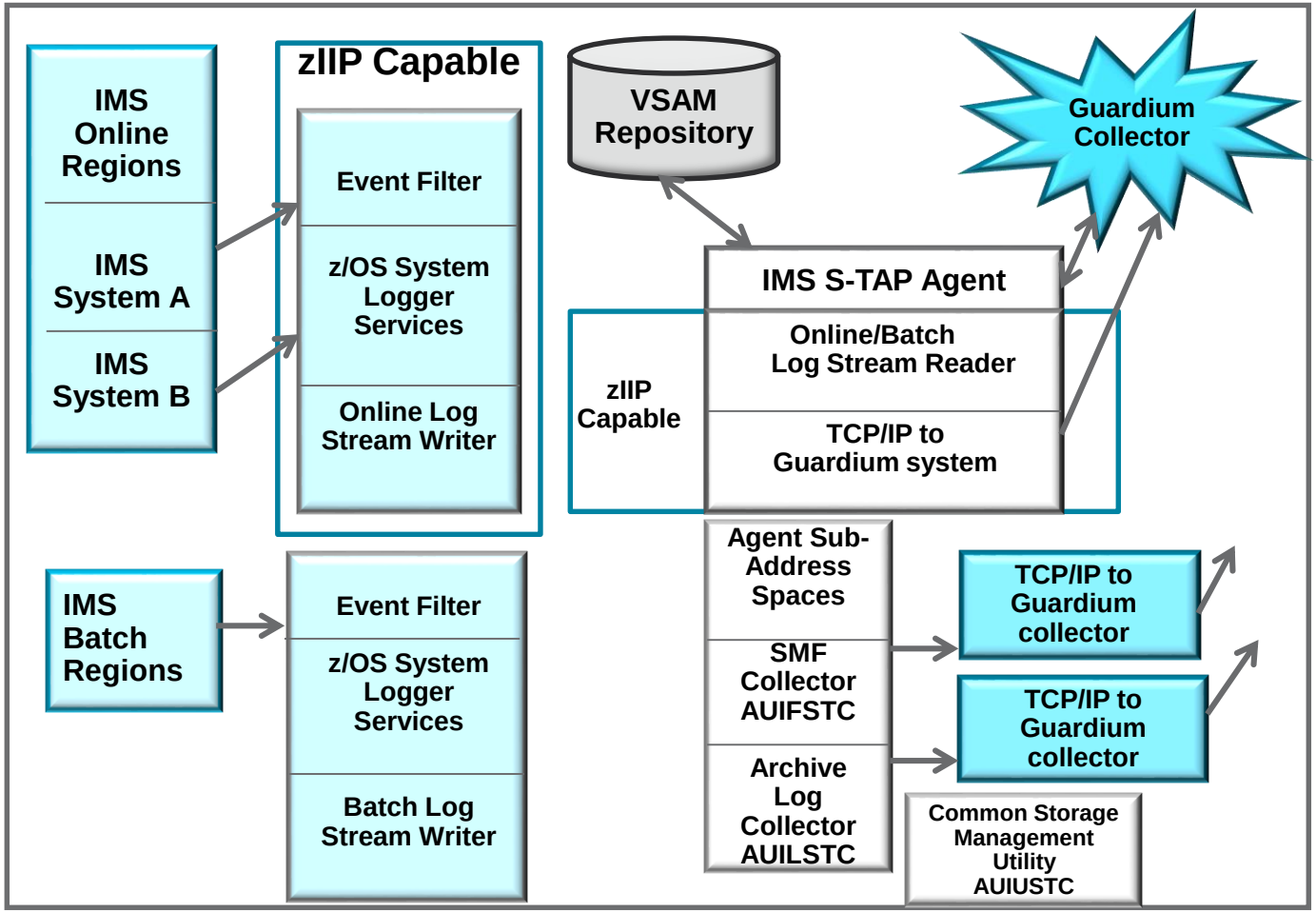
- S-TAP for IMS's function is to collect Audit information of access to IMS Databases and IMS artifacts
- Complete flexibility over which calls to audit per target. For example: all databases, all segments, one database and one segment of the database.
- Each segment can have different calls audited
- When a call is to be audited, the relevant information is gathered including:
  - Call type, userid, PSB name, DBName, Segment Name, etc.

What “non-IMS” Data is Collected?

Access to IMS related information outside the control of IMS services including:

- Database data sets
- Image copy data sets
- IMS Log data sets
- RECON data sets
- RENAMES: records and reports the original DSN and the new DSN
- User access to the IMS system via SIGNON and PSB and database (DBD) change of state activity as recorded in the IMS log
- Displayed as an EVENT with pertinent data (PSB name, DBD name, DBD name, USERID, etc.)

Guardium S-TAP for IMS V 9.1 Architecture



Sample IMS report

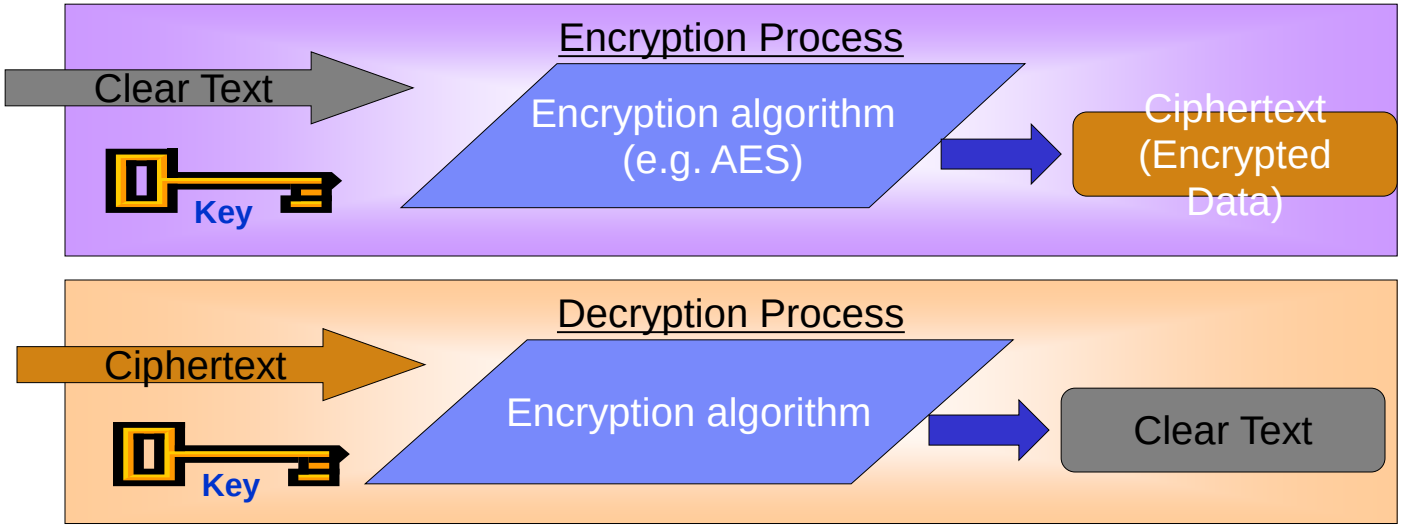
-RAP - IMS Data Access Details

Start Date: **2015-03-17 01:16:37** End Date: **2015-03-18 01:16:37**
Aliases: **OFF** ClientIP: **LIKE %**
Main Entity: **FULL SQL**

Timestamp	Client IP	Server Type	IMS/DATA SET Program Name	IMS Database	IMS Segment	IMS/DATA SET Context	IMS Transaction	IMS Terminal	IMS PCB Name
2015-03-17 14:43:53.0	9.39.68.147	IMS	DFSSAM07	DI21PART	PARTROOT	Segment Level GET	DSPALLI	DDS21620	DBPCB01
2015-03-17 14:43:53.0	9.39.68.147	IMS	DFSSAM07	DI21PART	STANINFO	Segment Level GET	DSPALLI	DDS21620	DBPCB01
2015-03-17 14:43:30.0	9.39.68.147	IMS	DFSSAM02	DI21PART	PARTROOT	Segment Level GET	PART	DDS21620	DBPCB01
2015-03-17 14:43:30.0	9.39.68.147	IMS	DFSSAM02	DI21PART	STANINFO	Segment Level GET	PART	DDS21620	DBPCB01
2015-03-17 14:43:17.0	9.39.68.147	IMS	DFSSAM04	DI21PART	STANINFO	Segment Level INSERT	ADDPART	DDS21620	DBPCB01
2015-03-17 14:43:17.0	9.39.68.147	IMS	DFSSAM04	DI21PART	PARTROOT	Segment Level INSERT	ADDPART	DDS21620	DBPCB01
2015-03-17 14:42:45.0	9.39.68.147	IMS	DFSSAM02	DI21PART	PARTROOT	Segment Level GET	PART	DDS21620	DBPCB01
2015-03-17 14:42:45.0	9.39.68.147	IMS	DFSSAM02	DI21PART	STANINFO	Segment Level GET	PART	DDS21620	DBPCB01
2015-03-17 14:42:24.0	9.39.68.147	IMS	DFSSAM07	DI21PART	PARTROOT	Segment Level GET	DSPALLI	DDS21620	DBPCB01
2015-03-17 14:42:24.0	9.39.68.147	IMS	DFSSAM07	DI21PART	STANINFO	Segment Level GET	DSPALLI	DDS21620	DBPCB01
2015-03-17 14:42:03.0	9.39.68.147	IMS	DFSSAM03	DI21PART	STANINFO	Segment Level GET	DSPINV	DDS21620	DBPCB01
2015-03-17 14:42:03.0	9.39.68.147	IMS	DFSSAM03	DI21PART	PARTROOT	Segment Level GET	DSPINV	DDS21620	DBPCB01
2015-03-17 14:41:41.0	9.39.68.147	IMS	DFSSAM04	DI21PART	STANINFO	Segment Level INSERT	ADDPART	DDS21620	DBPCB01
2015-03-17 14:41:41.0	9.39.68.147	IMS	DFSSAM04	DI21PART	PARTROOT	Segment Level INSERT	ADDPART	DDS21620	DBPCB01

Encryption for IMS

Encryption is a technique used to help protect data from unauthorized access



- Data that is not encrypted is referred to as “clear text”
- Clear text is encrypted by processing with a “key” and an encryption algorithm
  - Several standard algorithms exist, include DES, TDES and AES (next slide)
- Keys are bit streams that vary in length
  - For example AES supports 128, 192 and 256 bit key lengths

Common questions with data encryption

- What will be the performance overhead?
- How do we need to handle encryption Key management?
- Are application code changes required?

How is crypto invoked with the Data Encryption Tool?

- Crypto is invoked using an EDITPROC, for every row processed by any SQL Utility for DB2 or IMS
- Encrypted row same length as clear text row
- No application changes required
- One key per table or segment specified in the EDITPROC
- Can use Clear Key, Secure Key or Protected Key

Implementing IMS data encryption

- Configure the Integrated Cryptographic Service Facility (ICSF)*
- Enable CP Assist for Cryptographic Functions (CPACF)*
- Generate and store in the Cryptographic Key Data Set (CKDS) Key Labels
- Build the IMS User Exit or DB2 EDITPROC
- Back - Up and Unload Databases
- Create Exits for IMS
- Reload the Databases
- Validate the databases are encrypted

* This feature subject to US export restrictions

Encryption and Data at Rest Protection

- Encryption is a requirement for many data protection initiatives
- Main requirement is to protect data at rest to ensure only approved access with an approved business need-to-know will see the data in clear text.
- Accessing data directly will result in cyphertext which is no risk for the organization

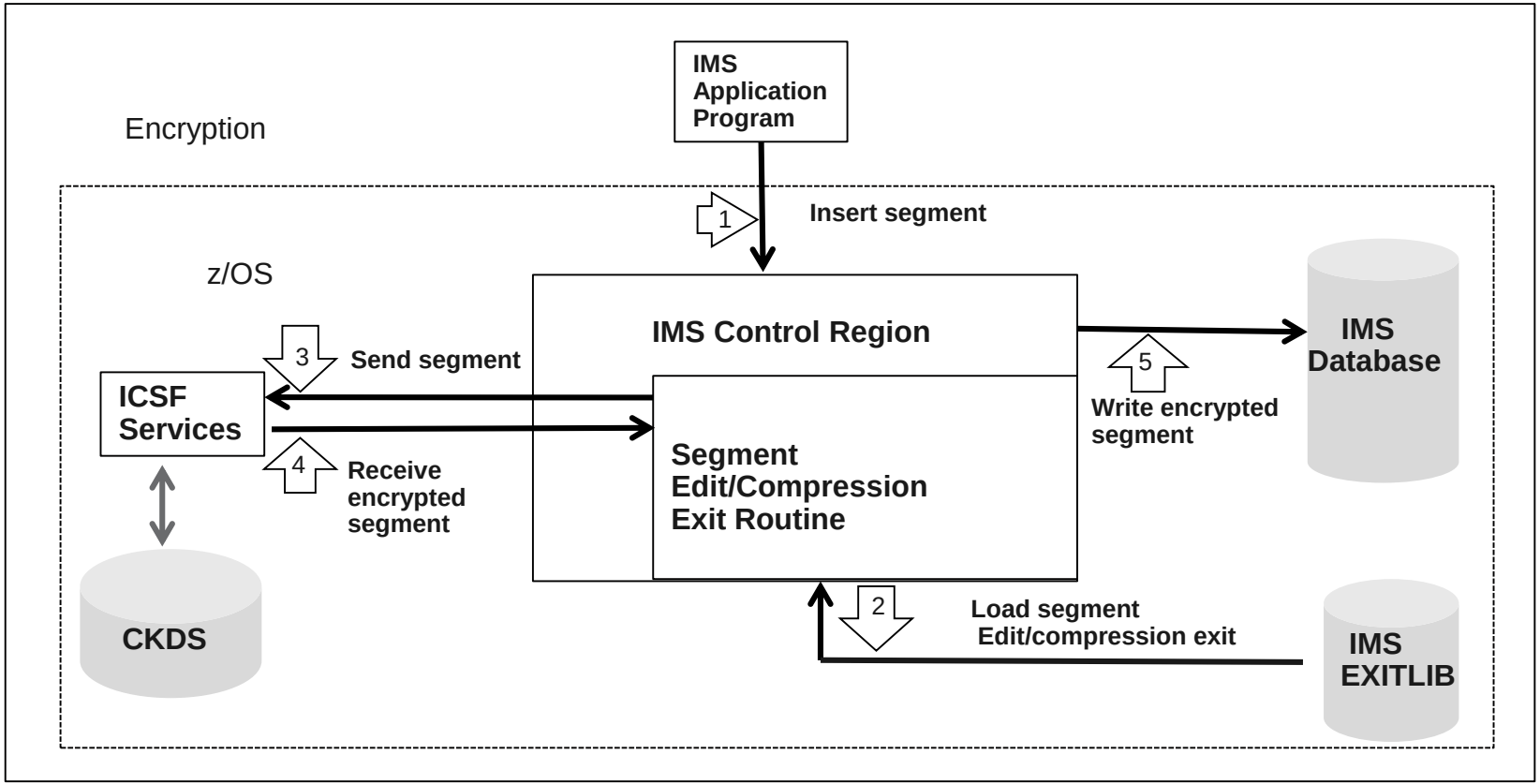
Encryption Algorithms – Which Ones Are Best?

- DES (Data Encryption Standard)
  - 56-bit, viewed as weak and generally unacceptable today by the NIST
- TDES (Triple Data Encryption Standard)
  - 128-bit, universally accepted algorithm
- AES (Advanced Encryption Standard)
  - 128- or 256- bit, strategic commercially used algorithm

Integrated Cryptographic Service Facility (ICSF)

- Provides: z/OS integrated software support for data encryption
- Operating System S/W API Interface to Cryptographic Hardware
  - CEX2/3C hardware feature for z114, z10 and z196
  - CEX4S hardware feature for z12BC and z12EC
  - CEX5S hardware feature for z13
- Enhanced Key Management for key creation and distribution including public and private keys, secure and clear keys and master keys
- Created keys are stored and accessed in the Cryptographic Key Data Set (CKDS) with unique key label
- CKDS itself is secured via Security Access Facility (SAF)

Encryption Flow for IMS



Summary

Auditing and protecting your z/OS environment

- Data breaches are a fact of life
- RACF is great, but not all inclusive
- Database activity monitoring provides insight into who did what and when
- Encryption removes the risk of non-authorized viewing of data
- Implementation of these tools has to be unobtrusive with minimal changes to the environment
- Where will you go from here?