USING AUDIT ANALYTICS IN IT INFRASTRUCTURE ENVIRONMENTS

1

Eckhardt Kriel C.A. (SA)
E Kriel & Associates Inc.
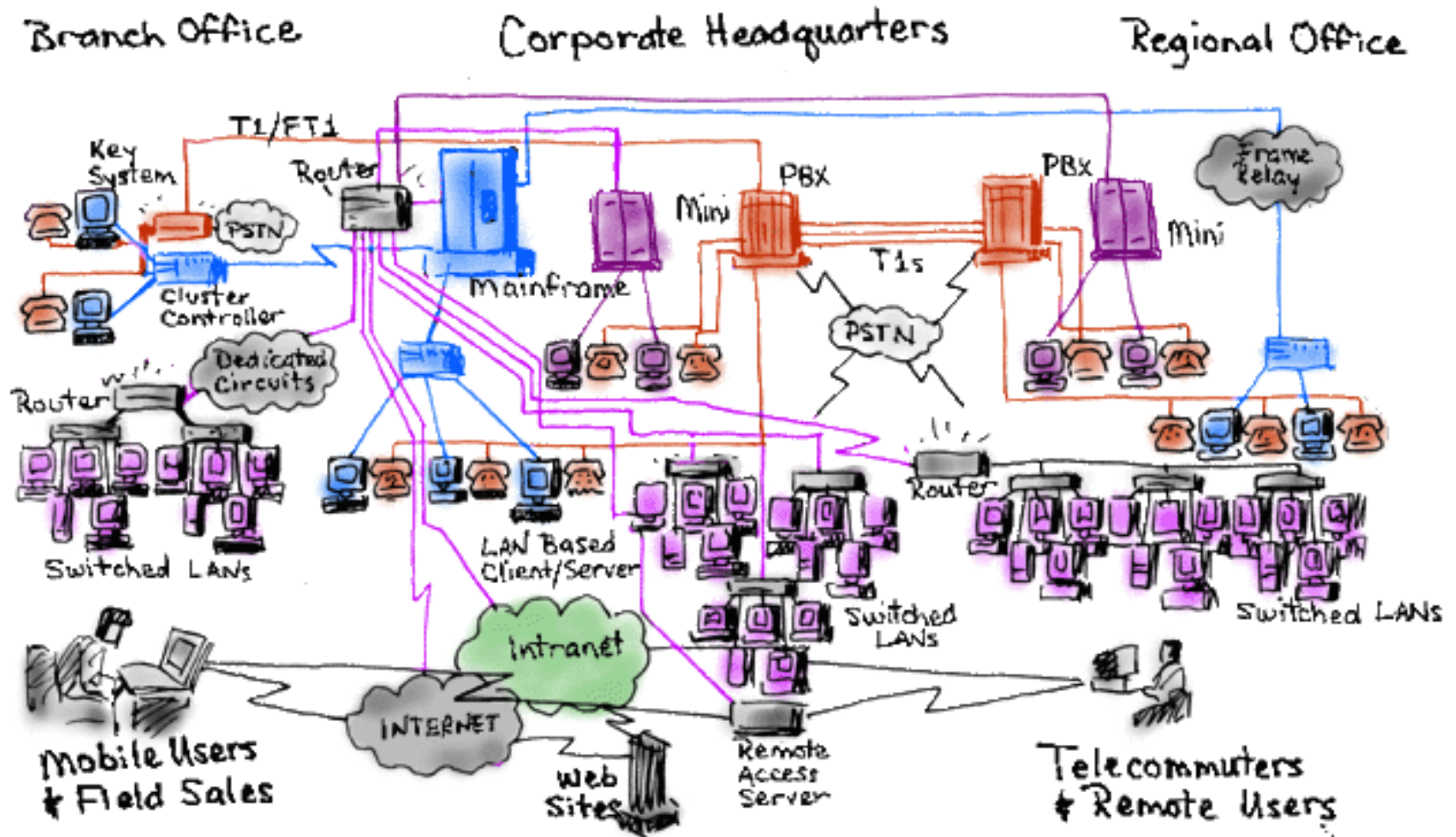
Connecting Business and IT

ITIL and IT Infrastructure

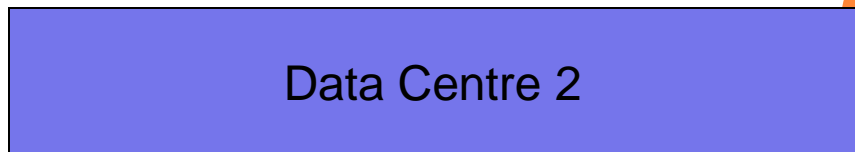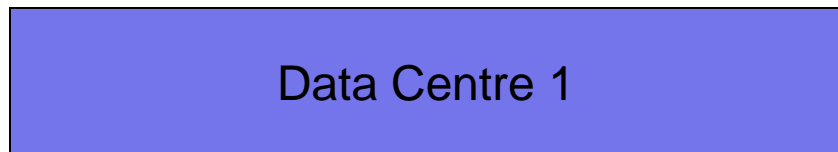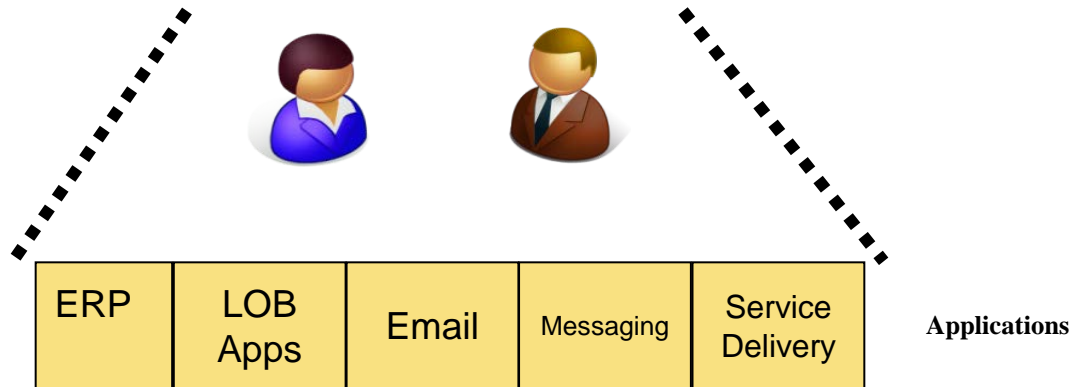**ITIL v2 defines IT infrastructure:**

All of the components (configuration items) that are needed to deliver IT services to customers.
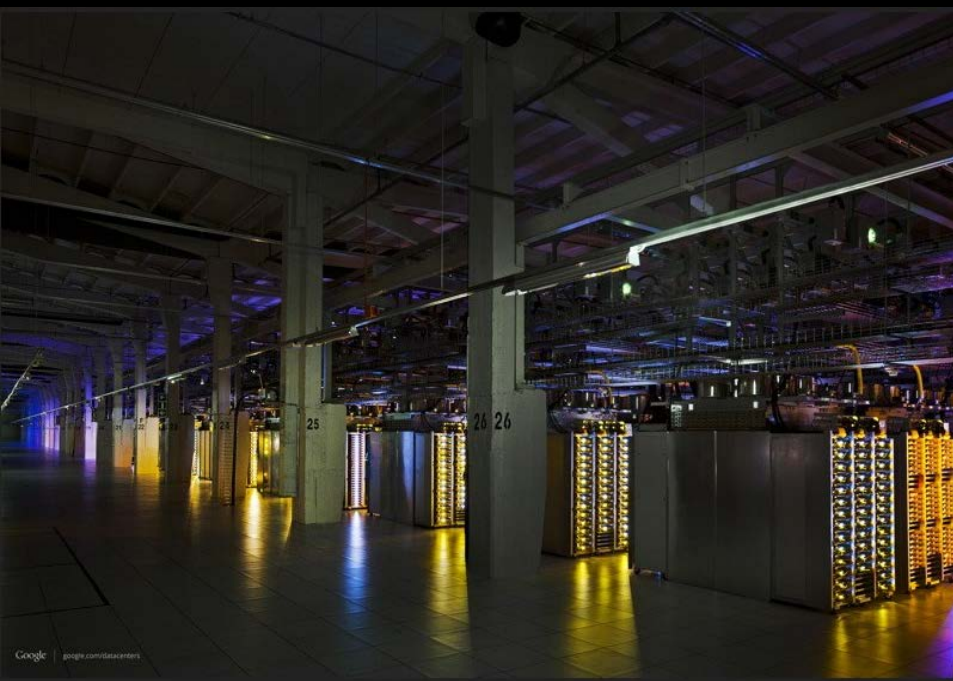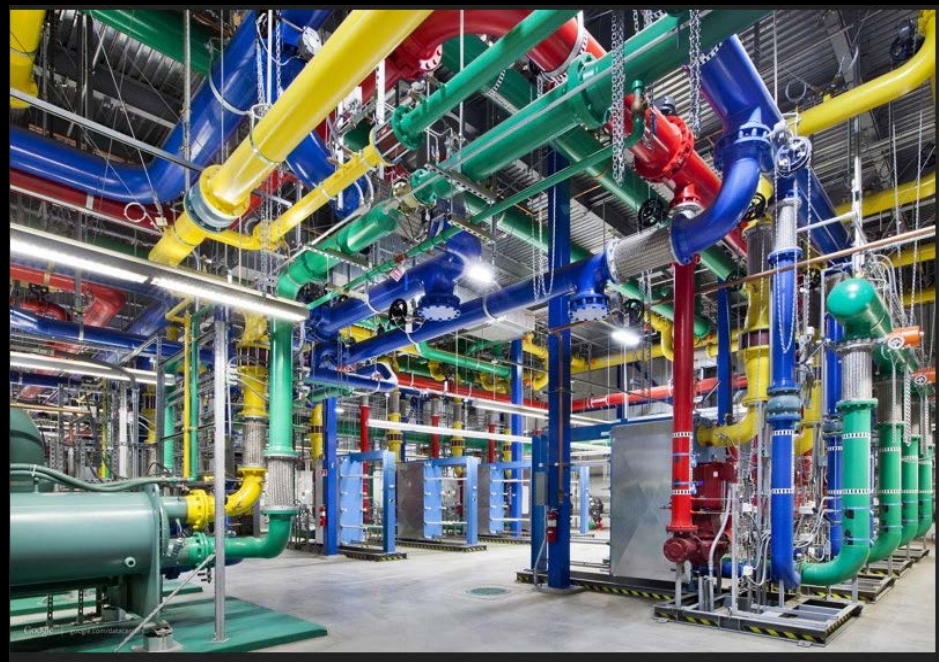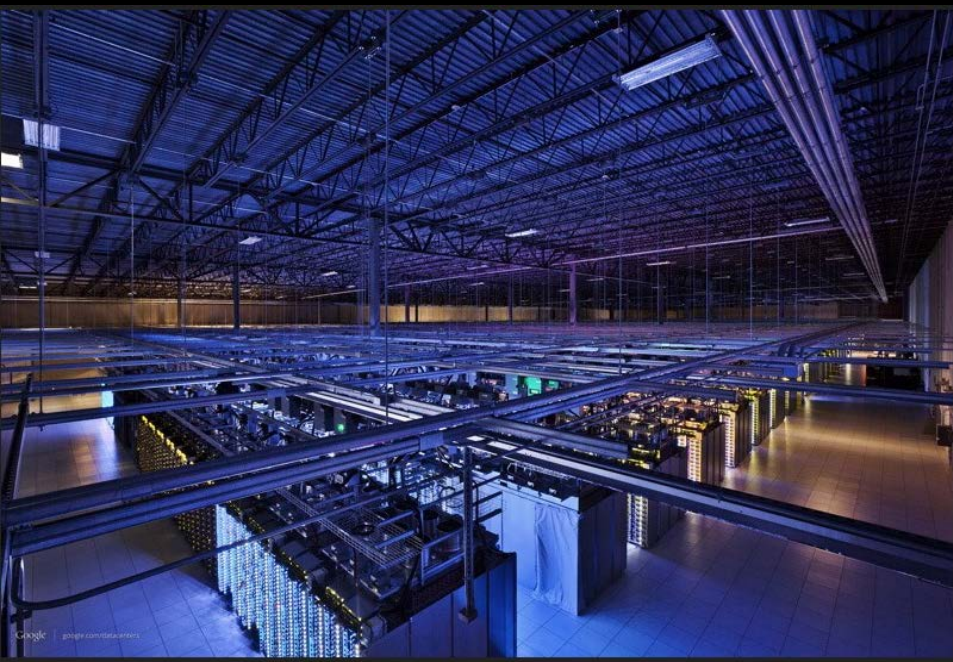
The IT Infrastructure consists of more than just hardware and software.

ANOTHER WAY OF LOOKING AT IT INFRA

PYRAMID

| ERP | LOB Apps | Email | Messaging | Service Delivery | **Applications** |

Thin Client Web Apps   Thick Client Terminals   Client/Server Application Servers   **Access Mechanism**

Databases   File Sharing   **Data Storage**

SAN   WAN   LAN   Routers Switches   DHCP   UPS   DNS   Power
Remote Access   VLAN   Authentication
Cabling   Generators   Transformers   Fire Suppression   **Infrastructure**

Data Centre 1   Data Centre 2   **Facilities**

4

5

Source: Engagdet http://www.engadget.com/2012/10/17/google-inside-data-centers/#continued Oct 17, 2012 Image Credit *Connie Zhou / Google]*
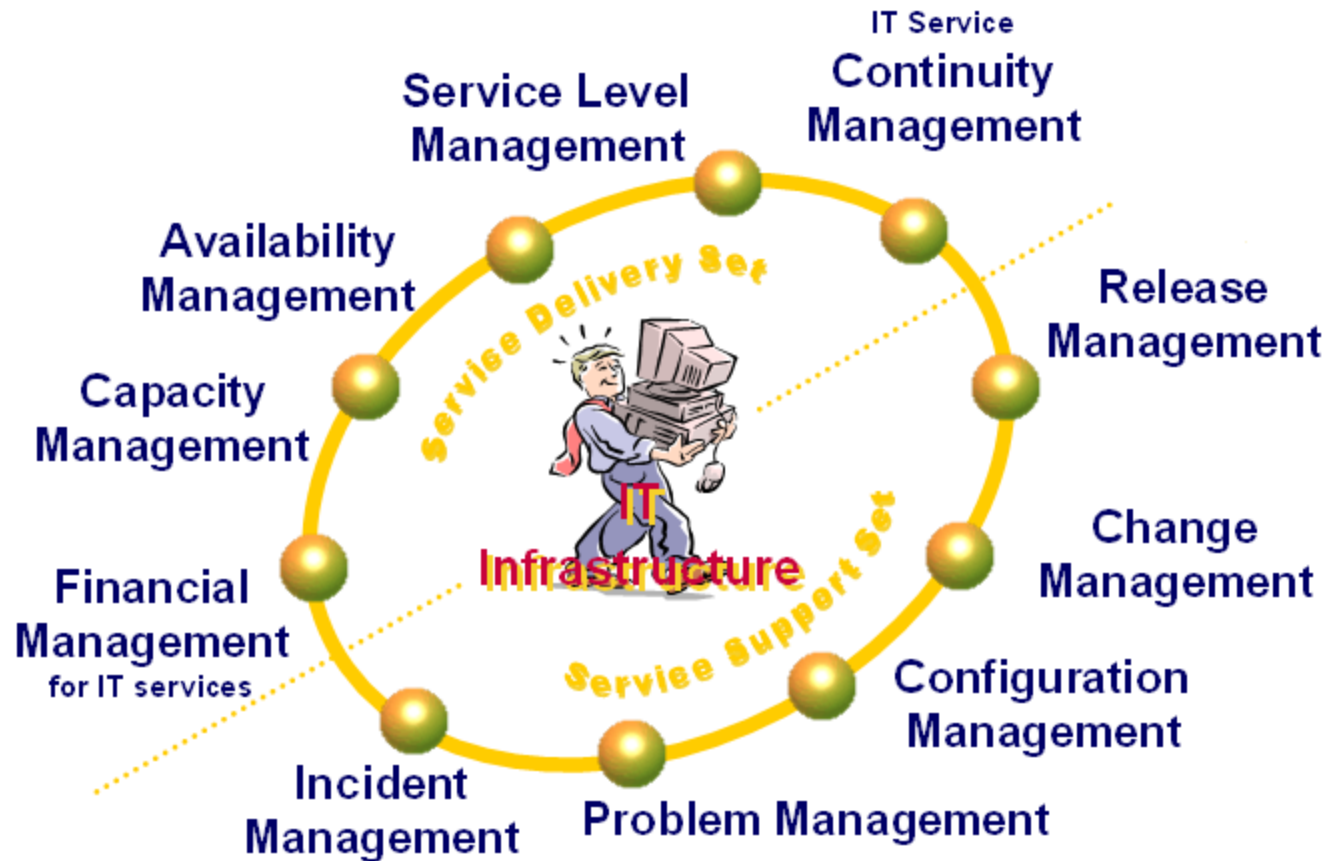
ITSM Components

BIG DATA (ALMOST)

- Volume
  - From 4 mainframes.
  - 17,000+ servers (AIX, LINUX, UNIX, Windows, iSeries).
  - Thousands of devices – firewalls, routers, etc
  - Millions of records created every hour.

- Limited Velocity
  - Little or no need to analyze in real time.

- Steady State Variety
  - Mainly text based structured records. No media files.

- Steady State Variability
  - Data comes from a steady state of known sources at a mostly steady rate.

Manage Operations

Mainframe Batch Processing
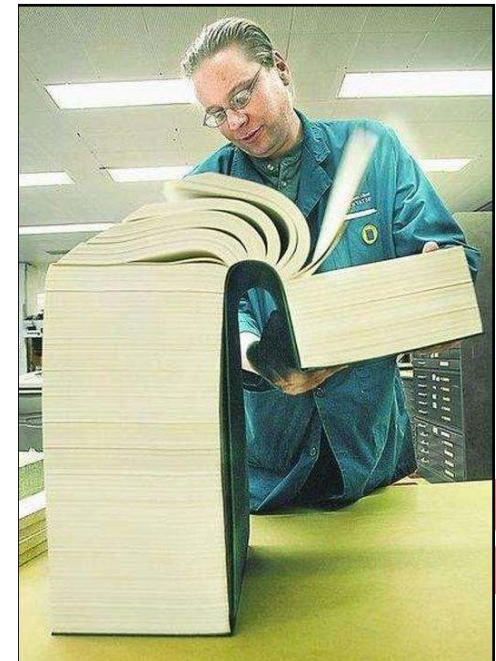
8

CA 7 – PRIMARY PROCEDURES

- Analysis and testing of Job Abends
- Analysis and testing of Changes to Job Schedules
- Testing links to Incident and Change Management systems

9

CA 7 – REPORTING ENVIRONMENT

- Large volume of data (CA-7 Job Log for 1 Month = 2000+ pages).
- Complex data structure (print image reports).
- *Automation with scripts and GUI – easily re-executed by anyone.*

WINDOWS BATCH AND ACL ROUTINES

CA 7 PREDICTIVE ANALYTICS CHANGES

Content restricted due to client confidentiality.

Item will be made available during presentation

CA 7 Predictive Analytics abends

Content restricted due to client confidentiality.

Item will be made available during presentation

CA 7 PREDICTIVE ANALYTICS CHANGES / ABENDS

Content restricted due to client confidentiality.

Item will be made available during presentation

CA 7 Predictive Analytics

Content restricted due to client confidentiality.

Item will be made available during presentation

MANAGE ACCESS
- ACCESS PROVISIONING

UNIX

Content restricted due to client confidentiality.

Item will be made available during presentation

UNIX

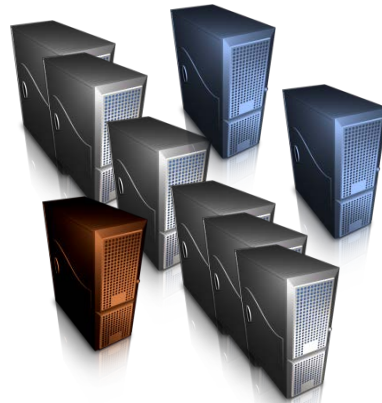Content restricted due to client confidentiality.

Item will be made available during presentation

UNIX – VERIFYING CHANGES IN USERS MONTH OVER MONTH

Month 1

Month 2

Month 3
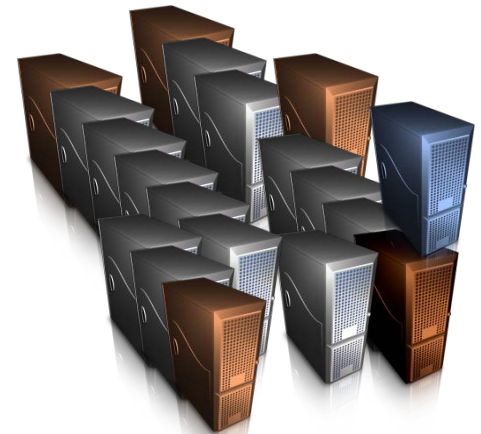
UNIX – VERIFYING CHANGES IN USERS MONTH OVER MONTH

Content restricted due to client confidentiality.

Item will be made available during presentation

Manage Change

Mainframe Endevor Changes

Content restricted due to client confidentiality.

Item will be made available during presentation

VISUALIZATION – ANALYTIC REVIEW

Content restricted due to client confidentiality.

Item will be made available during presentation

OPERATING SYSTEM CONFIGURATION

IBM Mainframe – z/OS

Content restricted due to client confidentiality.

Item will be made available during presentation

TRANSFORMATION
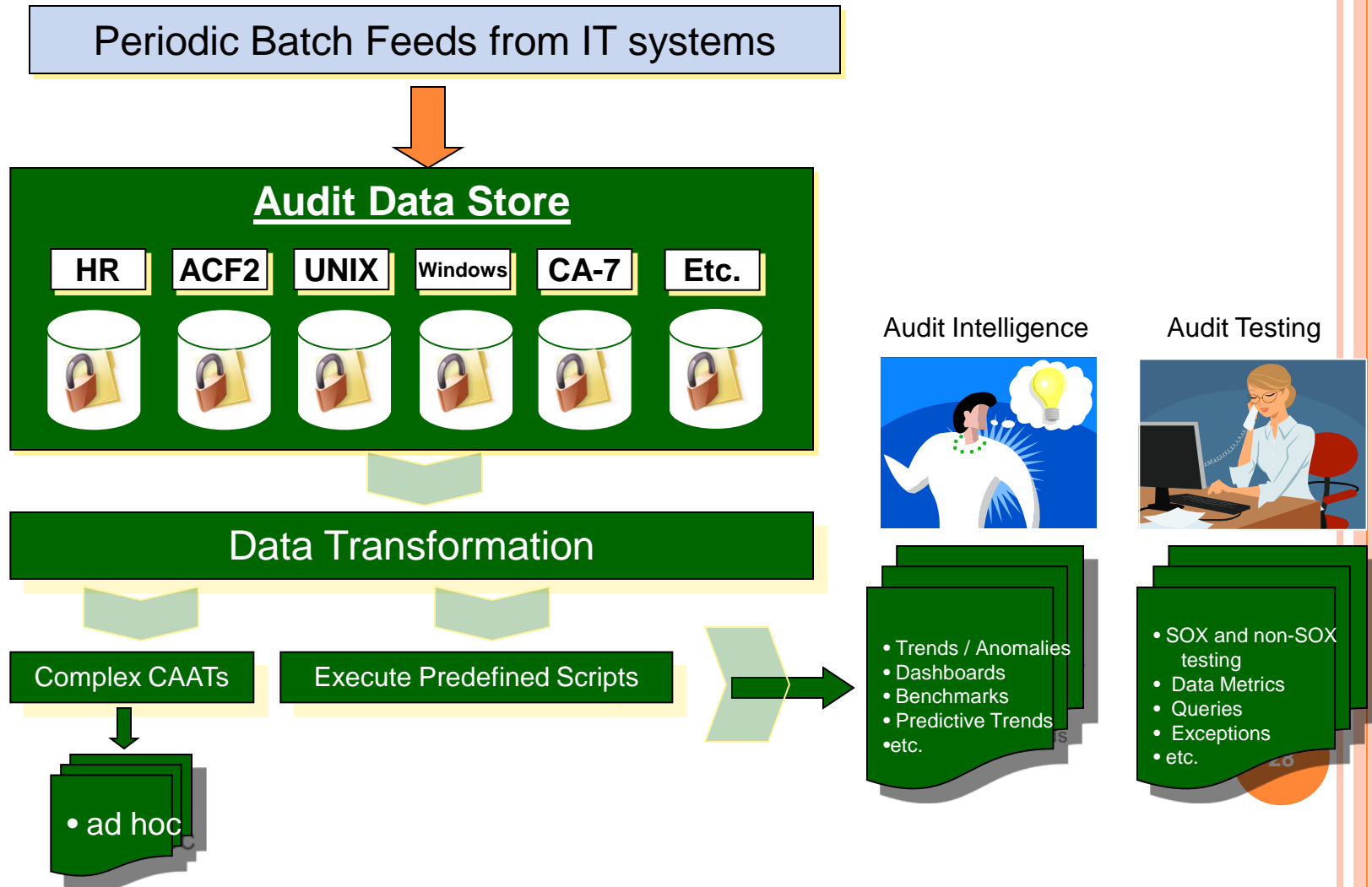
Content restricted due to client confidentiality.

Item will be made available during presentation

AUDIT TESTS

Content restricted due to client confidentiality.

Item will be made available during presentation

MOVE TO MORE FREQUENT TESTING

Periodic Batch Feeds from IT systems

Audit Data Store

| HR | ACF2 | UNIX | Windows | CA-7 | Etc. |

Data Transformation

Complex CAATs

Execute Predefined Scripts

• ad hoc

Audit Intelligence

Audit Testing

• Trends / Anomalies
• Dashboards
• Benchmarks
• Predictive Trends
• etc.

• SOX and non-SOX testing
• Data Metrics
• Queries
• Exceptions
• etc.

QUESTIONS

Eckhardt Kriel CA (SA)

E Kriel & Associates Inc.
1148 Forest Trail Place
Oakville
ON L6M 3H7

www.krielassoc.com

Mobile: +1. 416 451-3919
Direct: +1. 416 451-3919
Email: ekriel@live.ca

E Kriel & Associates Inc.
Connecting Business and IT