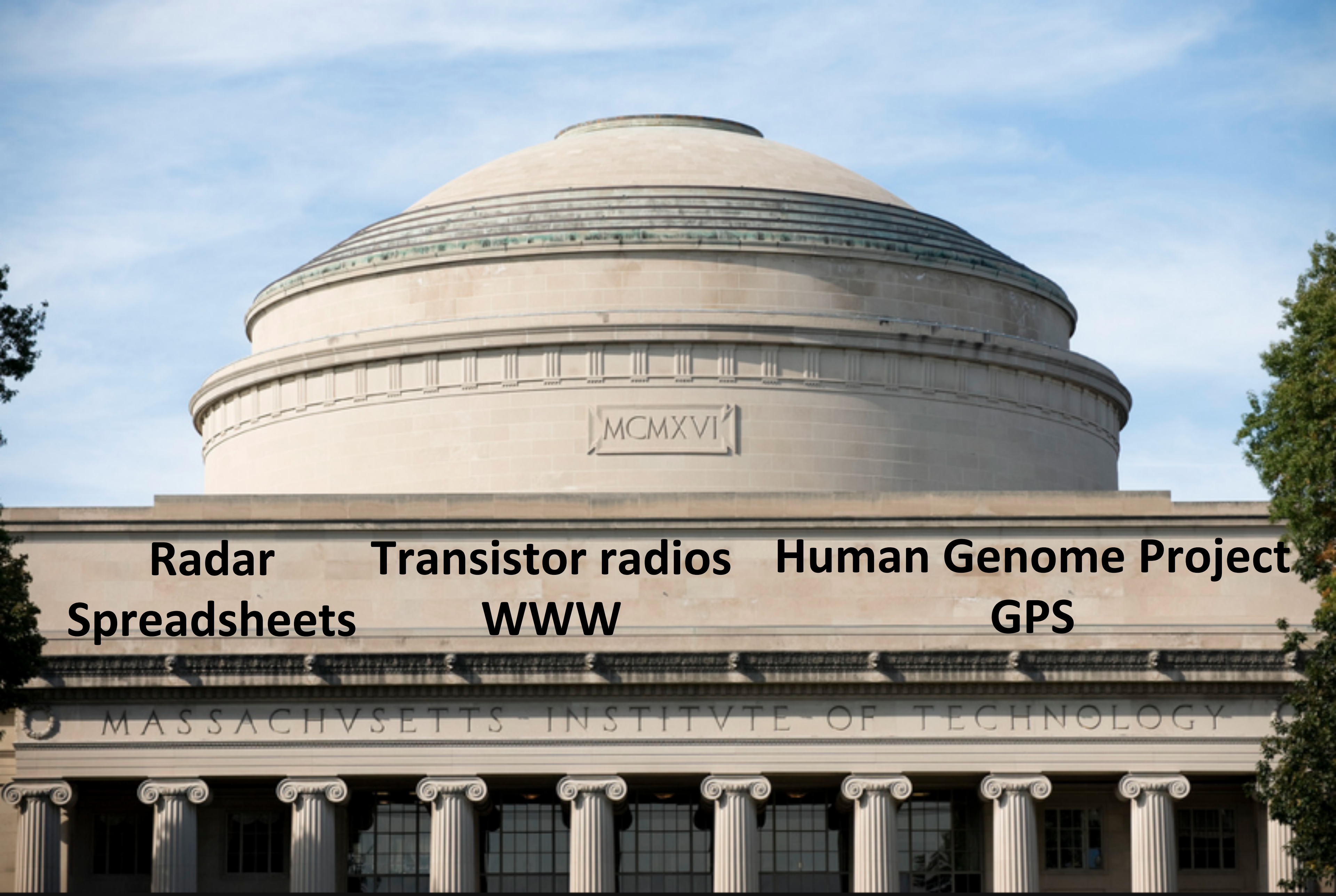
Governance, Risk and Compliance

Bart Dahlstrom
bartd@mit.edu

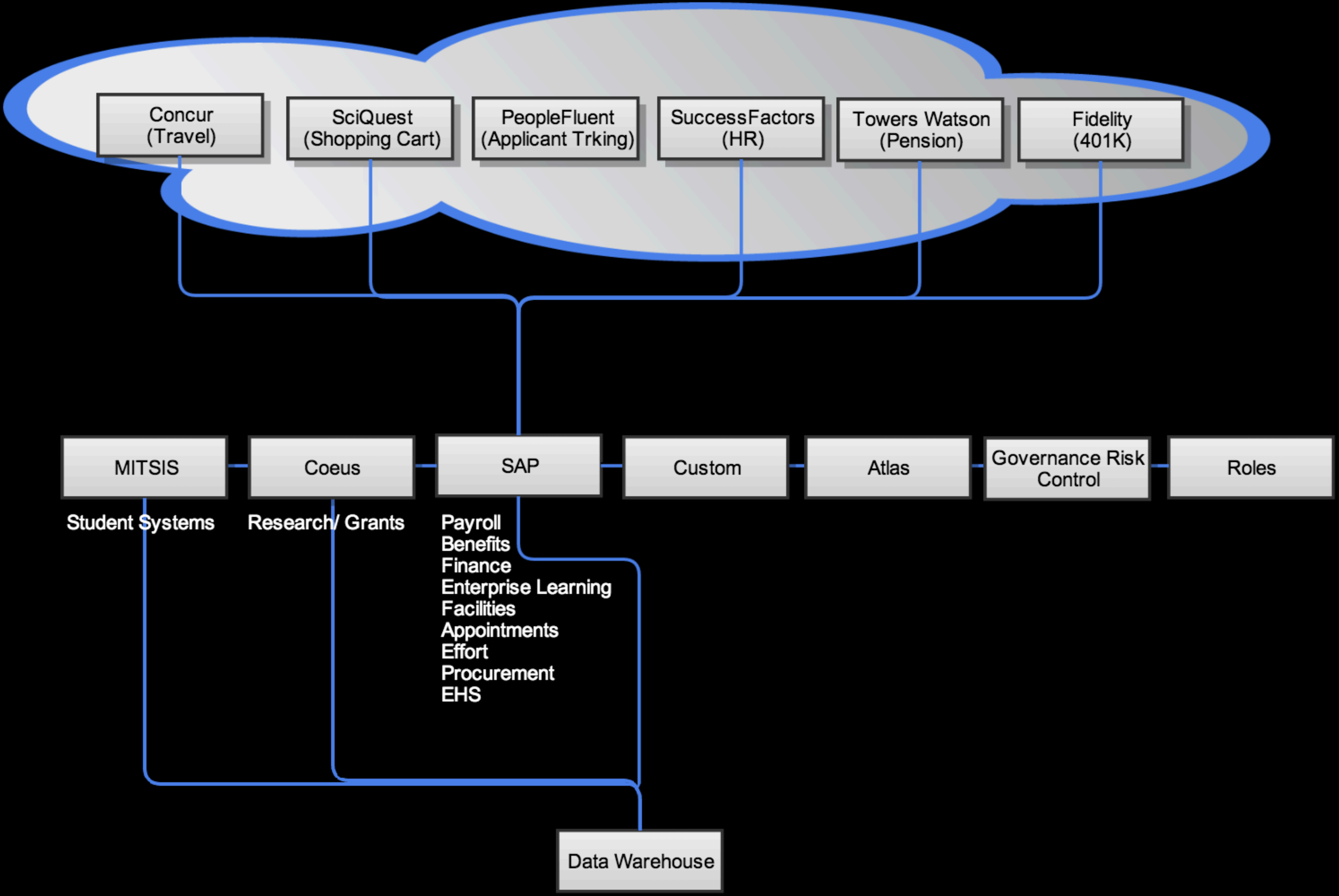


Radar
Spreadsheets

Transistor radios
WWW

Human Genome Project
GPS

MIT FIRE DEPT.



Concur (Travel)

SciQuest (Shopping Cart)

PeopleFluent (Applicant Trking)

SuccessFactors (HR)

Towers Watson (Pension)

Fidelity (401K)

MITSIS

Coeus

SAP

Custom

Atlas

Governance Risk Control

Roles

Student Systems

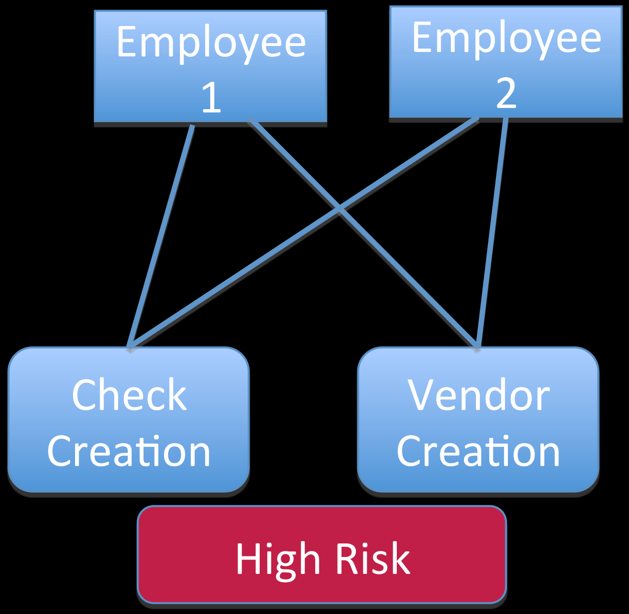
Research/ Grants

Payroll
Benefits
Finance
Enterprise Learning
Facilities
Appointments
Effort
Procurement
EHS

Data Warehouse

Segregation of Duties

Old Approach



Employee 1

Employee 2

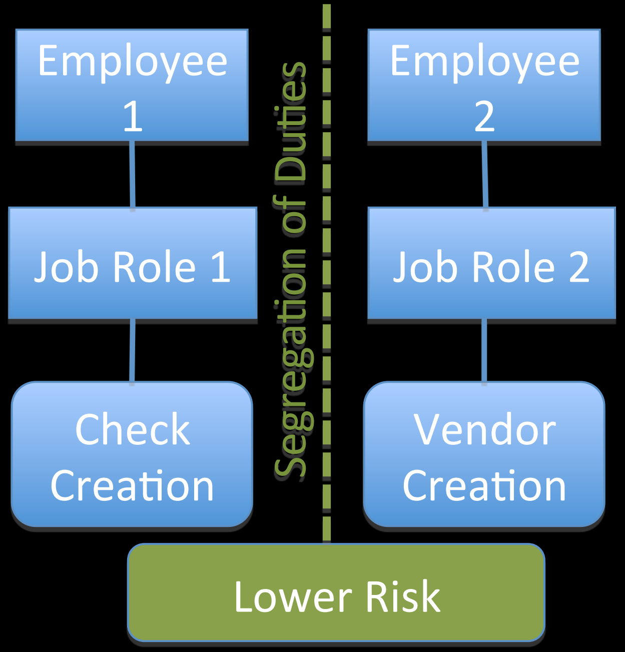
Check Creation

Vendor Creation

High Risk

- Vague system for requesting access
- No access reports for managers
- Employees retained access after transfers
- Access determined arbitrarily

New Approach



Employee 1

Employee 2

Job Role 1

Job Role 2

Check Creation

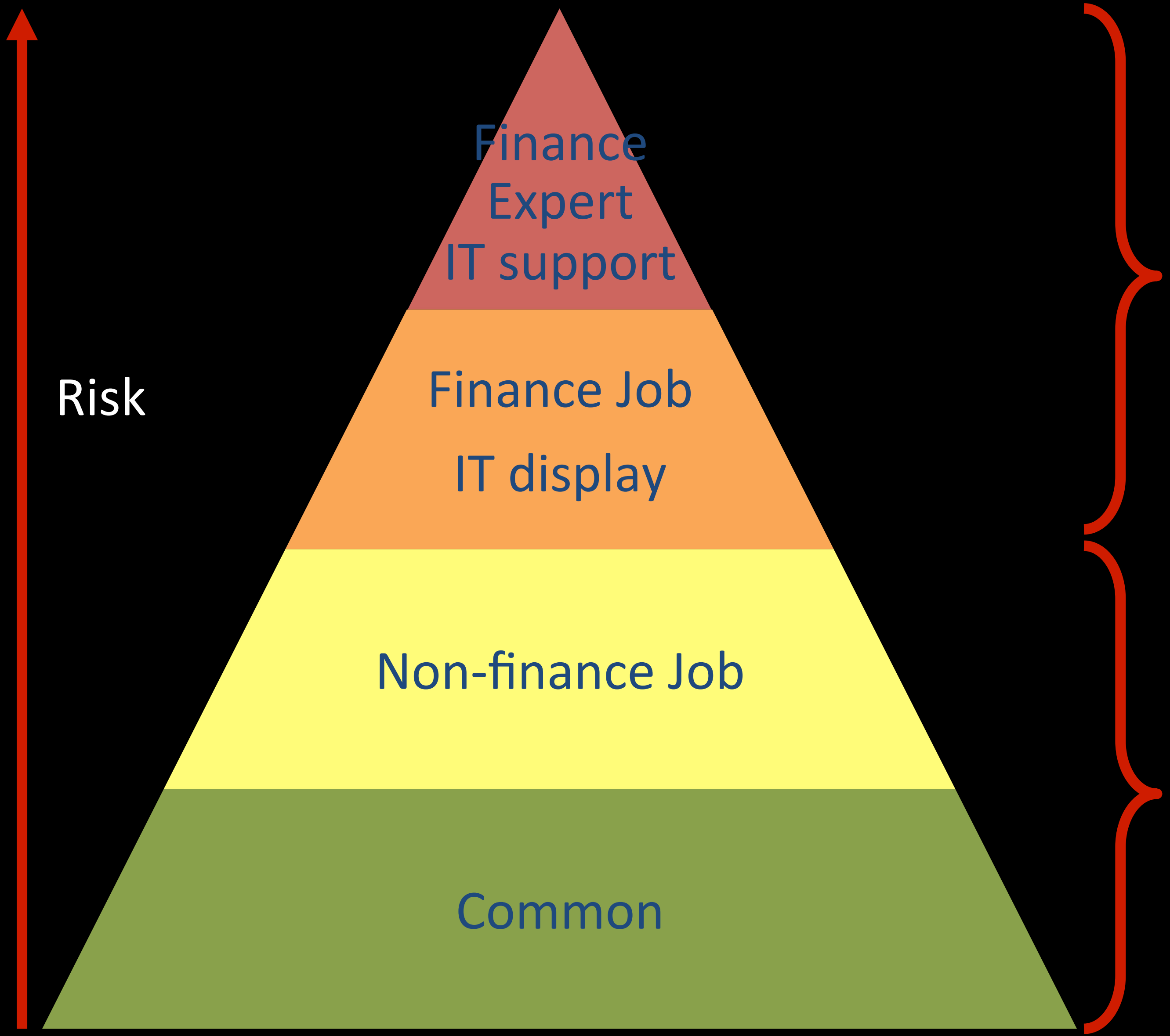
Vendor Creation

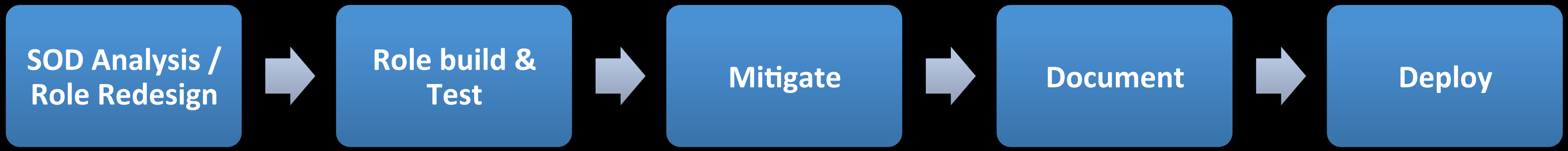
Segregation of Duties

Lower Risk

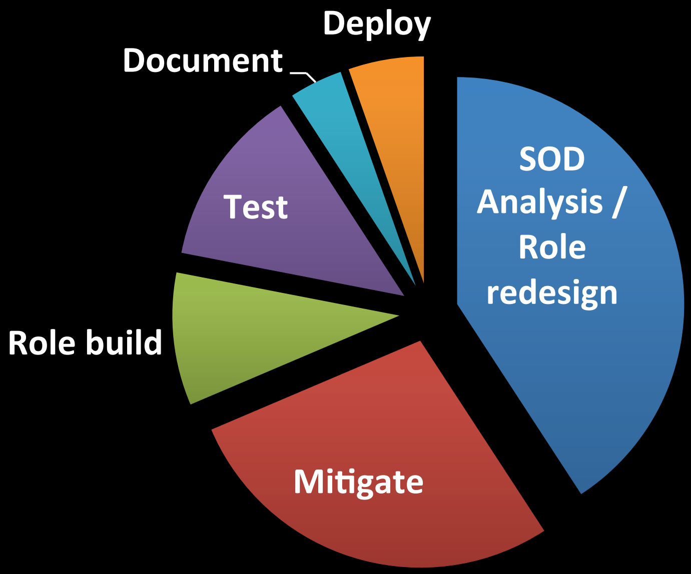
- Access and risks defined, documented, and monitored
- Defined process for modifying access
- Defined roles for access ownership and risk ownership
- Mitigation reports

Roles


Finance
Expert
IT support
Finance Job
IT display
Non-finance Job
Common
Risk
Segregate
or
Mitigate
Confirm



SOD Analysis / Role Redesign → Role build & Test → Mitigate → Document → Deploy



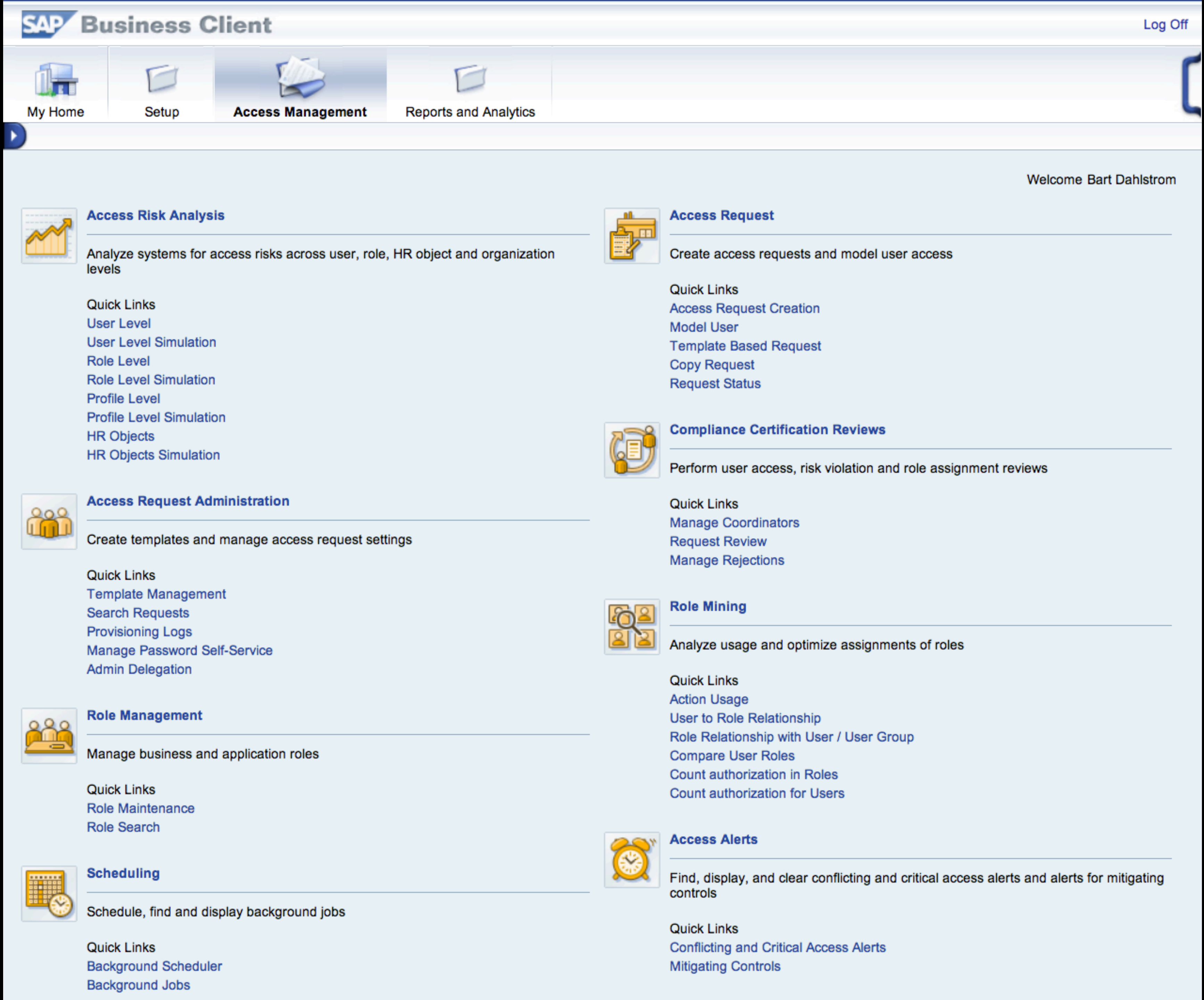
Responsibilities

Role Owner = Business owner

- Define role content
- Define user role access
- Approve user role access

Risk Owner = Manager of Business Owner

- Identify and define high risk access and SOD risks
- Define mitigation controls for SOD conflicts
- Collaborate with Internal Controls and Audit to ensure compliance
- Collaborate with Security Team to minimize risk in roles
- Review and approve or reject risks associated with roles and users
- Perform periodic review of risks and mitigation control



Welcome Bart Dahlstrom

Access Risk Analysis

Analyze systems for access risks across user, role, HR object and organization levels

Quick Links
- User Level
- User Level Simulation
- Role Level
- Role Level Simulation
- Profile Level
- Profile Level Simulation
- HR Objects
- HR Objects Simulation

Access Request Administration

Create templates and manage access request settings

Quick Links
- Template Management
- Search Requests
- Provisioning Logs
- Manage Password Self-Service
- Admin Delegation

Role Management

Manage business and application roles

Quick Links
- Role Maintenance
- Role Search

Scheduling

Schedule, find and display background jobs

Quick Links
- Background Scheduler
- Background Jobs

Access Request

Create access requests and model user access

Quick Links
- Access Request Creation
- Model User
- Template Based Request
- Copy Request
- Request Status

Compliance Certification Reviews

Perform user access, risk violation and role assignment reviews

Quick Links
- Manage Coordinators
- Request Review
- Manage Rejections

Role Mining

Analyze usage and optimize assignments of roles

Quick Links
- Action Usage
- User to Role Relationship
- Role Relationship with User / User Group
- Compare User Roles
- Count authorization in Roles
- Count authorization for Users

Access Alerts

Find, display, and clear conflicting and critical access alerts and alerts for mitigating controls

Quick Links
- Conflicting and Critical Access Alerts
- Mitigating Controls

Segregation of Duty

SOD: SAP Risk F001
Maintain fictitious GL account & hide activity via postings

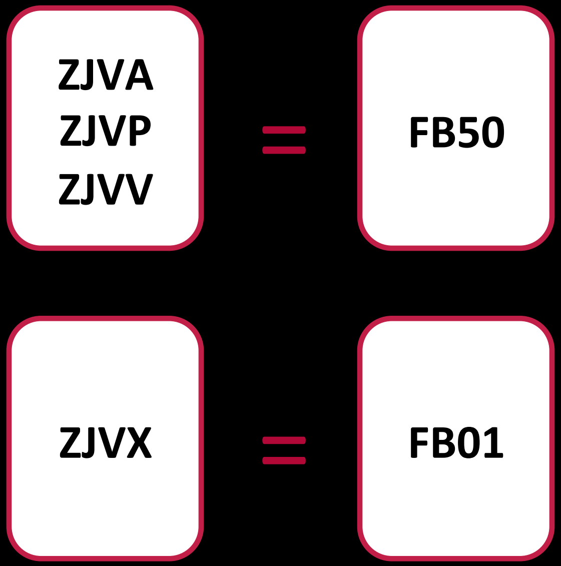
=

Function: GL01
F.56
F.57
F-02
FB01
FB08
FB09
FB50
FBRA
FBU8
FBV0
… (66 total)

+

Function: GL02
FS00
FS01
FS02
FSP0
FSP1
FSP2
FSS1
FSS2
GJ83
GJ85
…(319 total)

Custom transaction



ZJVA
ZJVP
ZJVV
=
FB50

ZJVX
=
FB01

Mitigation

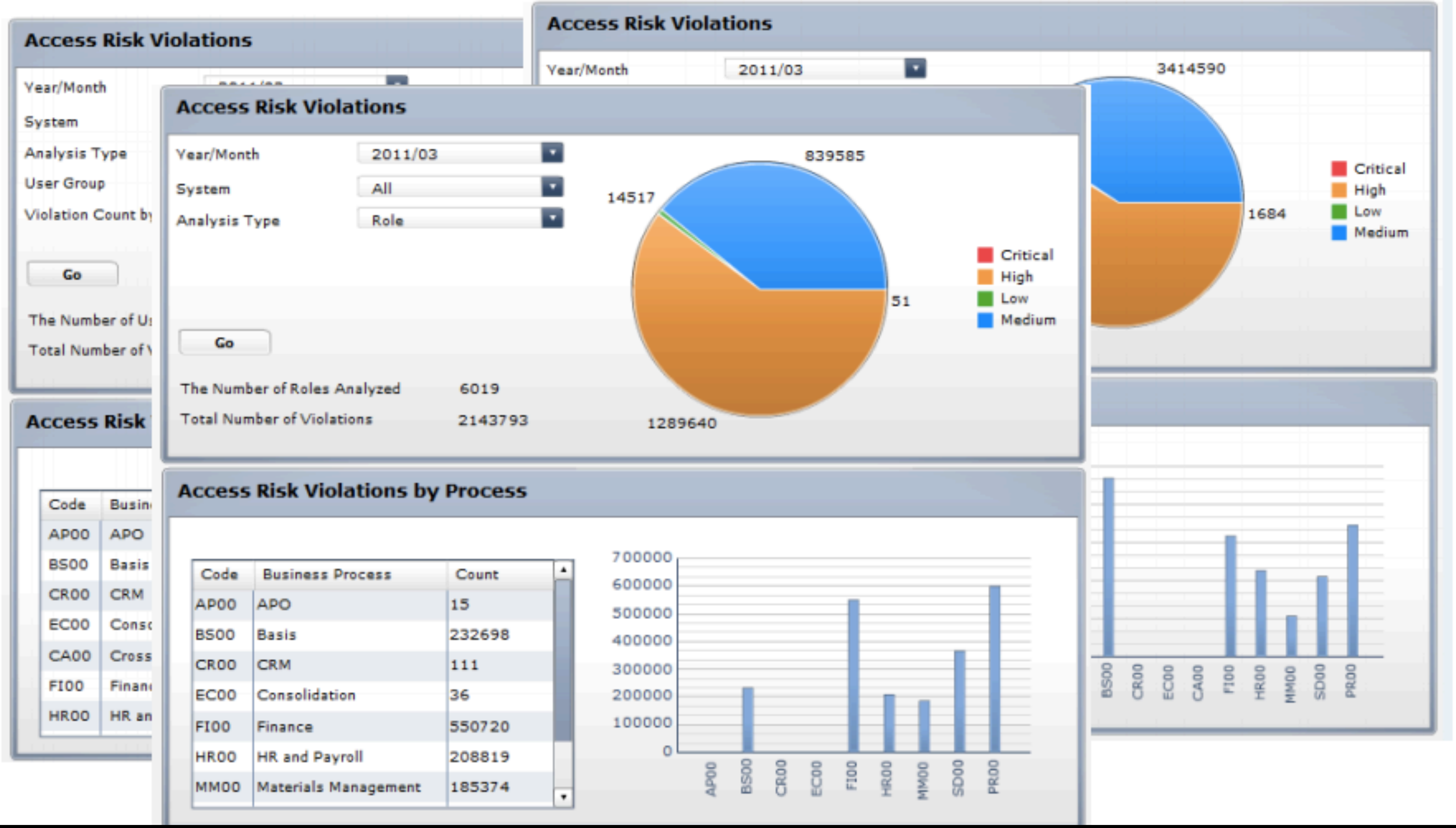
Risk

- Create vendor and initiate payment
- Assigned to Accounts Payable Manager role

Mitigation

- Report – vendor changes and invoices posted by same user
- Execute at least monthly
- Review by manager who does not have vendor master access
- Quarterly management review
- Annual audit review

GRC Reporting & Analysis



Access Risk Violations

Year/Month

System

Analysis Type

User Group

Violation Count by

Go

The Number of U

Total Number of V

Access Risk

Code	Busin
AP00	APO
BS00	Basis
CR00	CRM
EC00	Cons
CA00	Cross
FI00	Finan
HR00	HR an

Access Risk Violations

Year/Month 2011/03

Access Risk Violations

Year/Month 2011/03

System All

Analysis Type Role

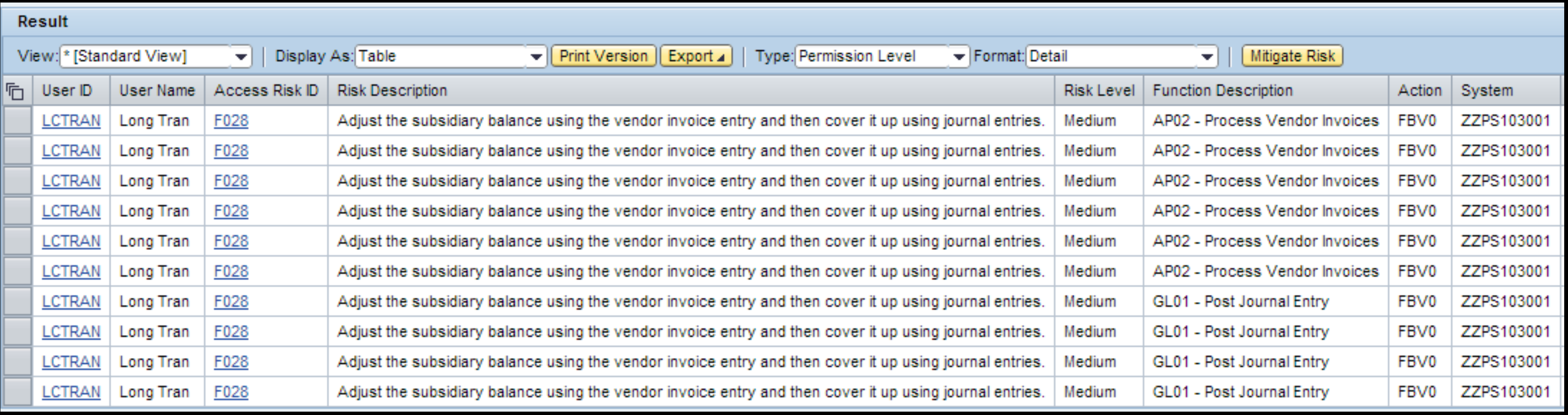
Go

The Number of Roles Analyzed	6019
Total Number of Violations	2143793

Access Risk Violations by Process

Code	Business Process	Count
AP00	APO	15
BS00	Basis	232698
CR00	CRM	111
EC00	Consolidation	36
FI00	Finance	550720
HR00	HR and Payroll	208819
MM00	Materials Management	185374

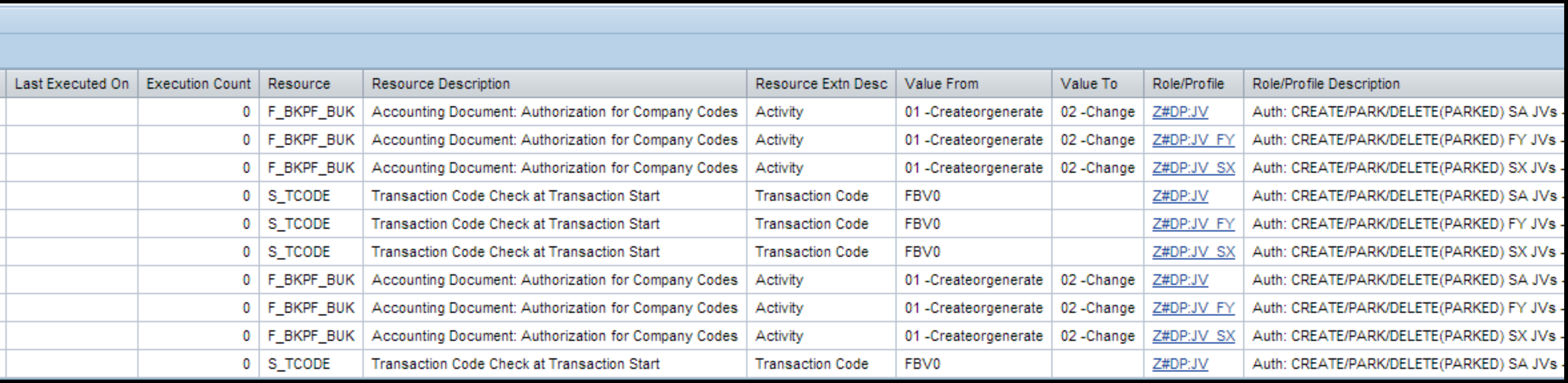
GRC Reporting & Analysis



Result

View: * [Standard View] | Display As: Table | Type: Permission Level | Format: Detail

User ID	User Name	Access Risk ID	Risk Description	Risk Level	Function Description	Action	System
LCTRAN	Long Tran	F028	Adjust the subsidiary balance using the vendor invoice entry and then cover it up using journal entries.	Medium	AP02 - Process Vendor Invoices	FBV0	ZZPS103001
LCTRAN	Long Tran	F028	Adjust the subsidiary balance using the vendor invoice entry and then cover it up using journal entries.	Medium	AP02 - Process Vendor Invoices	FBV0	ZZPS103001
LCTRAN	Long Tran	F028	Adjust the subsidiary balance using the vendor invoice entry and then cover it up using journal entries.	Medium	AP02 - Process Vendor Invoices	FBV0	ZZPS103001
LCTRAN	Long Tran	F028	Adjust the subsidiary balance using the vendor invoice entry and then cover it up using journal entries.	Medium	AP02 - Process Vendor Invoices	FBV0	ZZPS103001
LCTRAN	Long Tran	F028	Adjust the subsidiary balance using the vendor invoice entry and then cover it up using journal entries.	Medium	AP02 - Process Vendor Invoices	FBV0	ZZPS103001
LCTRAN	Long Tran	F028	Adjust the subsidiary balance using the vendor invoice entry and then cover it up using journal entries.	Medium	AP02 - Process Vendor Invoices	FBV0	ZZPS103001
LCTRAN	Long Tran	F028	Adjust the subsidiary balance using the vendor invoice entry and then cover it up using journal entries.	Medium	GL01 - Post Journal Entry	FBV0	ZZPS103001
LCTRAN	Long Tran	F028	Adjust the subsidiary balance using the vendor invoice entry and then cover it up using journal entries.	Medium	GL01 - Post Journal Entry	FBV0	ZZPS103001
LCTRAN	Long Tran	F028	Adjust the subsidiary balance using the vendor invoice entry and then cover it up using journal entries.	Medium	GL01 - Post Journal Entry	FBV0	ZZPS103001
LCTRAN	Long Tran	F028	Adjust the subsidiary balance using the vendor invoice entry and then cover it up using journal entries.	Medium	GL01 - Post Journal Entry	FBV0	ZZPS103001



Last Executed On	Execution Count	Resource	Resource Description	Resource Extn Desc	Value From	Value To	Role/Profile	Role/Profile Description
	0	F_BKPF_BUK	Accounting Document: Authorization for Company Codes	Activity	01 -Createorgenerate	02 -Change	Z#DP:JV	Auth: CREATE/PARK/DELETE(PARKED) SA JVs -
	0	F_BKPF_BUK	Accounting Document: Authorization for Company Codes	Activity	01 -Createorgenerate	02 -Change	Z#DP:JV_FY	Auth: CREATE/PARK/DELETE(PARKED) FY JVs -
	0	F_BKPF_BUK	Accounting Document: Authorization for Company Codes	Activity	01 -Createorgenerate	02 -Change	Z#DP:JV_SX	Auth: CREATE/PARK/DELETE(PARKED) SX JVs -
	0	S_TCODE	Transaction Code Check at Transaction Start	Transaction Code	FBV0		Z#DP:JV	Auth: CREATE/PARK/DELETE(PARKED) SA JVs -
	0	S_TCODE	Transaction Code Check at Transaction Start	Transaction Code	FBV0		Z#DP:JV_FY	Auth: CREATE/PARK/DELETE(PARKED) FY JVs -
	0	S_TCODE	Transaction Code Check at Transaction Start	Transaction Code	FBV0		Z#DP:JV_SX	Auth: CREATE/PARK/DELETE(PARKED) SX JVs -
	0	F_BKPF_BUK	Accounting Document: Authorization for Company Codes	Activity	01 -Createorgenerate	02 -Change	Z#DP:JV	Auth: CREATE/PARK/DELETE(PARKED) SA JVs -
	0	F_BKPF_BUK	Accounting Document: Authorization for Company Codes	Activity	01 -Createorgenerate	02 -Change	Z#DP:JV_FY	Auth: CREATE/PARK/DELETE(PARKED) FY JVs -
	0	F_BKPF_BUK	Accounting Document: Authorization for Company Codes	Activity	01 -Createorgenerate	02 -Change	Z#DP:JV_SX	Auth: CREATE/PARK/DELETE(PARKED) SX JVs -
	0	S_TCODE	Transaction Code Check at Transaction Start	Transaction Code	FBV0		Z#DP:JV	Auth: CREATE/PARK/DELETE(PARKED) SA JVs -

Thank You!