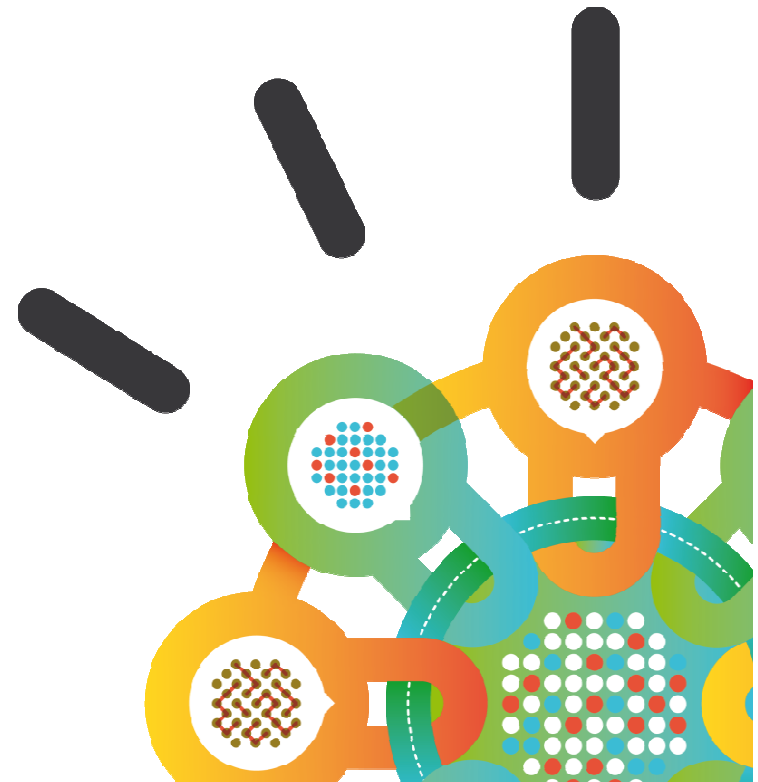


Security Intelligence.
Think Integrated.

IBM Security Identity Governance (CrossIdeas)

Technical presentation & Demo

Marco Venuti
VP Technical Sales
CrossIdeas – an IBM Company
Marco.venuti@crossideas.com





Agenda

- ISIM + ISIG Integration scenario
- Integration roadmap
- Live demo
- Q&A

The background of the slide is a vibrant blue with a pattern of abstract, semi-transparent geometric shapes. These shapes include circles, squares, and lines, some of which are arranged in a grid-like pattern, suggesting a technical or data-driven theme. The overall aesthetic is clean and modern.

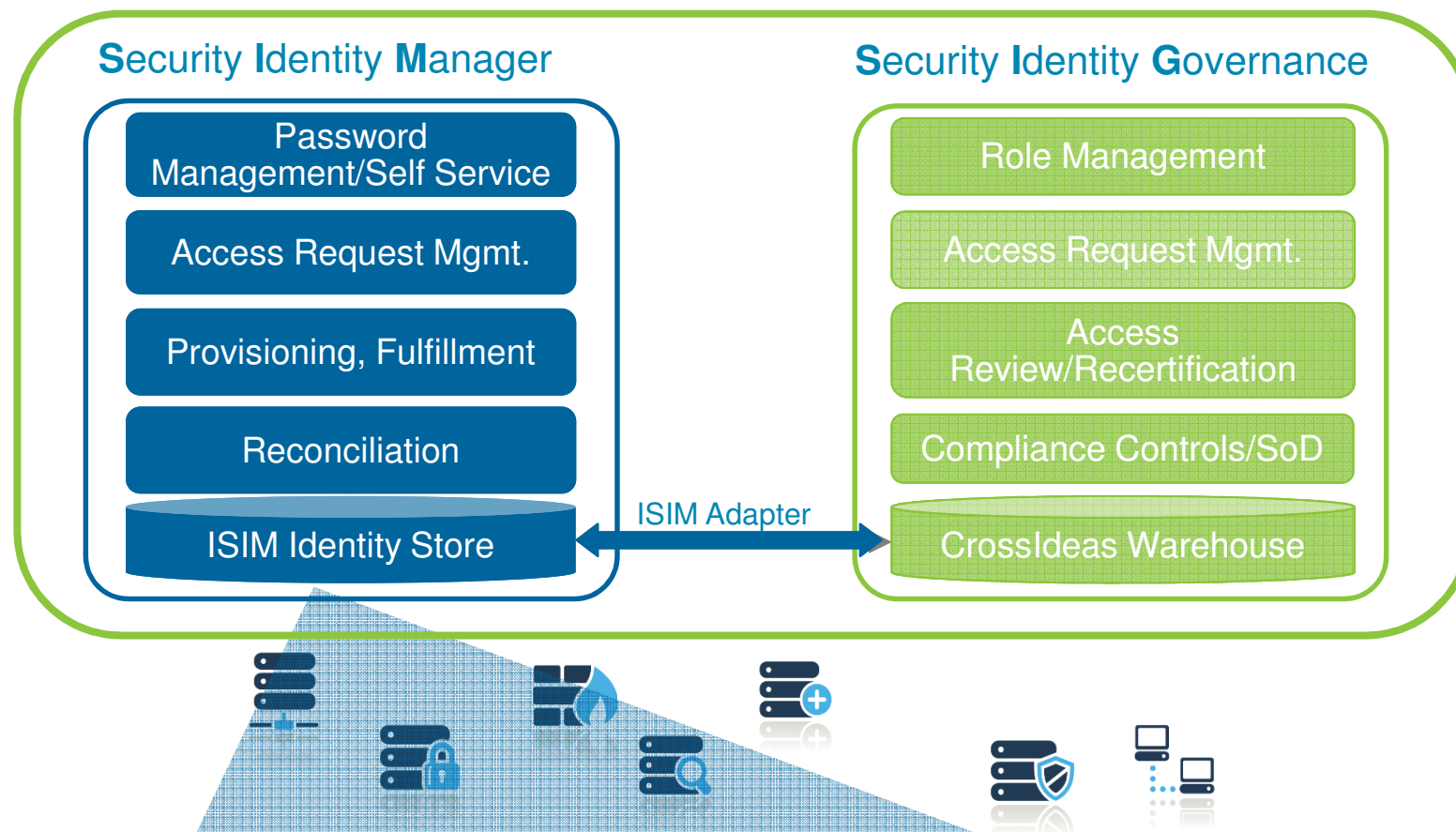
ISIM + ISIG

Integration Scenario

ISIM + ISIG for existing ISIM customers

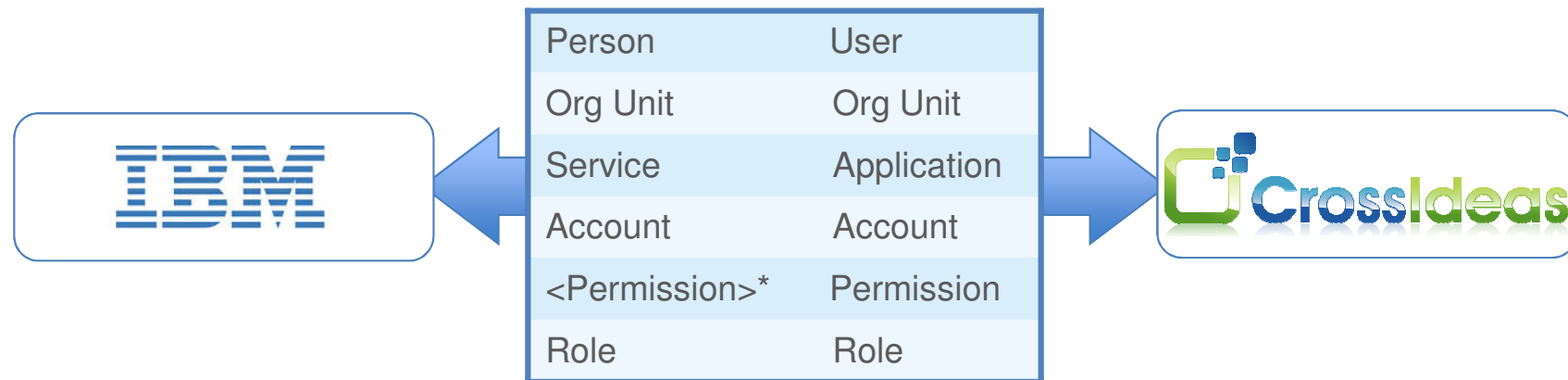
IBM Security Identity Governance and Administration

- Existing ISIM customer with Access Request Management exposed to business users
- Introducing ISIG to deliver Recertification campaign and Analytics capabilities



ISIM – ISIG Integration

- Available now, developed as a TDI adapter
- TDI Assembly line for full and delta synchronization
- Developed on TDI version 7.1, ISIM 6.1 – TDI7.0 and ITIM 5.1 are supported
- IDEAS API based integration



* Connector Specific (e.g. “Group” for AD)

ISIM → ISIG: Supported Events

Org Unit

- Add / Modify / Delete
- Add / Remove Member

User

- Add / Modify / Delete
- Suspend / Restore

Account

- Add / Modify / Delete
- Suspend / Restore

Service

- Add / Modify / Delete

Permission

- Add / Remove
- Add / Remove Member

Role

- Add / Remove
- Add / Remove Member

IBM

Bulk Sync + Incremental

CrossIdeas

ISIG ← ISIM: Supported Events

Org Unit

- Add / Modify / Delete
- Add / Remove Member

User

- Add / Modify / Delete
- Suspend / Restore

Account

- Add / Modify / Delete
- Suspend / Restore

Service

- Add / Modify / Delete

Permission

- Add / Remove
- Add / Remove Member

Role

- Add / Remove
- Add / Remove Member



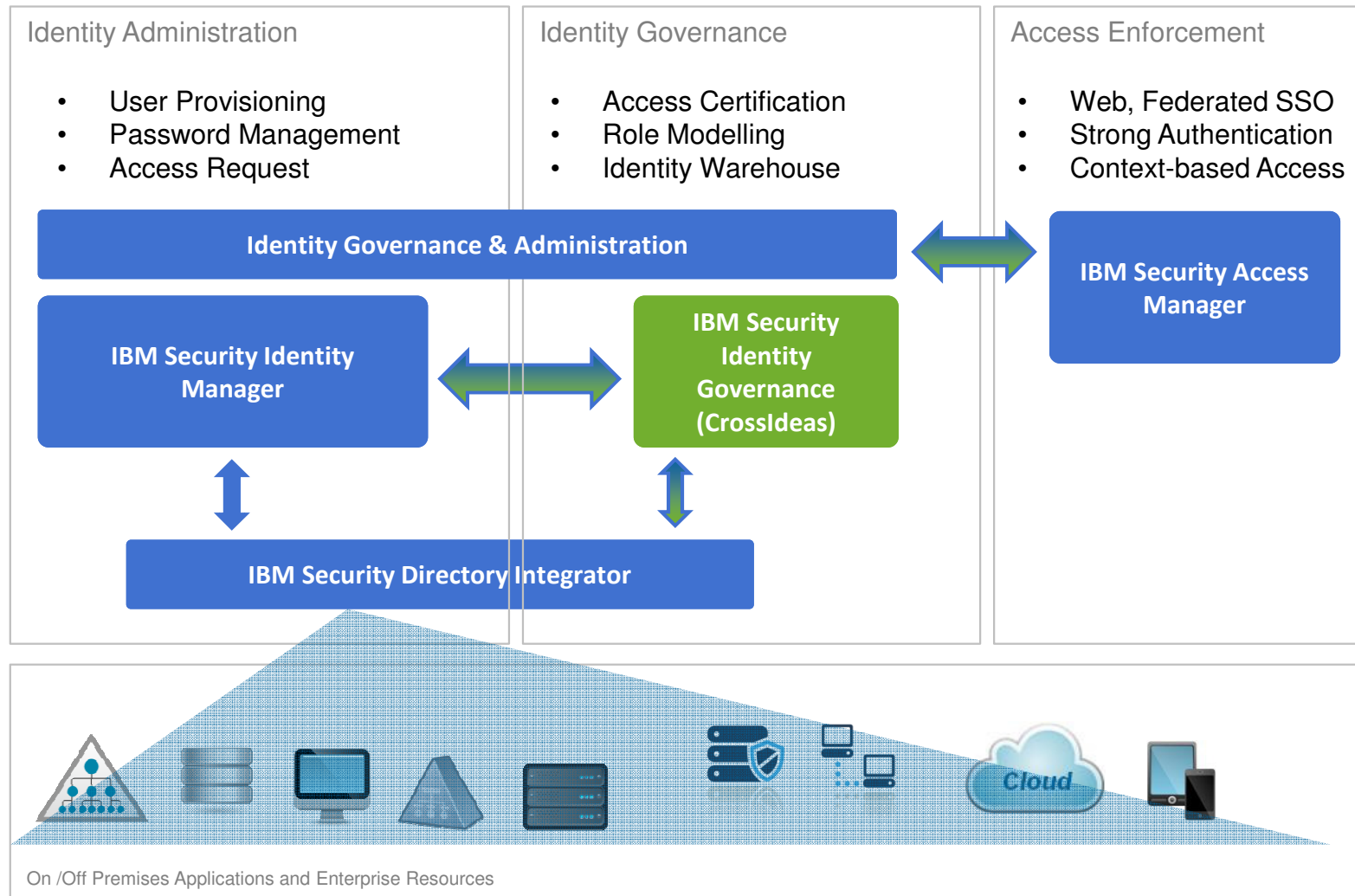
Write Back



Integration Roadmap

Scenario based easy to use interface for a line of business persona and do-it-yourself administrators. Option on ISC are controlled via user permissions.

Integrated IGA vision



Live Demo

ISIG... to answer common IGA questions



IT Security

How do I model policies and then detect and manage violations?



Business
Manager

What does an attestation campaign or an access request look like?



Application
Managers

How can I build meaningful roles?

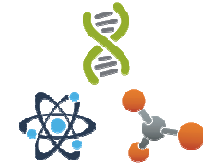


CFO / CRO
Office

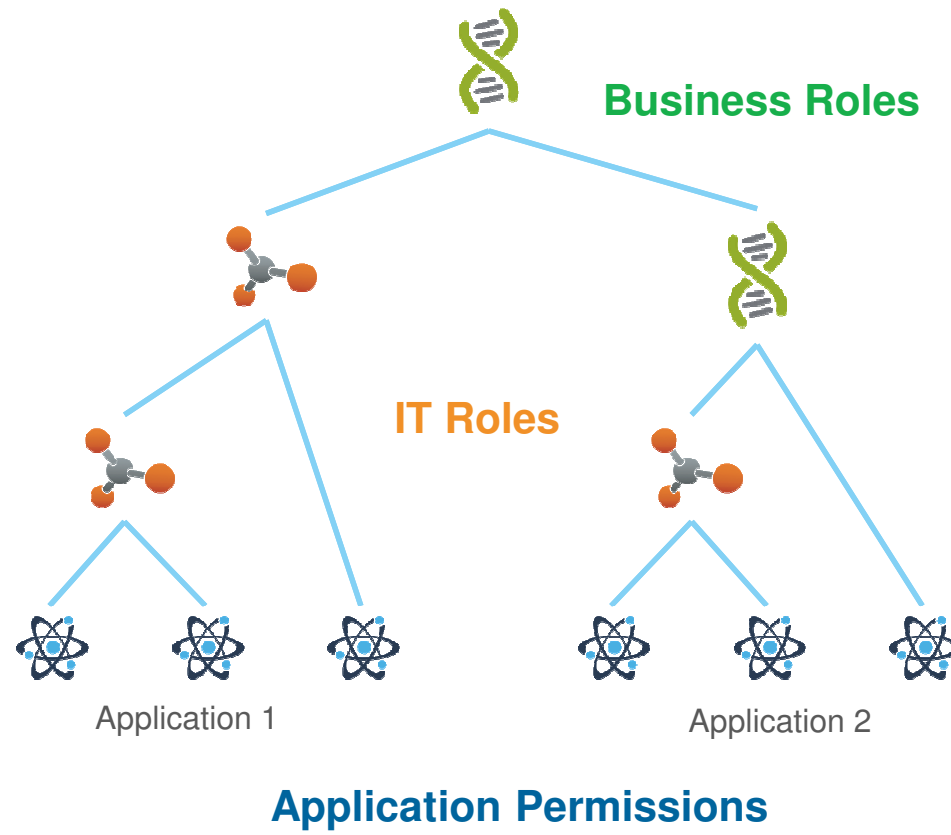
How do I measure access risk and monitor progresses?



IDEAS Glossary - Entitlement Hierarchy

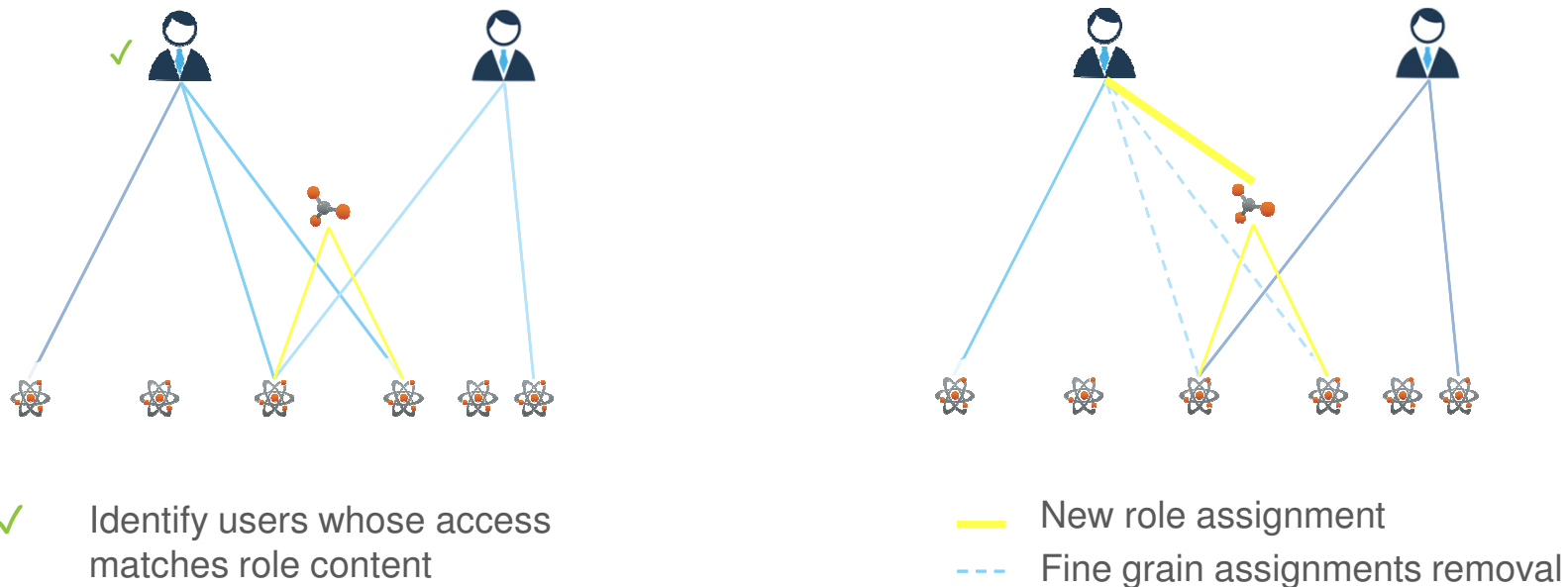


Entitlements



Role Deployment

How do I deal with existing users?



Upshifting applicable assignment - from permission to role

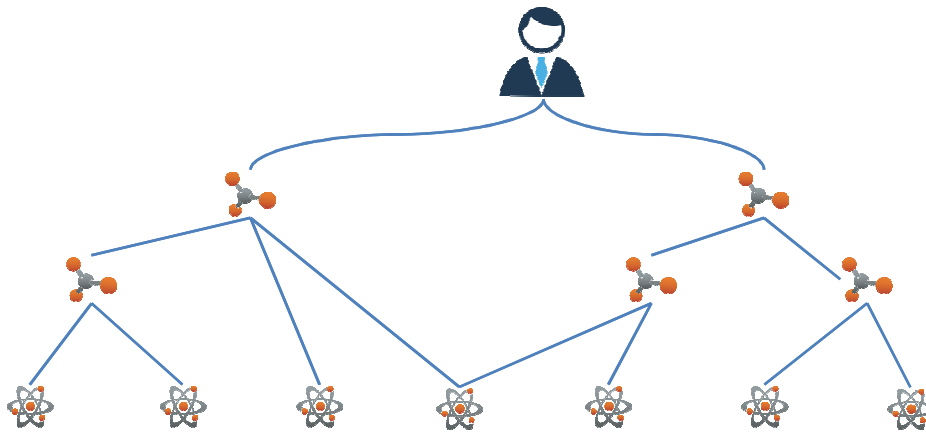
- Reduction of user assigned items in the IDEAS perspective
- No impact on user access



Managing Segregation of Duties

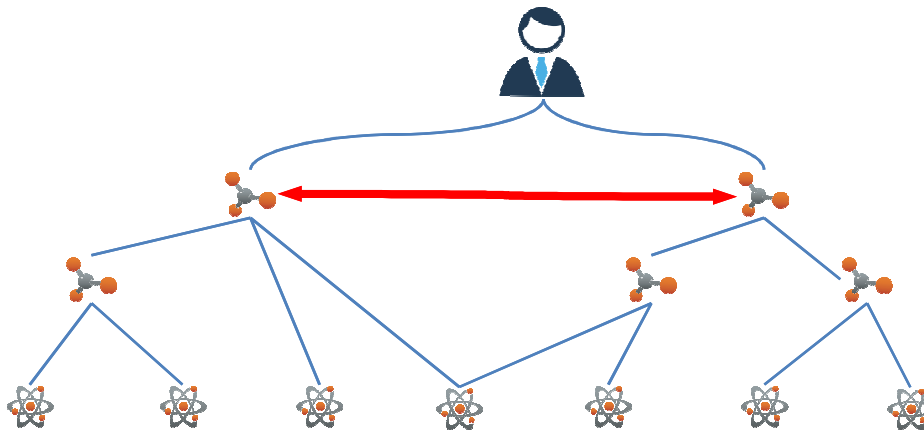
About Roles...

- The company invested in Roles to better model 'who-could-do-what'



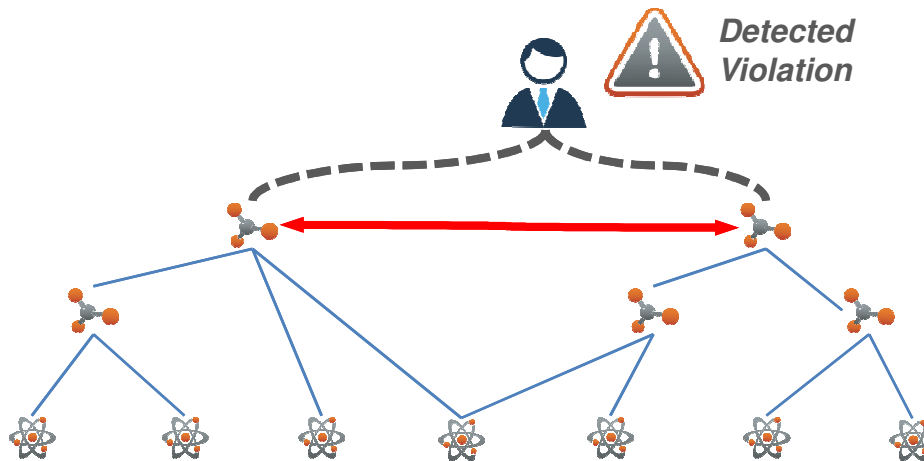
About Roles...

- The company invested in Roles to better model ‘who-could-do-what’
- They started implementing SoD on Roles
 - *e.g. Role A should not be jointly delivered with Role B*



About Roles...

- The company invested in Roles to better model ‘who-could-do-what’
- They started implementing SoD on Roles
 - *e.g. Role A should not be jointly delivered with Role B*

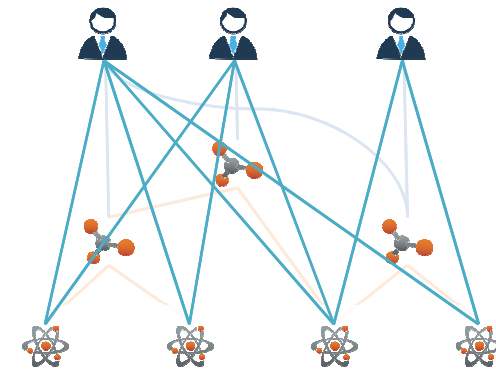


But..... auditors do not “trust” roles

IT Thinks in Terms of Roles – Auditors Don't

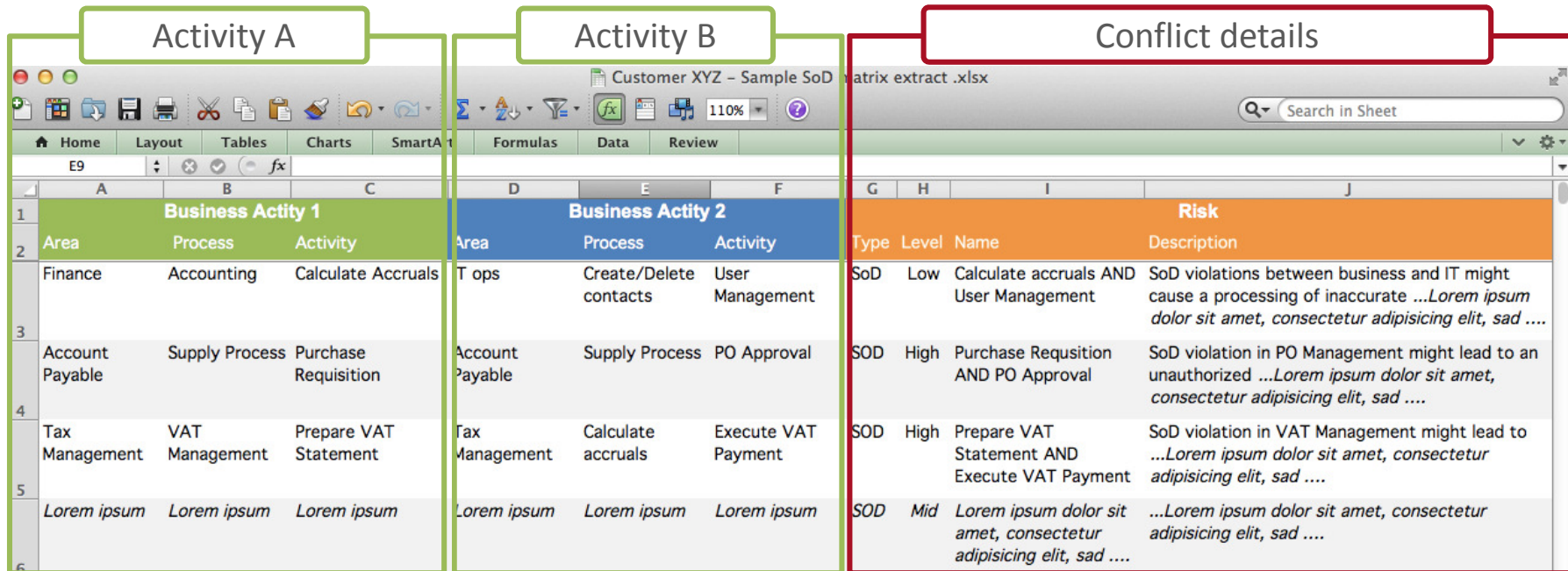
Auditor:

- “Let me ignore roles and look directly at user permissions assignments”
- “By the way...roles should be subject to the audit too”



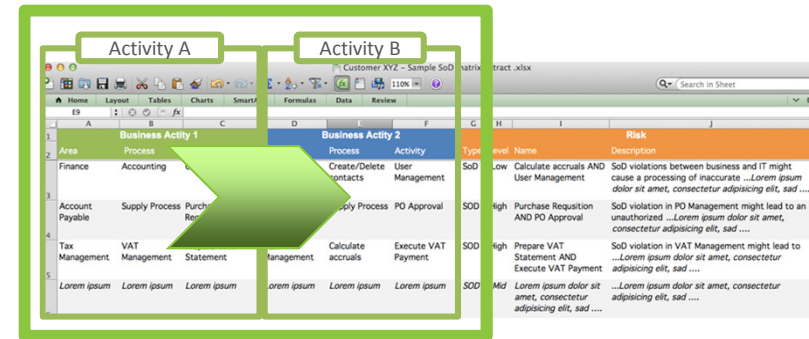
SoD Rules = Business Rules

- Auditors do think of SoD in terms of conflicting business activities



Business Activity 1			Business Activity 2			Risk			
Area	Process	Activity	Area	Process	Activity	Type	Level	Name	Description
Finance	Accounting	Calculate Accruals	IT ops	Create/Delete contacts	User Management	SoD	Low	Calculate accruals AND User Management	SoD violations between business and IT might cause a processing of inaccurate ...Lorem ipsum dolor sit amet, consectetur adipiscing elit, sad
Account Payable	Supply Process	Purchase Requisition	Account Payable	Supply Process	PO Approval	SOD	High	Purchase Requisition AND PO Approval	SoD violation in PO Management might lead to an unauthorized ...Lorem ipsum dolor sit amet, consectetur adipiscing elit, sad
Tax Management	VAT Management	Prepare VAT Statement	Tax Management	Calculate accruals	Execute VAT Payment	SOD	High	Prepare VAT Statement AND Execute VAT Payment	SoD violation in VAT Management might lead to ...Lorem ipsum dolor sit amet, consectetur adipiscing elit, sad
Lorem ipsum	Lorem ipsum	Lorem ipsum	Lorem ipsum	Lorem ipsum	Lorem ipsum	SOD	Mid	Lorem ipsum dolor sit amet, consectetur adipiscing elit, sadLorem ipsum dolor sit amet, consectetur adipiscing elit, sad

IDEAS Glossary – Activity Tree

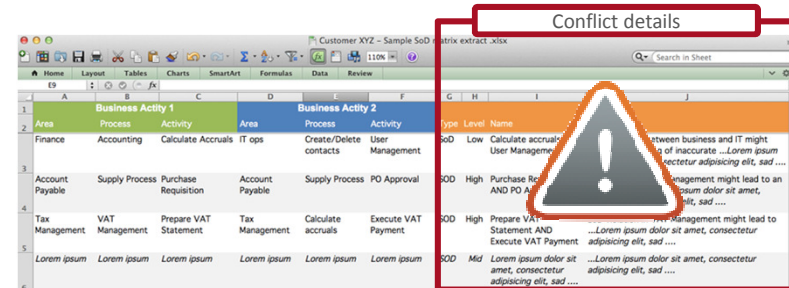
Area	Process	Activity	Type	Level	Name	Description
Finance	Accounting	Create/Delete Contacts	SoD	Low	Calculate accruals AND User Management	SoD violations between business and IT might cause a processing of inaccurate ...Lorem ipsum dolor sit amet, consectetur adipiscing elit, sad ...
Account Payable	Supply Process	Purchase Request	SoD	High	Purchase Request AND PO Approval	SoD violation in PO Management might lead to an unauthorized ...Lorem ipsum dolor sit amet, consectetur adipiscing elit, sad ...
Tax Management	VAT Management	Statement Management	SoD	High	Prepare VAT Statement AND Execute VAT Payment	SoD violation in VAT Management might lead to ...Lorem ipsum dolor sit amet, consectetur adipiscing elit, sad ...
...

The xls based activity list can be converted in IDEAS in a tree like representation

- *Pure business level description of a company's tasks*
 - Derived from Auditor / Advisor recommendations
 - OR Extracted from company existing GRC/PM systems
 - OR Created from industry specific templates



IDEAS Glossary – SoD Constraints

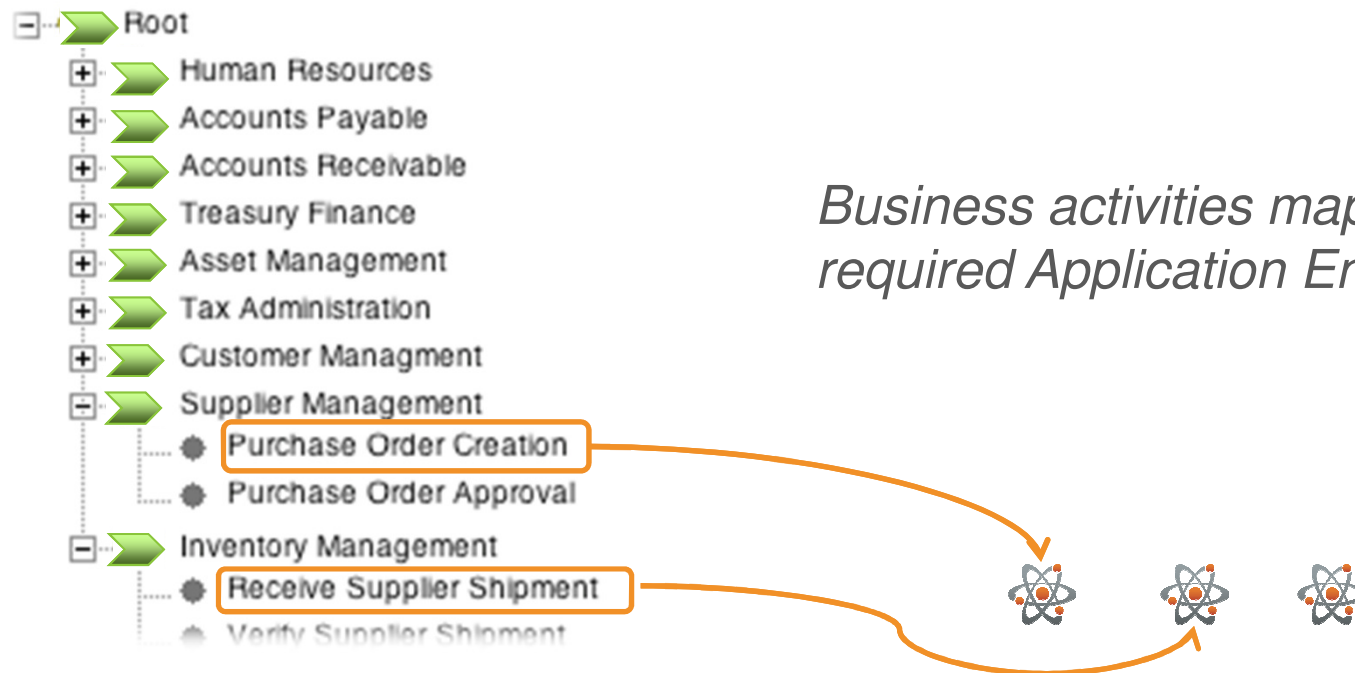



Business Activity 1			Business Activity 2			Type	Level	Name
Area	Process	Activity	Area	Process	Activity			
Finance	Accounting	Calculate Accruals	IT ops	Create/Delete	User Management	SOD	Low	Calculate accruals and user management might lead to an inaccurate...
Account Payable	Supply Process	Purchase Request	Account Payable	Supply Process	PO Approval	SOD	High	Purchase Request and PO Approval management might lead to an inaccurate...
Tax Management	VAT Management	Prepare VAT Statement	Tax Management	Calculate accruals	Execute VAT Payment	SOD	High	Prepare VAT Statement and Calculate accruals management might lead to an inaccurate...
...	SOD	Mid	...

SoD constraints are links among activities, also coming from the xls version

- *Pure business level description of a Risk - no IT details*
 - Derived from Auditor / Advisor recommendations
 - OR Extracted from company existing GRC/PM systems
 - OR Created from industry specific templates

IDEAS Glossary – Technical Transformation



- Making IT Entitlement names understandable to business users
- Provided by the application owners



IDEAS Glossary – SoD Modeling

Two complementary ways to look at the application estate....

User and Roles

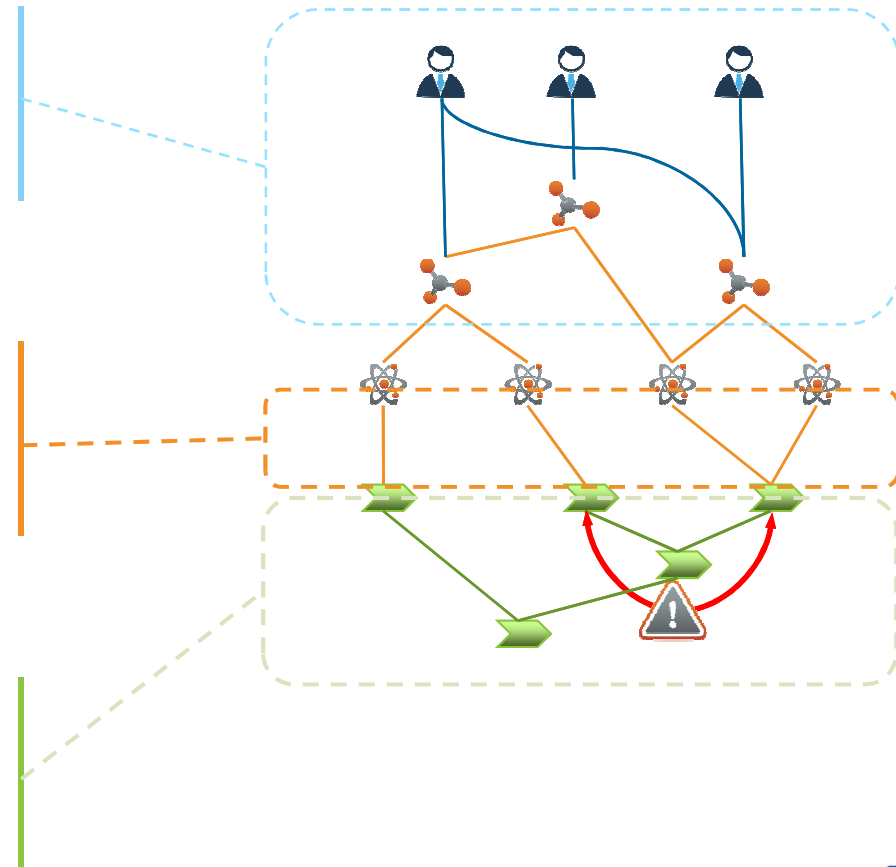
- Subject of the violation analysis

Technical Transformation

- Application-owner defined

Activities and SoD rules

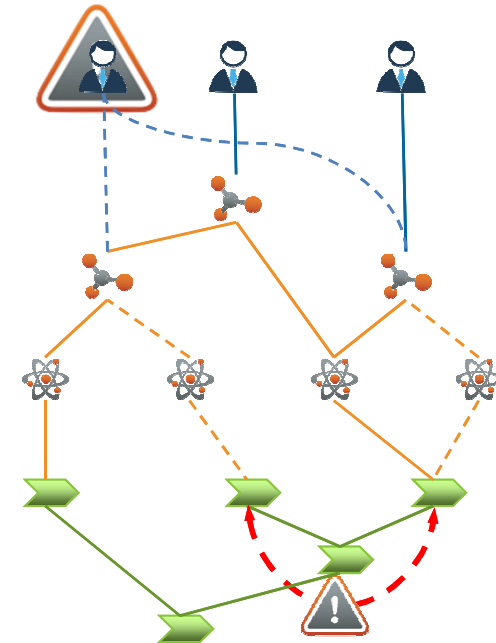
- Best practices or business-owner defined



IDEAS Glossary - User Analysis

User Violation

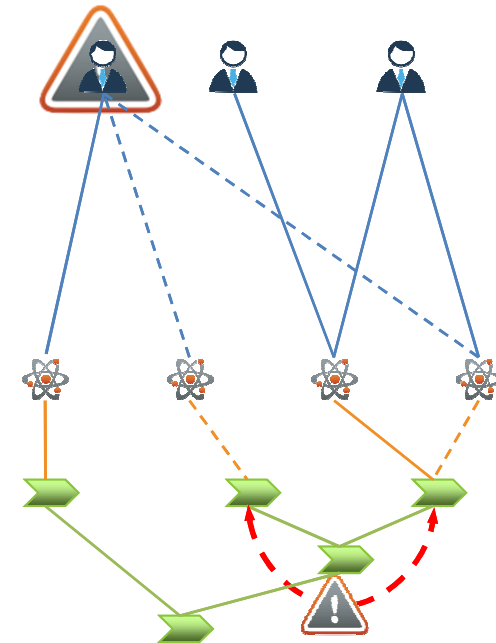
- User assigned to entitlements linked to conflicting activities, either through conflicting roles...



IDEAS Glossary - User Analysis

User Violation

- User assigned to entitlements linked to conflicting activities, either through conflicting roles...or directly



Roles Vs Activities

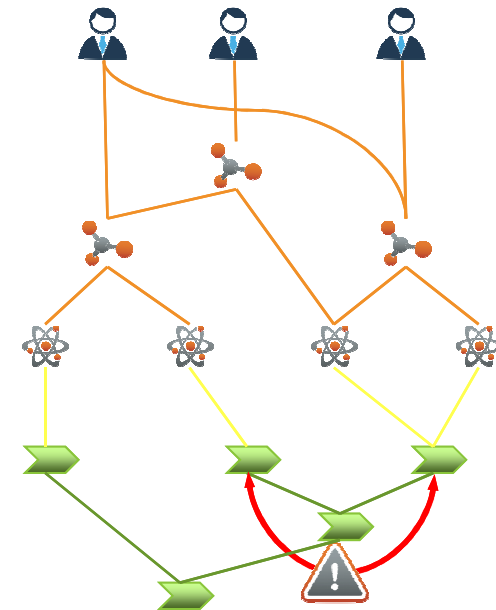
Clean distinction between Access delivery Vs. Access control

Roles

- Best Approach for effective Provisioning

Activities

- Best approach for effective SoD modeling

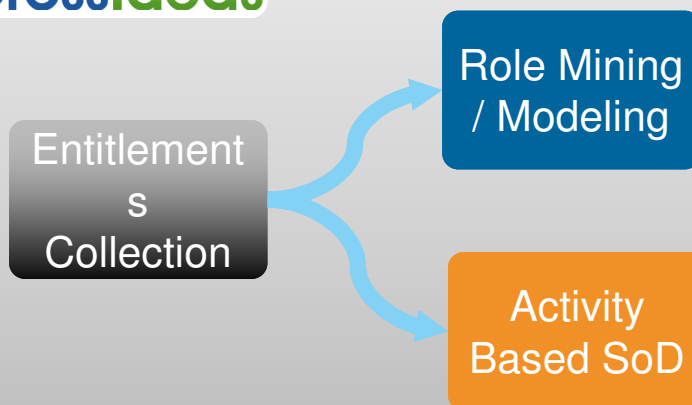


Activity vs. Role Based SoD



Role Based SoD

- Role needs to come first
- Access Review to allow Role Mining is further delaying the SoD Introduction



Activity Based SoD

- SoD Analysis can be the first, or the only, objective
- Roles can be the subject of the SoD Analysis



Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed or misappropriated or can result in damage to or misuse of your systems, including to attack others. No IT system or product should be considered completely secure and no single product or security measure can be completely effective in preventing improper access. IBM systems and products are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT SYSTEMS AND PRODUCTS ARE IMMUNE FROM THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

Thank You
www.ibm.com/security



© Copyright IBM Corporation 2014. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, these materials. Nothing contained in these materials is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software. References in these materials to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. Product release dates and/or capabilities referenced in these materials may change at any time at IBM's sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.



