

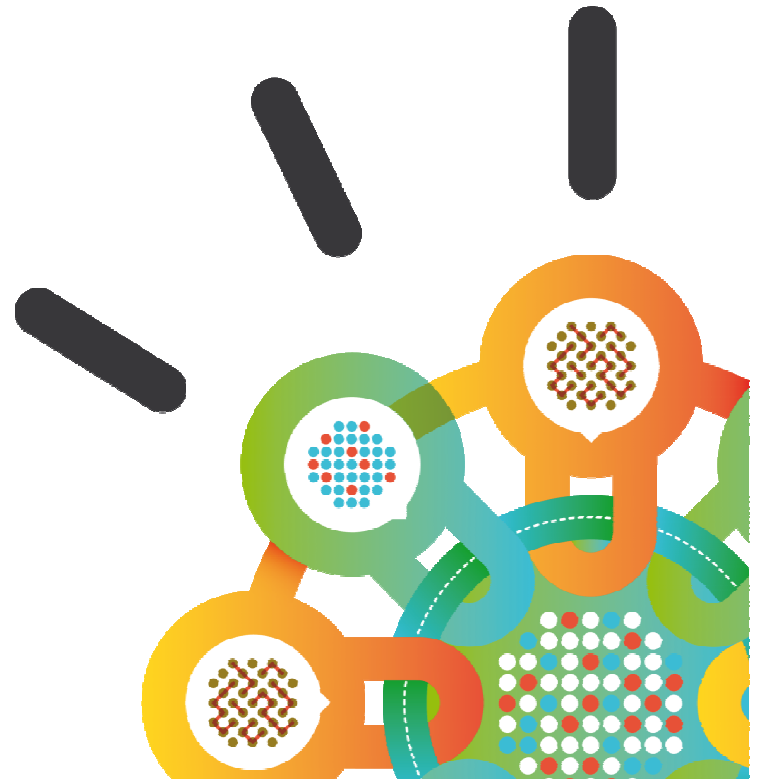
Security Intelligence.
Think Integrated.

CrossIdeas

Company and Product Overview

Andrea Rossi
VP Sales @ CrossIdeas - an IBM
Company

Andrea.rossi@crossideas.com



Senior executives drive Identity Governance adoption

- **Financial Reporting**

SOX, CA 52-313, Turnbull, LSF,
Transparency Directive, JSOX, MAR, L.262

- **Industry Mandated Initiatives**

Basel II, Solvency II, GLBA, FERC/NERC,
FFIEC, FISMA, HIPAA/HITECH, ITAR,
Smart Grid

- **Privacy Mandates**

PCI, State Based (CA 1386, MA Privacy
201), Country Based, EU Data Protection

- **CxO/Senior Executives**

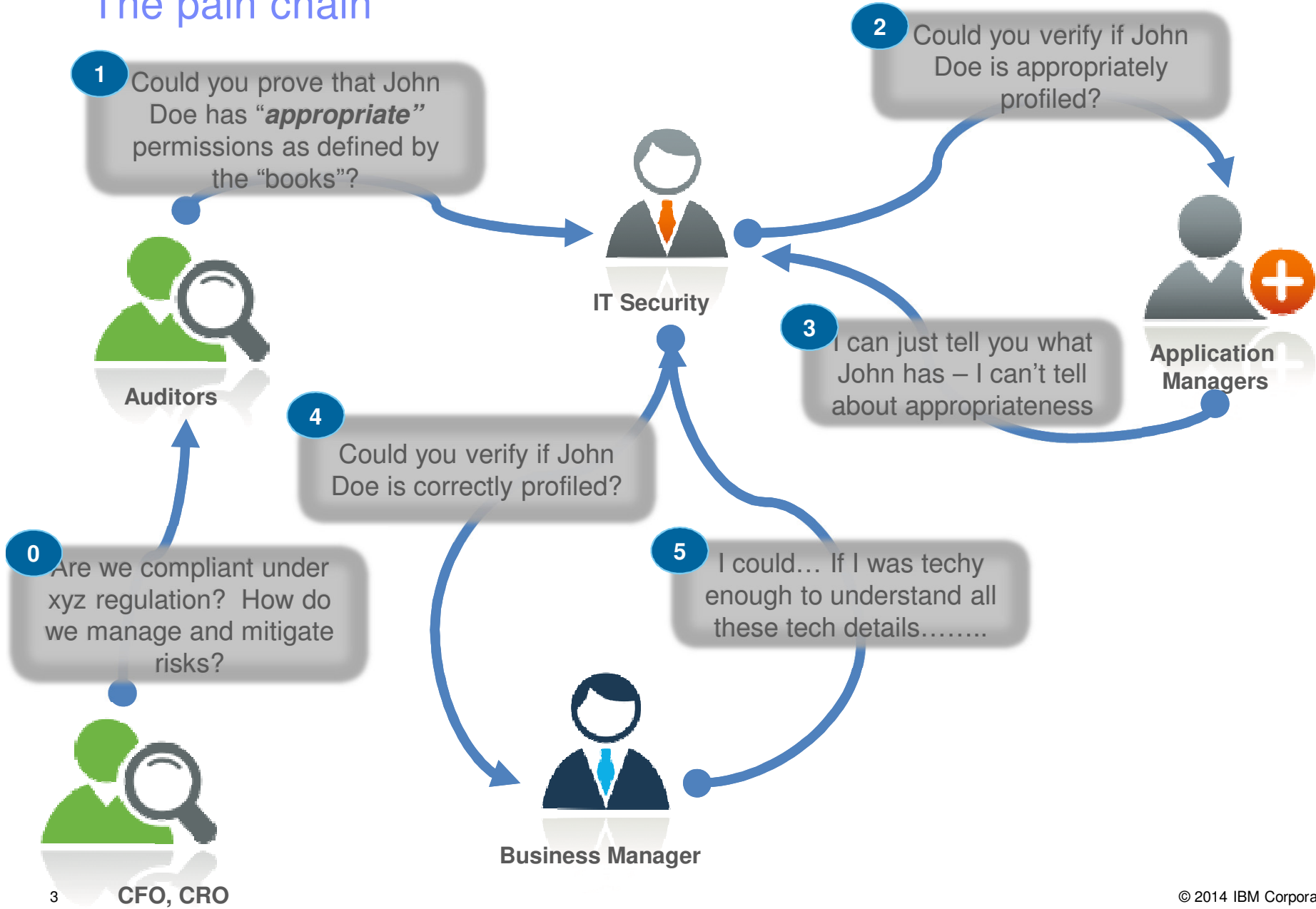
take individual responsibility for the
accuracy and completeness

- **Auditors**

require certified information to
approve Accounts / Risk Mgt reports



The pain chain



Typical Audit findings



- X Manual efforts to retrieve data:** weeks, meetings, 3rd party consulting fees.
- X Inability to detect existing ‘toxic combinations’:** privileged application accounts assigned to ‘standard’ employees, conflicting permissions creating SoD violations.
- X Inability to determine ‘who approved what when’:** many approval processes, ‘like Mike’ habits, etc.

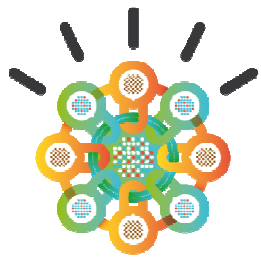
About CrossIdeas



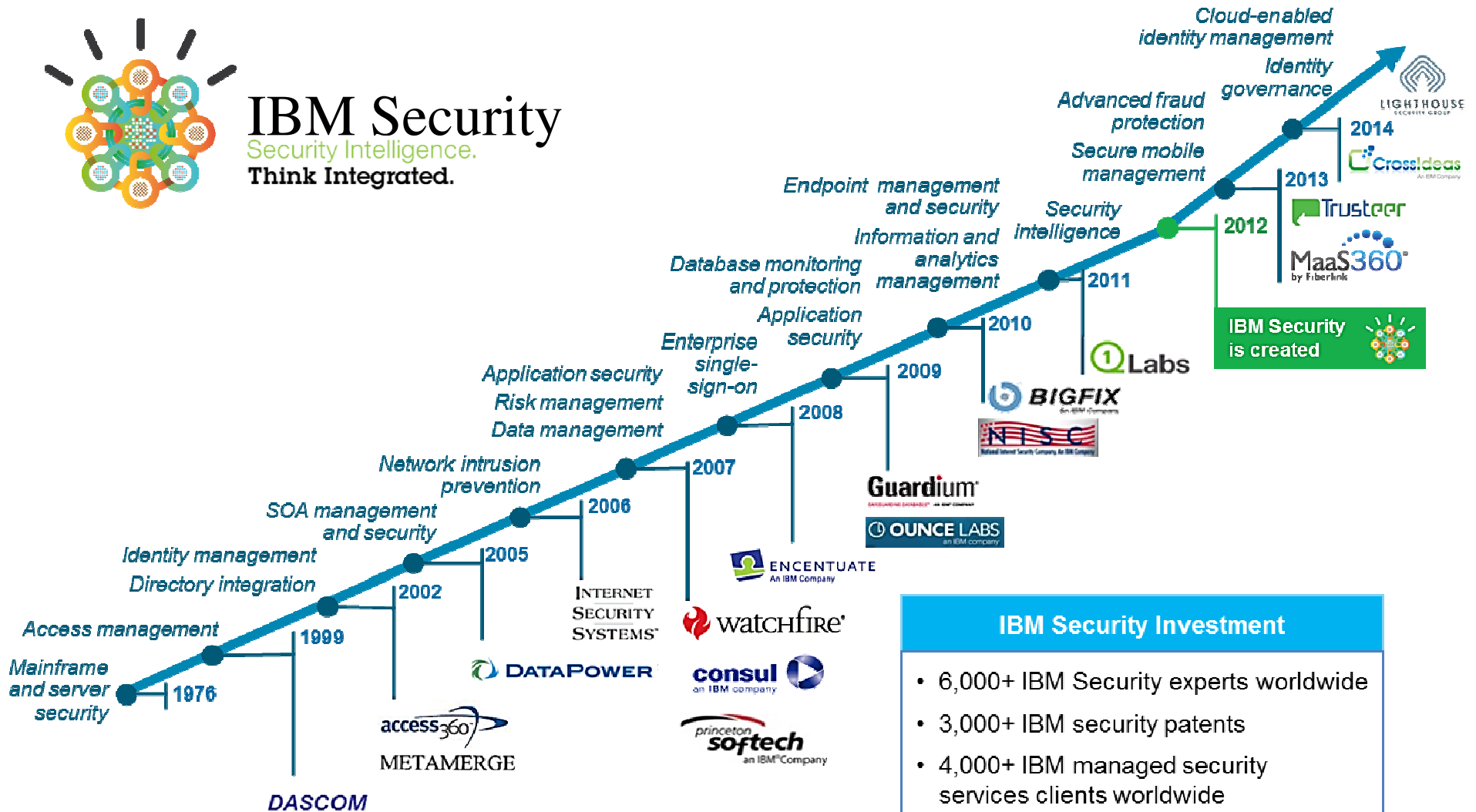
CrossIdeas is a leading player of Identity Governance Solutions, enabling organizations to achieve their Compliance, Audit and Access Risk Management objectives

- Founded in 2011, product originates in 2005
- HQ in Italy (Rome)
- Rated as “visionaire” in the Gartner IAG MQ 2011/2012 and IGA 2013
- Fortune 500 companies run CrossIdeas
- Acquired by IBM on July 31st 2014

Now part of IBM Security Division...



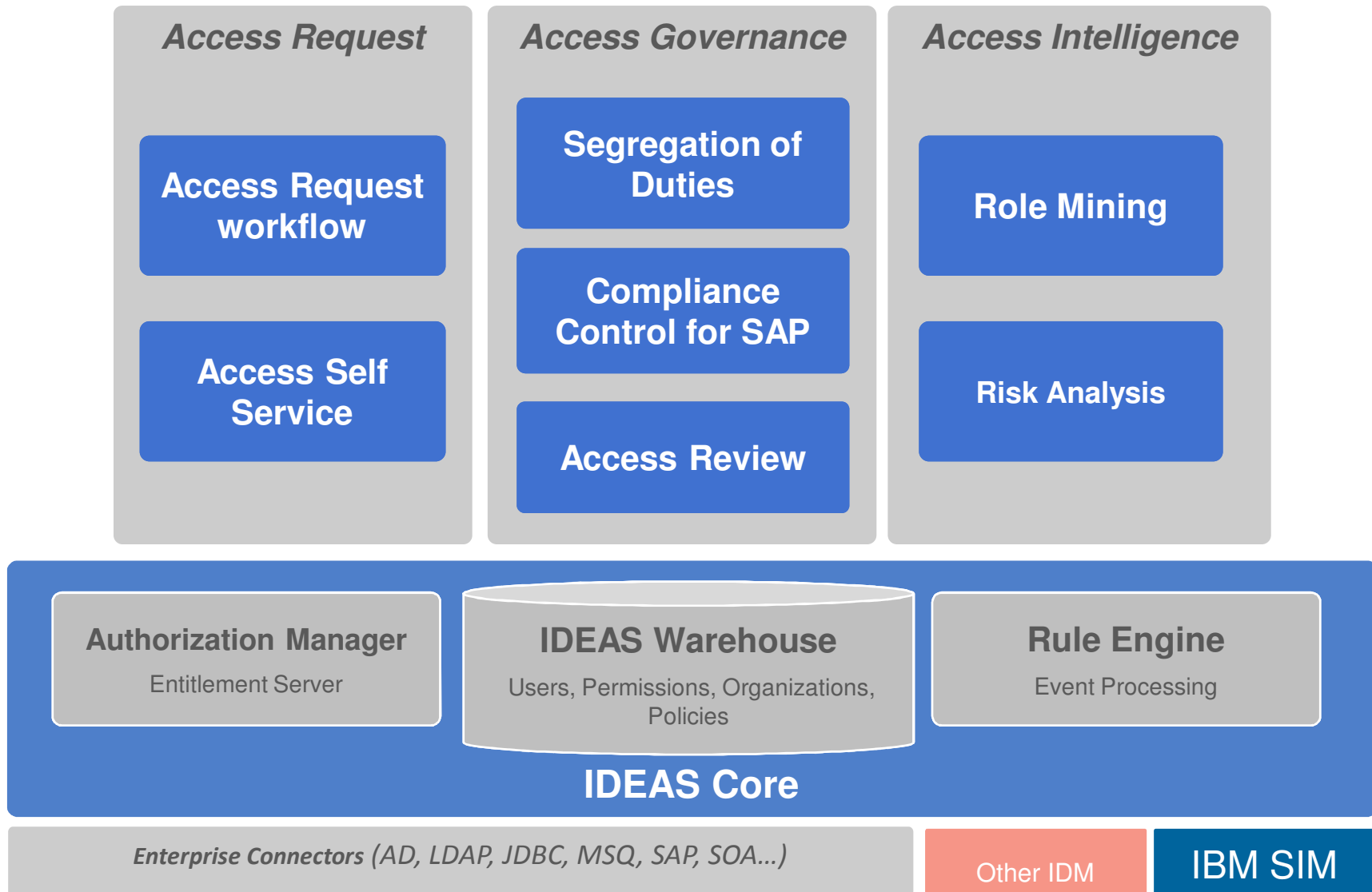
IBM Security
Security Intelligence.
Think Integrated.



IBM Security Investment

- 6,000+ IBM Security experts worldwide
- 3,000+ IBM security patents
- 4,000+ IBM managed security services clients worldwide
- 25 IBM Security labs worldwide

IDEAS Solution Modules



IBM/CrossIdeas @ a glance

The 'ISIM-CrossIdeas' integration:

- Provides **bidirectional integration** between IBM SIM and CrossIdeas' IDEAS
- **Adds** strong Identity Governance capabilities, SAP specific controls, innovative Access/Role Intelligence to SIM

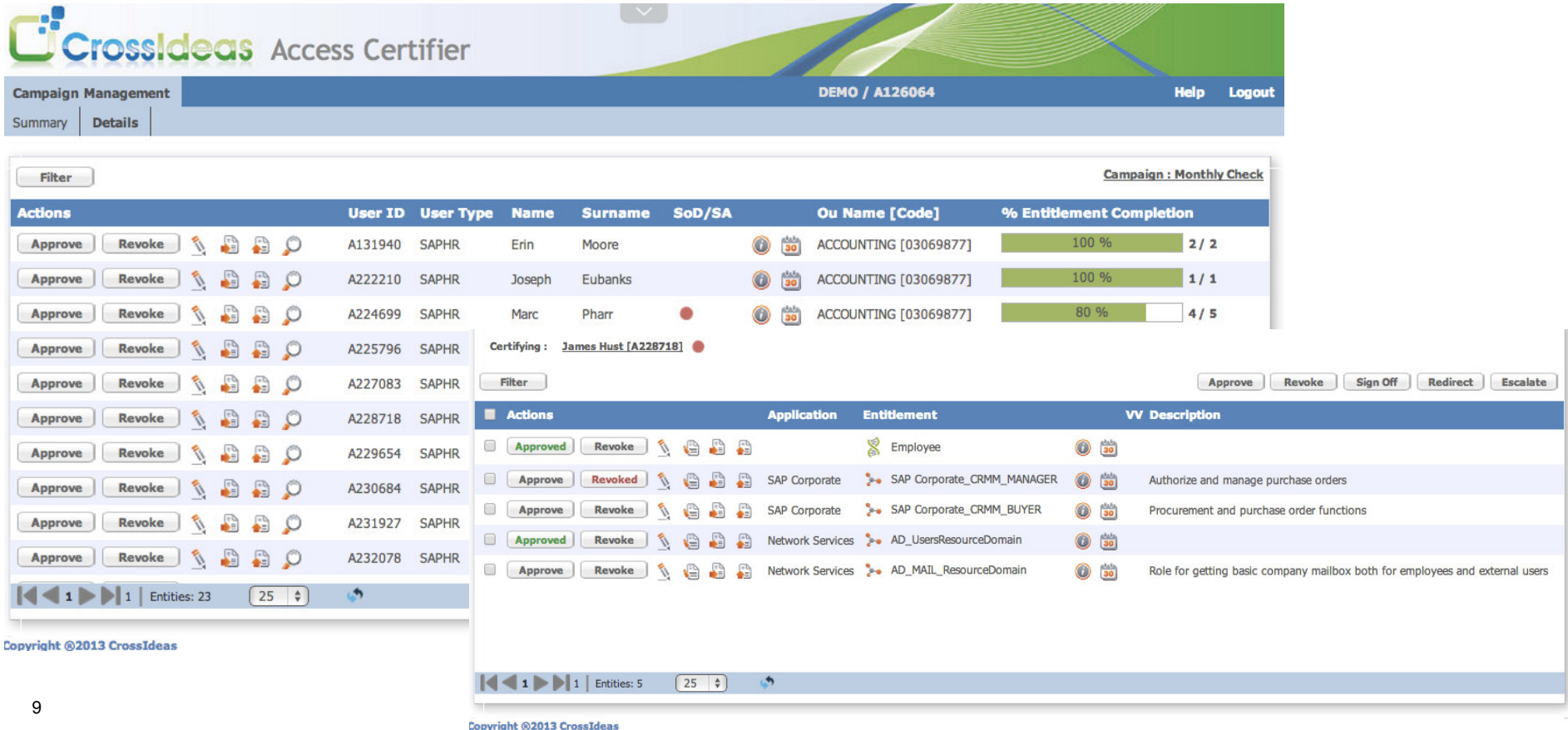


- **ISIM customers** can rapidly introduce Access Governance capabilities with no changes in their existing ISIM environment
- **Non-ISIM customers** can introduce Governance capabilities and then either **a)** expand into Provisioning, or **b)** replace their existing Identity management system (Sun, NetIQ, ...)

Use Case #2: Access Certification

IDEAS key features

- Business ready, intuitive interface
- Multi-attribute campaign: by Application, by OU, time-limited, etc
- Workflow based, multi-level approvals












The screenshot displays the CrossIdeas Access Certifier interface. At the top, it shows the 'Campaign Management' section with a 'Summary' tab selected and 'Details' tab. The campaign is identified as 'Monthly Check' with a 'DEMO / A126064' identifier. The main area shows a list of users being certified, with columns for 'Actions', 'User ID', 'User Type', 'Name', 'Surname', 'SoD/SA', 'Ou Name [Code]', and '% Entitlement Completion'. The users listed are Erin Moore, Joseph Eubanks, and Marc Pharr. Below this, a detailed view for user 'James Hust [A228718]' is shown, including a 'Filter' button and a table of entitlements. The entitlement table has columns for 'Application', 'Entitlement', and 'VV Description'. The entitlements listed are 'Employee', 'SAP Corporate - SAP Corporate_CRMM_MANAGER', 'SAP Corporate - SAP Corporate_CRMM_BUYER', 'Network Services - AD_UsersResourceDomain', and 'Network Services - AD_MAIL_ResourceDomain'. The interface includes navigation controls at the bottom, such as 'Entities: 23' and '25' per page, and 'Entities: 5' and '25' per page for the detailed view.

Copyright ©2013 CrossIdeas

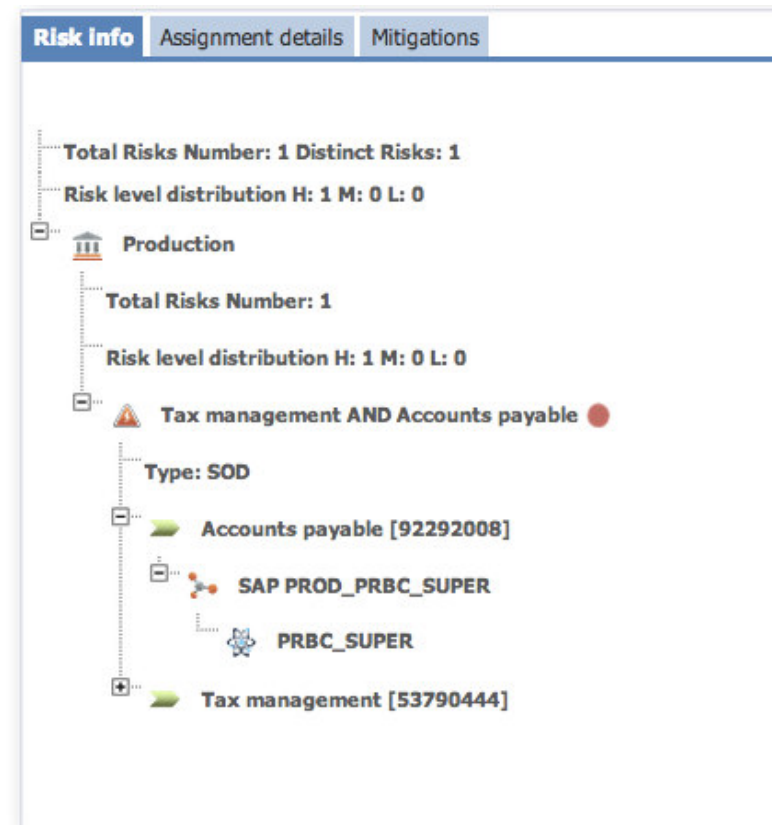
Use Case #2: Segregation of Duty

IDEAS key features

- Process-based SoD, does not require Role modeling
- Multi-domain, attribute based SoD maps the complexity of business apps
- Specific SoD controls for SAP

Filter					
SoD	RMD	Name	Surname	Identifier	DN
●	↓	 Giorgio	Callas	AE00189	
●	↓	 Miro	Van Basten	AE00190	
●	↓	 Deborah	Correa	A264404	
●	←	 Sandra	Harmon	A123048	
●	↓	 Julio	Hutt	A132083	
●	↓	 Serafina	Hackett	A223841	
●	↓	 Marc	Pharr	A224699	
●	←	 Kimberly	Strausbaugh	A254902	
●	←	 James	Petty	A231927	
●	↓	 Dorothy	Fultz	A232021	
●	←	 Melissa	Ragan	A254893	

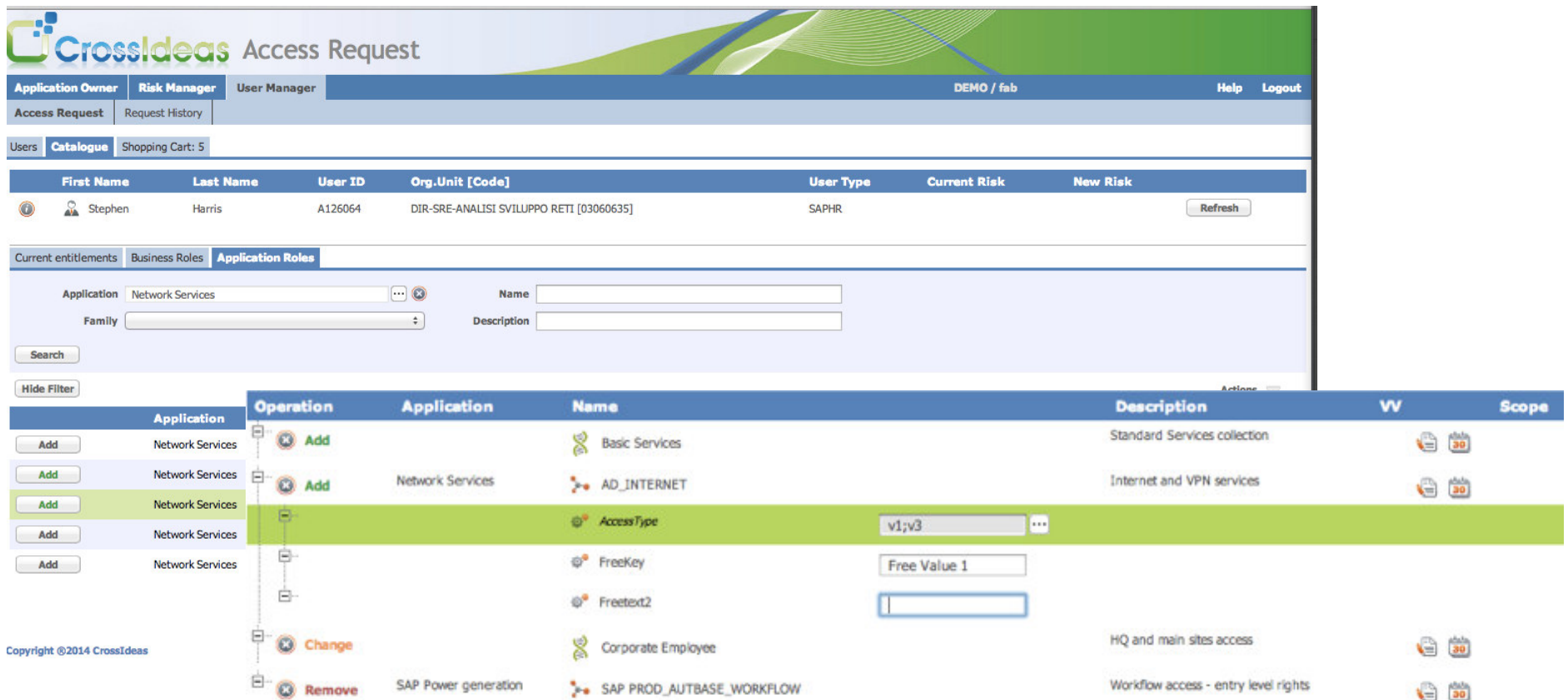
Entities: 43 25



Use Case #3: Access Request Management

IDEAS key features

- Shopping Cart approach eases Business adoption
- Preventive Segregation of Duty takes control of risk
- Fine-grain application rights dramatically reduce complexity



CrossIdeas Access Request

Application Owner | Risk Manager | User Manager | DEMO / fab | Help | Logout

Access Request | Request History

Users | Catalogue | Shopping Cart: 5

First Name	Last Name	User ID	Org.Unit [Code]	User Type	Current Risk	New Risk
Stephen	Harris	A126064	DIR-SRE-ANALISI SVILUPPO RETI [03060635]	SAPHR		

Current entitlements | Business Roles | Application Roles

Application: Network Services | Name: | Family: | Description: | Search: | Hide Filter: | Actions: |

Application	Operation	Application	Name	Description	W	Scope
Add	Add	Network Services	Basic Services	Standard Services collection		
Add	Add	Network Services	AD_INTERNET	Internet and VPN services		
Add		Network Services	AccessType	v1;v3		
Add		Network Services	FreeKey	Free Value 1		
Add		Network Services	Freertext2			
	Change		Corporate Employee	HQ and main sites access		
	Remove	SAP Power generation	SAP PROD_AUTBASE_WORKFLOW	Workflow access - entry level rights		

Copyright ©2014 CrossIdeas

CrossIdeas Capabilities: Highlights

- **An ‘Unusually clean data model for IGA’** *(ref. Gartner)*
 - SoD based on ‘business processes’, allows to implement it without having to go through ‘Role design’ first.
- **The only IGA player with SAP specific controls**
 - Fine-grain SoD controls on users and roles.
 - One product to manage SAP and non SAP apps.
- **Interoperate with existing Provisioning/IDM platforms**
 - Designed for “Embrace & Extend” approach.
 - Native integration with IBM SIM and NetIQ IDM.
- **Scalable architecture, field proven**
 - J2EE architecture, customers with 100.000+ users.
 - Product originates (2005) as ‘Dynamic authorization server’.



IBM Security

CrossIdeas: Client Snapshot



INSURANCE



GENERALI

helvetia



Posteitaliane

FINANCIAL SERVICES



**SOCIETE
GENERALE**



**Banca Popolare
di Milano**



**Banca
Marche**

ENERGY & UTILITIES

e.on

Alitalia



**Informatica
Trentina SpA**



ENERGY IN TUNE WITH YOU.

MANUFACTURING

Ferrari

Salvatore Ferragamo



WhiteWave



PIAGGIO*

PUBLIC SECTOR



Ministero della Giustizia

Percorsi chiari e precisi: un tuo diritto

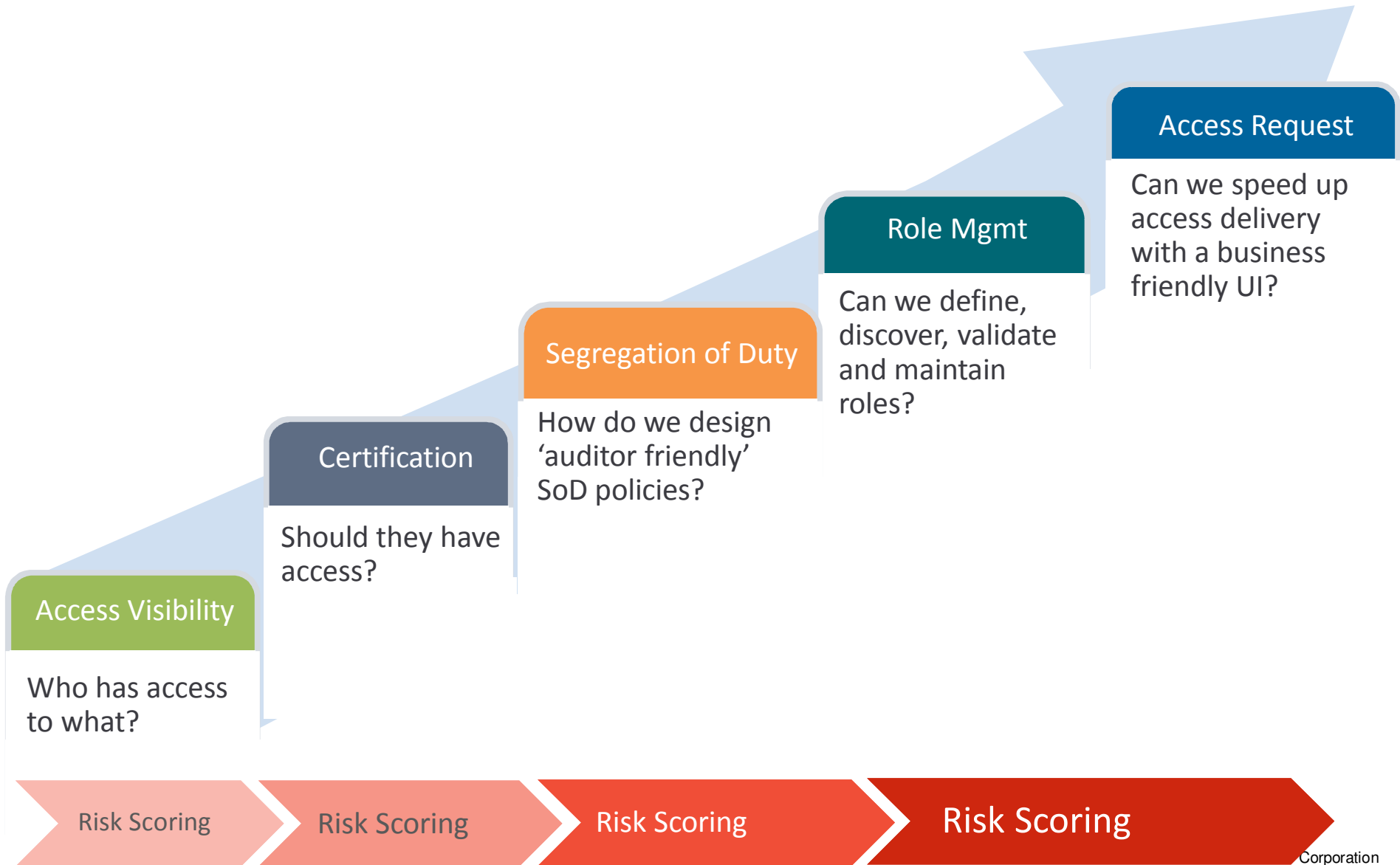


**Aeroporti
di Roma**

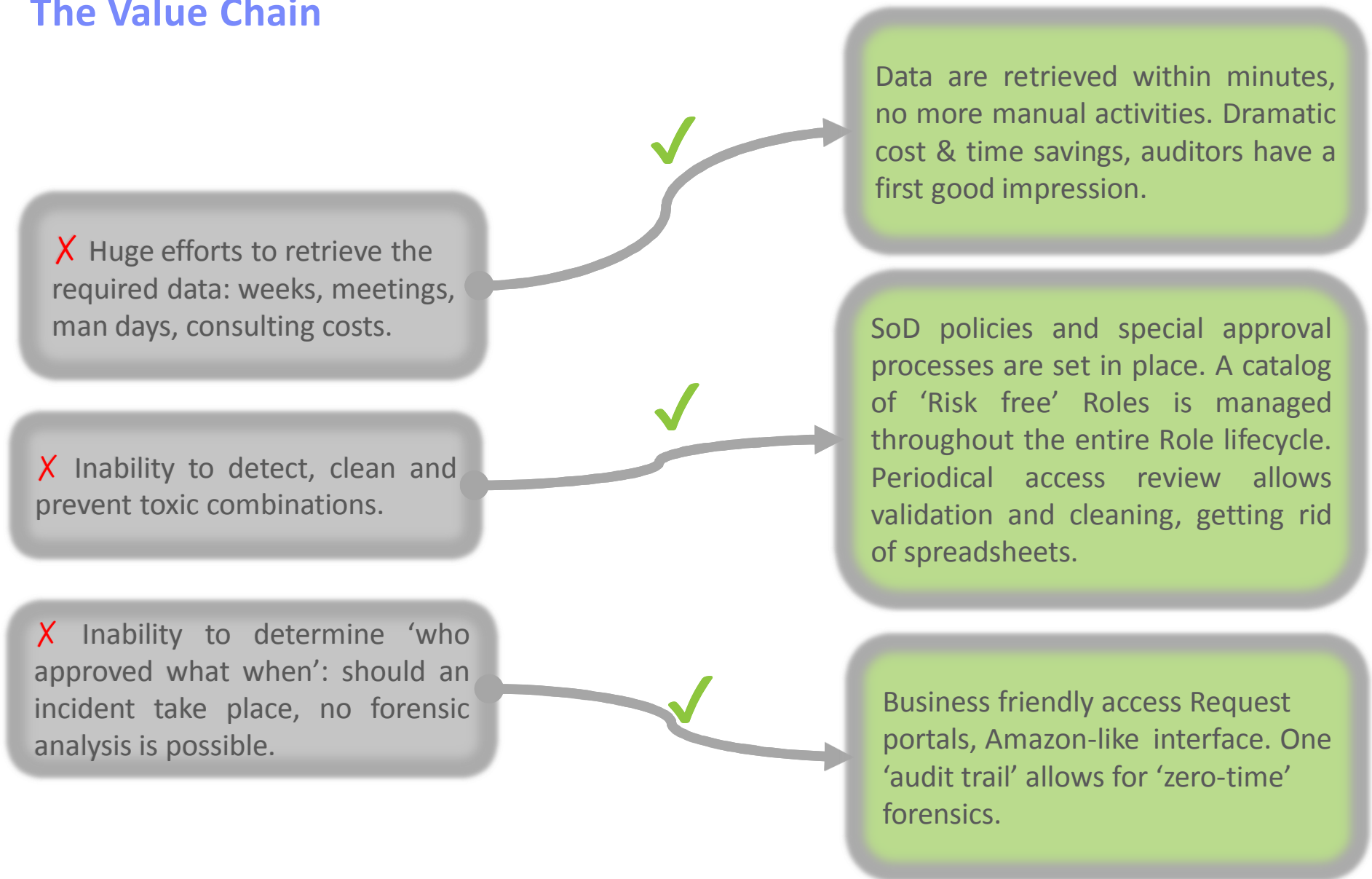
MINISTERO DELLA SALUTE



IGA Maturity Model: where are you now?



The Value Chain



The pain chain

1 Could you prove that John Doe has “appropriate” permissions as defined by the “books”?

2 Could you verify if John Doe is appropriately profiled?

Lesson learned

- Do not neglect the ‘**Translation & Readability**’ requirements
- When the Audit pressure is high, stars align between IT and Business
- Plan for multiple, short phases

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.