DKMS

WE DELETE BLOOD CANCER

Supporting Information Security Management with LeanIX

Dr. Kai Höfler
Enterprise Architect DKMS

Dennis Endert
Manager GRC DKMS

The Founding Of DKMS

Our story began in 1991, when our founder, Dr. Peter Harf, lost his wife Mechtild to leukemia. Peter set about delivering on the promise he had made to his wife: to find a matching donor for every blood cancer patient.

At that time, there were only 3,000 potential stem cell donors available to provide a transplant in Germany. Peter Harf founded DKMS Germany, and within just one year the number of stem cell donors increased to 68,000.

Today DKMS operates in Germany, the USA, Poland, the UK, Chile, in India together with DKMS and in South Africa with our partner The Sunflower Fund. We register more than 1 million new potential donors globally each year and so far have provided over 86,000 second chances at life.

Bringing Hope To People All Over The World

10,213,281 active DKMS donors

More than **86,000** second chances at life have been provided by DKMS

Over 1 Million new donors registered per year

20 stem cell collections per day

27 percent of all potential blood stem cell donors worldwide are registered with DKMS

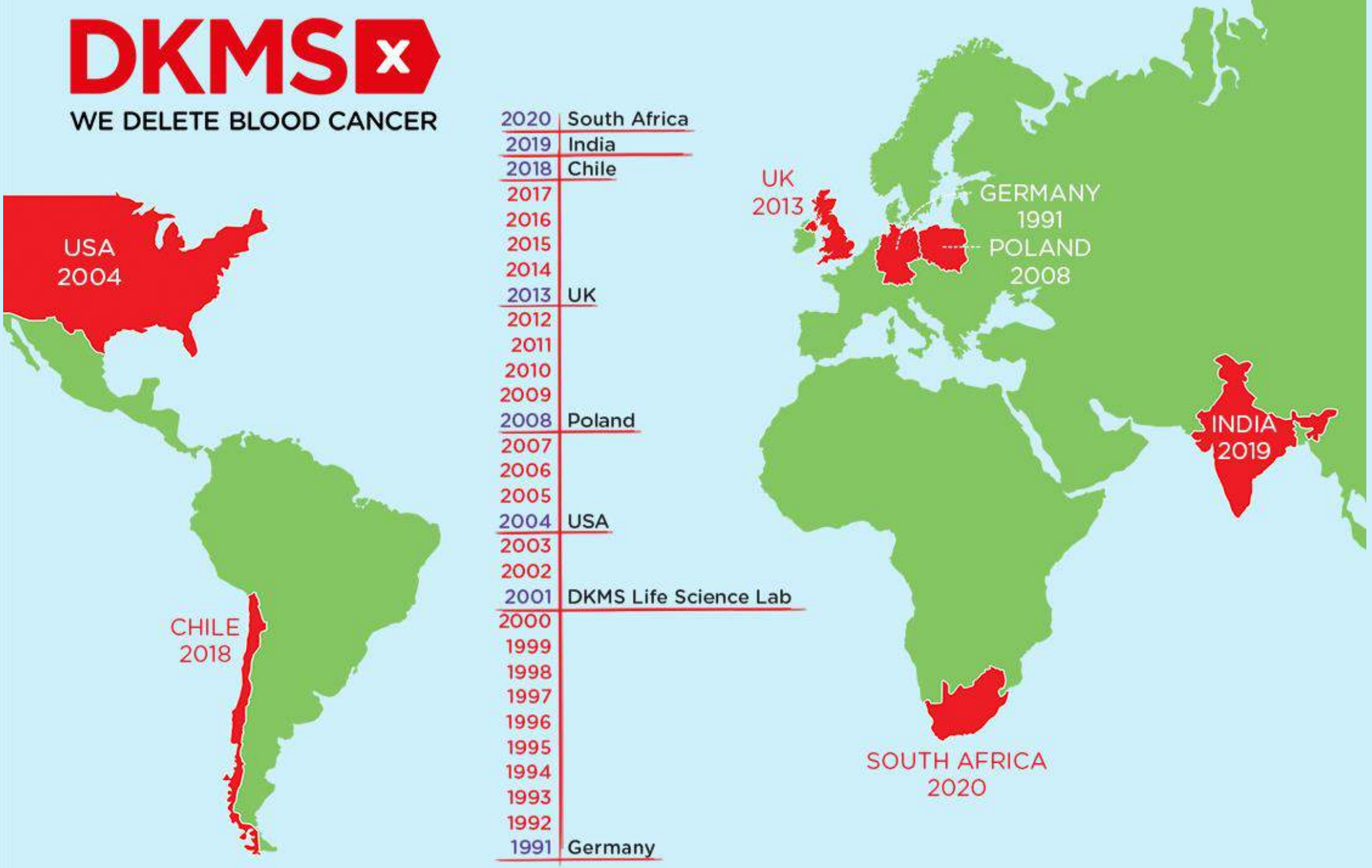
40 percent of all unrelated stem cell transplants worldwide are made possible by DKMS donors

75 percent of blood stem cell collections are sent abroad

We provide patients in **57** different countries a second chance at life

DKMS

WE DELETE BLOOD CANCER



2020	South Africa
2019	India
2018	Chile
2017	
2016	
2015	
2014	
2013	UK
2012	
2011	
2010	
2009	
2008	Poland
2007	
2006	
2005	
2004	USA
2003	
2002	
2001	DKMS Life Science Lab
2000	
1999	
1998	
1997	
1996	
1995	
1994	
1993	
1992	
1991	Germany

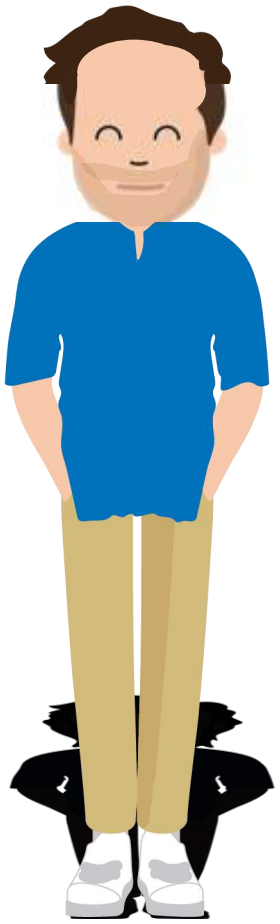
Vita

KAI HÖFLER

Software- and Enterprise Architecture are the professional passions of Kai.

As **Enterprise Architect** and Team Lead for Software Development he is introducing EAM in DKMS and is working together with the other enterprise functions to drive the digitalization of the DKMS.

He formerly worked for one of the leading IT consulting companies as principal architect and as enterprise architect for an insurance company.



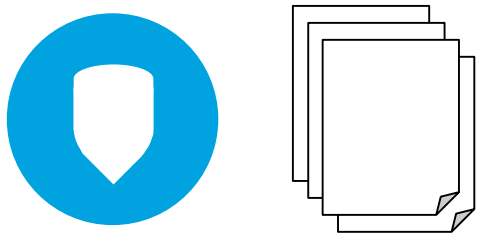
DENNIS ENDERT

Dennis Endert is the **Manager for IT-Security, Governance, Risk & Compliance** at DKMS and responsible for establishing and maintaining the Information Security Management System.

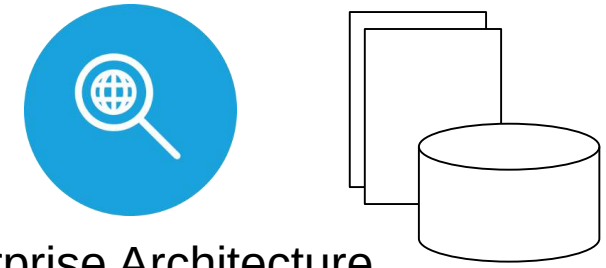
He formerly worked for an audit firm where he gained deep insights into a large number of financial service providers and advised them regarding IT compliance.

He holds CISA, TISP, ISO/IEC27001, ITIL and ITGCP certifications.

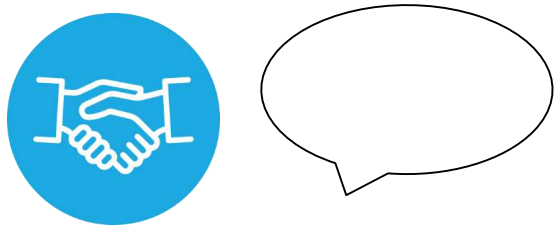
Different corporate functions need the same related information



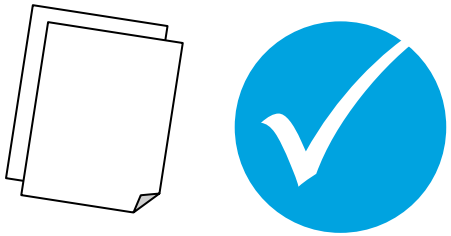
Information Security Management (ISMS)



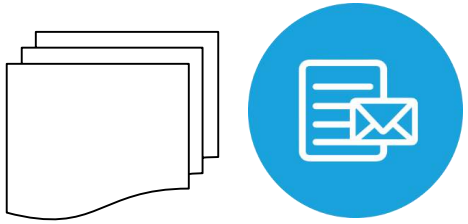
Enterprise Architecture Management



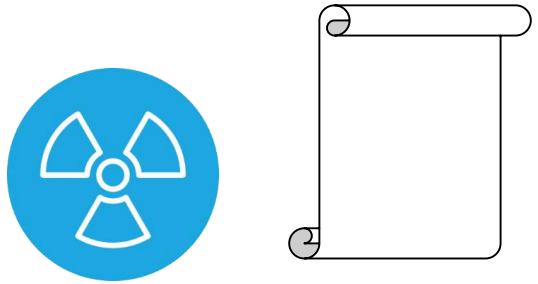
Provider Management



Quality Management (QM)



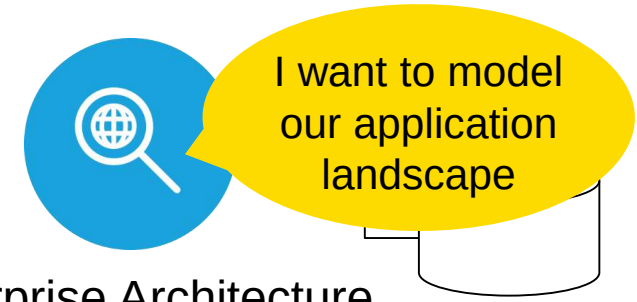
Data Protection Management



Business Continuity Management

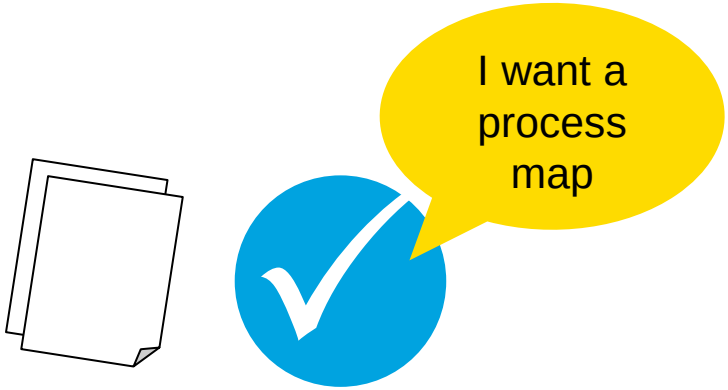
Different corporate functions need the same related information

Information Security Management (ISMS)

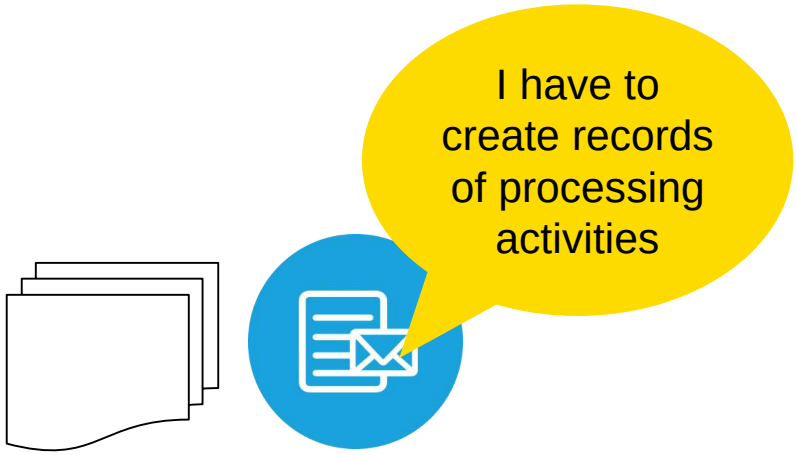


Enterprise Architecture Management

Provider Management



Quality Management (QM)

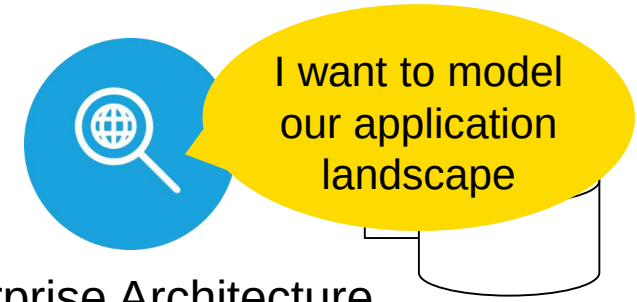


Data Protection Management

Business Continuity Management

Different corporate functions need the same related information

Information Security Management (ISMS)



Enterprise Architecture Management

Provider Management

Why not integrate them?

(starting with ISMS and EAM)

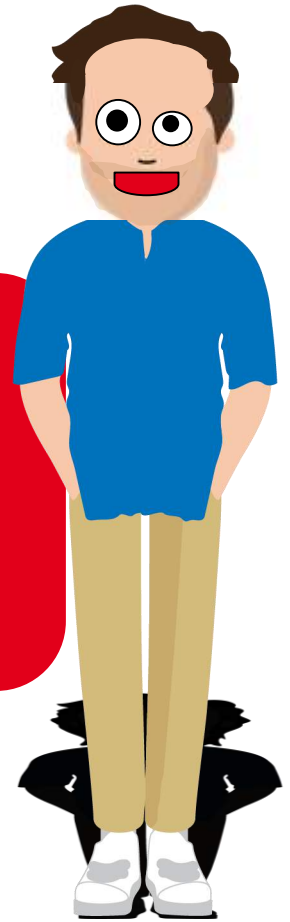
Quality Management (QM)

Data Protection Management

Business Continuity Management

Different corporate functions need the same related information

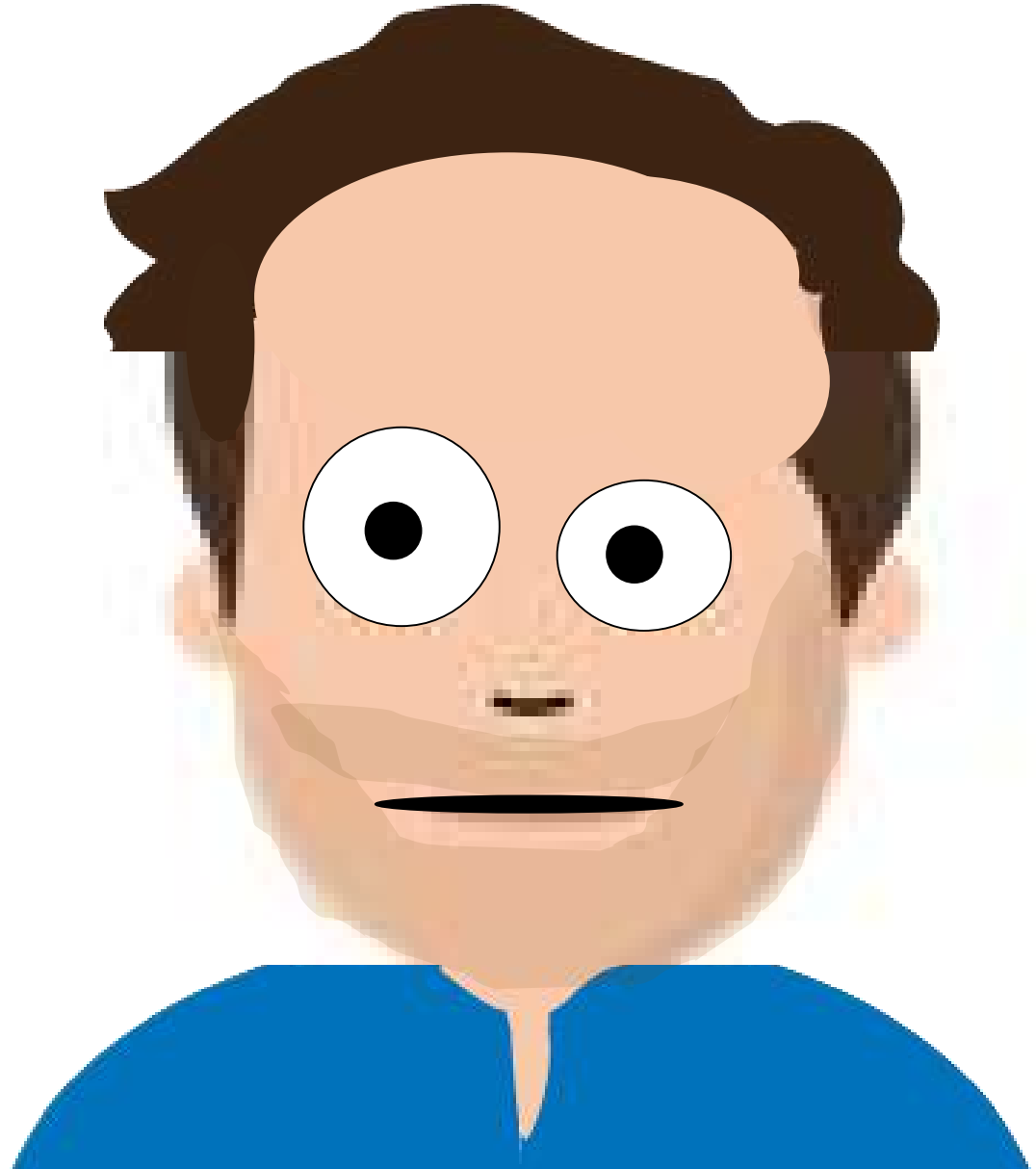
A HUGE model that contains ALL the information!



Different corporate functions need the same related information

Different corporate functions need the same related information

Different corporate functions need the same related information



The basic principles of our information security management approach

CONFIDENTIALITY

Confidentiality "is the property, that information is not made available or disclosed to unauthorized individuals, entities, or processes."

- C1 Public
- C2 Sensitive
- C3 Restricted
- C4 Confidential

INTEGRITY

Integrity means maintaining and assuring the accuracy and completeness of data over its entire lifecycle.

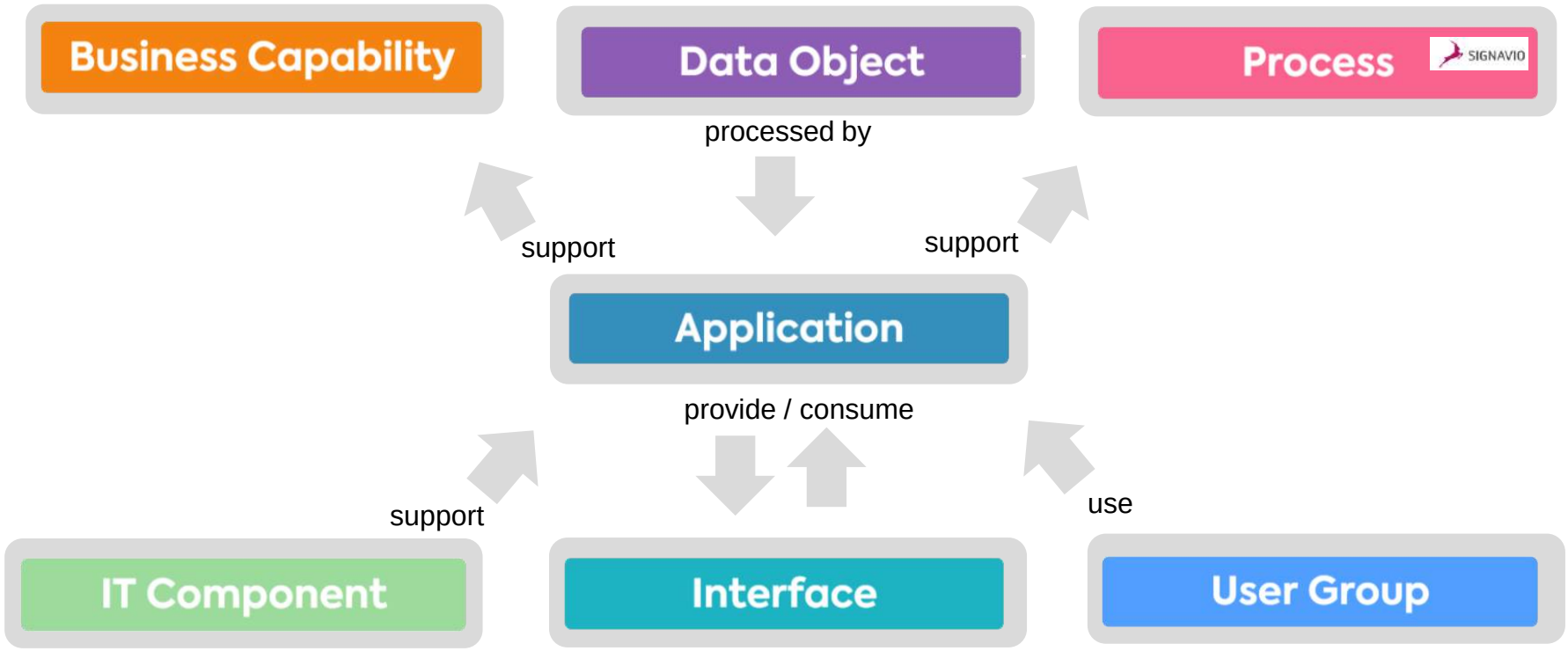
- I1 Low
- I2 Normal
- I3 High
- I4 Very High

AVAILABILITY

Availability requires that information must be available when it is needed, to serve its purpose.

- A1 Administrative Service
- A2 Business Operational
- A3 Business Critical
- A4 Mission Critical

The core of our Enterprise Architecture Model is also the basis for our ISMS



The security goals are identified based on the requirements of Data Objects and Business Processes

Confidentiality and Integrity of Data Objects is documented in LeanIX:

- Tag **Confidentiality** (= Field „Data Classification“**)**
- Tag **Integrity**

C Confidentiality

I Integrity

A Availability

C4 I3

Data Object

Process

SIGNAVIO

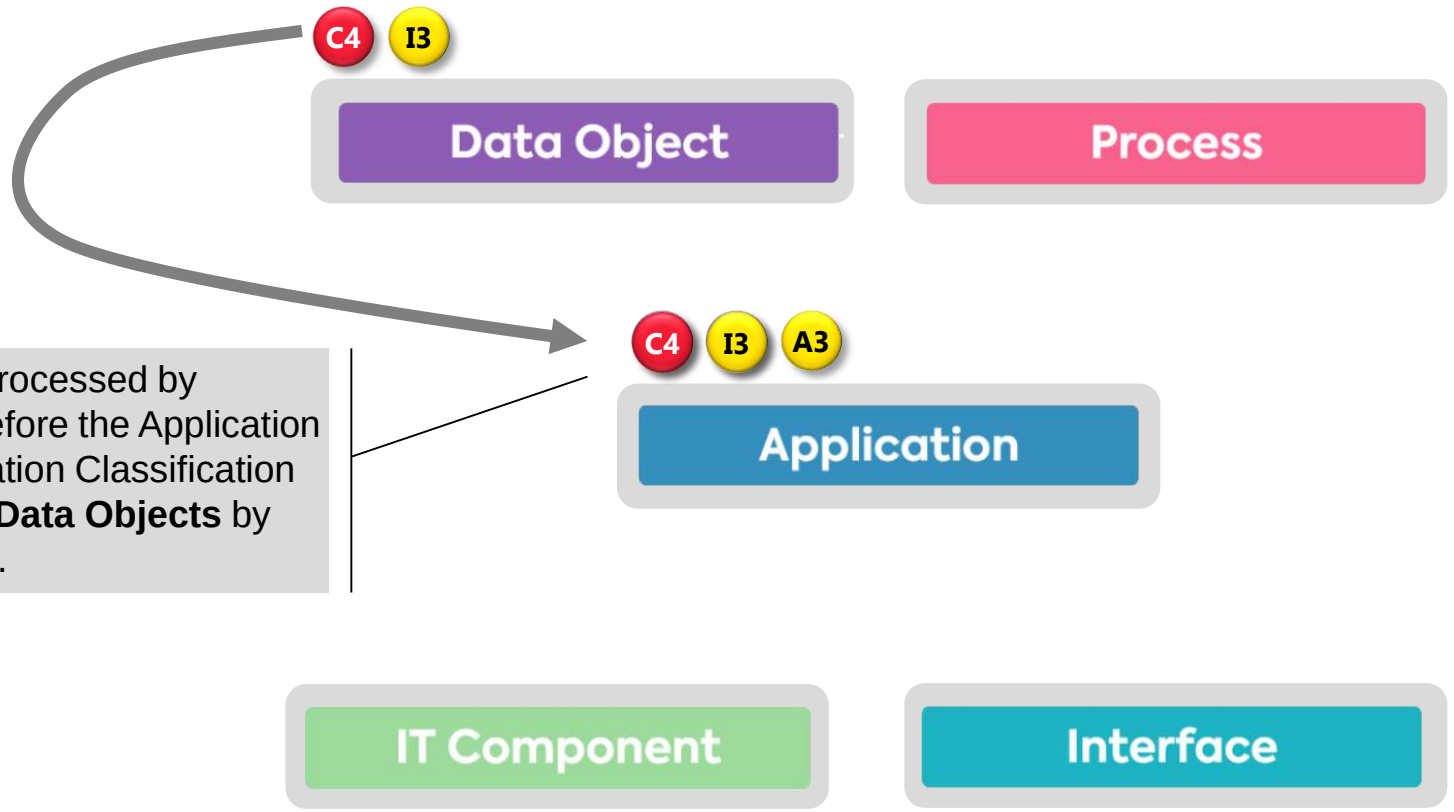
A3

Application

Availability of Applications is determined based on the supported Business Processes.

- Tag **Availability** (= Field „Business Criticality“)

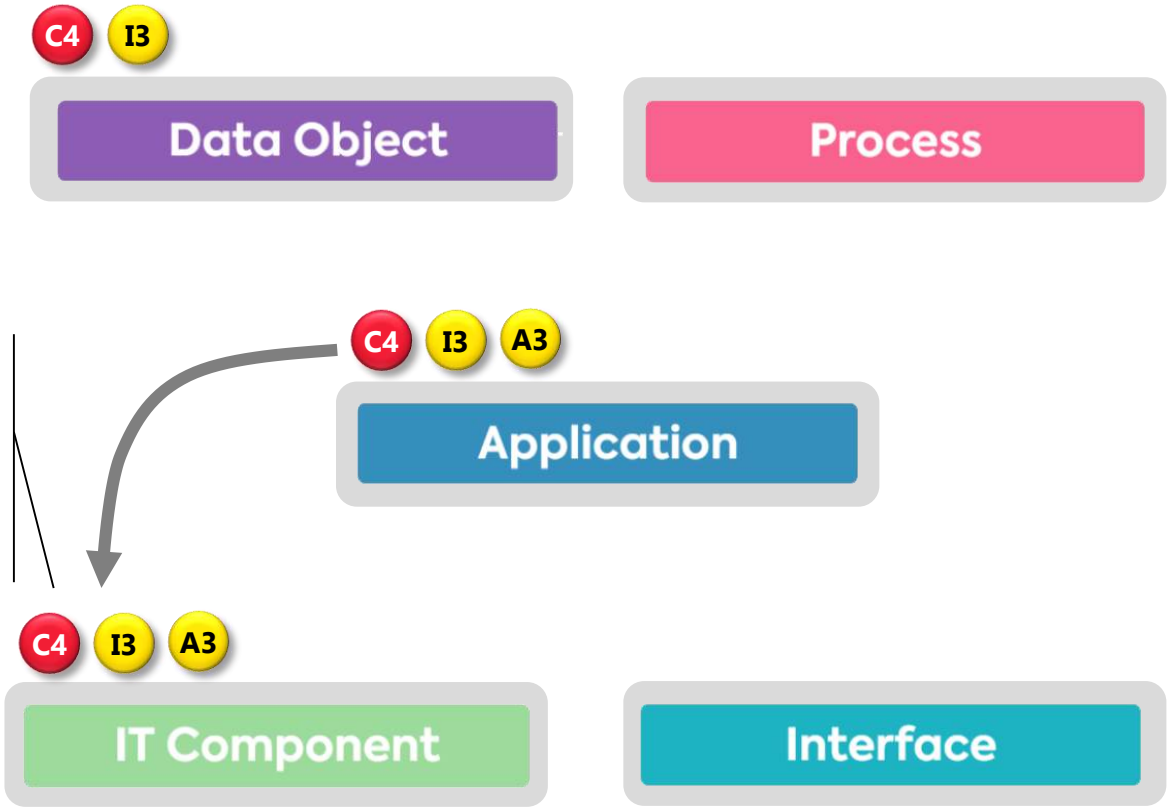
Inheritance of Information Classification



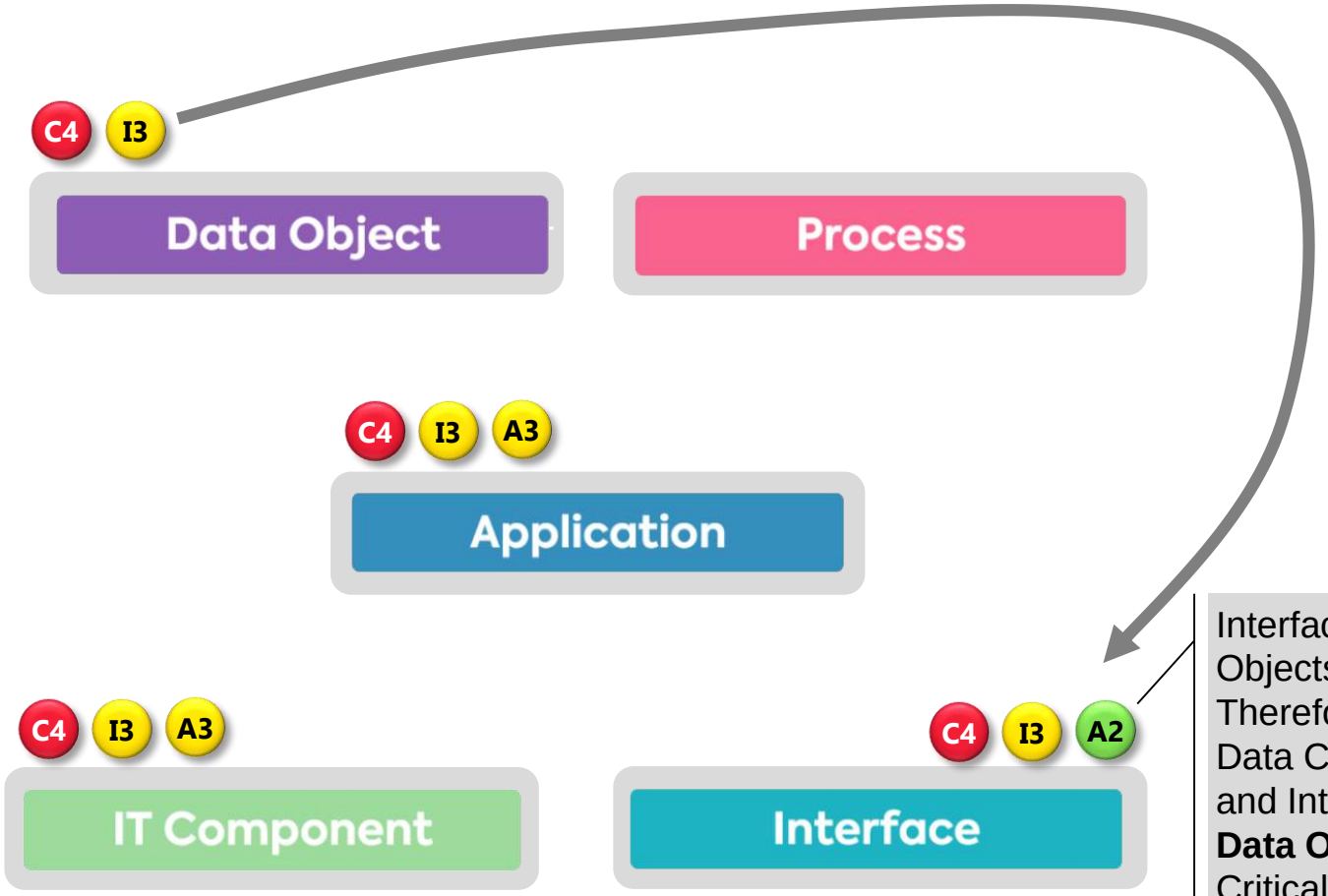
Data Objects are processed by Applications. Therefore the Application inherits the Information Classification **of the processed Data Objects** by maximum principle.

Inheritance of Information Classification

IT Components support Applications. Therefore the Component inherits the Information Classification **of the supported Applications** by maximum principle.



Inheritance of Information Classification



Interfaces process some of the Data Objects of the Application.
Therefore the Interface inherits the Data Classification (Confidentiality and Integrity) **of the processed Data Objects** the Business Criticality of the Interface has to be evaluated based on the availability requirements of the Interface.

Policies govern the implementation based on the ISMS classification

C4 I3 A3

IT Component

Policies and Checklists for:

- Databases
- Storage
- Network
- Penetration Testing
- Patch Management
- System Hardening
- Service Provider Security Contracts
- Service Provider Audits
- …

C4 I3 A4

Application

Policies and Checklists for:

- Software Architecture based on Application Type (e.g. Web Application)
- Software Development
- Testing
- Penetration Testing
- Access/Roles Concept
- …

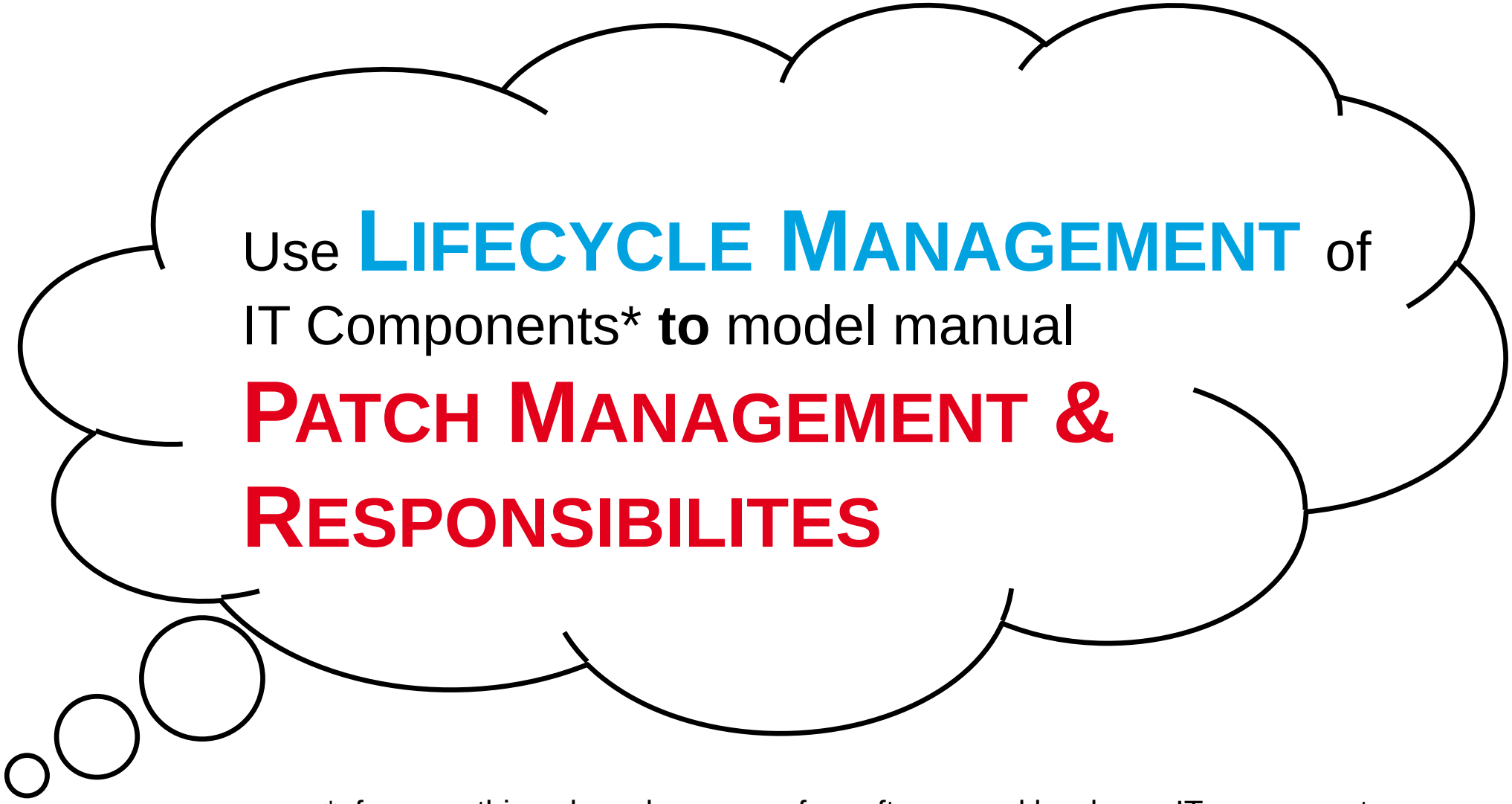
C4 I3 A4

Interface

Policies for:

- Interface Technologies
- Protocols
- Encryption
- Key Management
- …

Further Aspects of ISMS in EAM



*of course this only makes sense for software and hardware IT components

Further Aspects of ISM

Tag **PROVIDER** fact sheets **to** model

TOMs* AND COMPLIANCE CERTIFICATIONS

*TOMs are **T**echnical and **O**rganisational **M**easures. Ask your Data Protection Officer. He knows TOMs.

Further

Use **RESSOURCES**

in Fact Sheets **to** link

SECURITY CONCEPTS

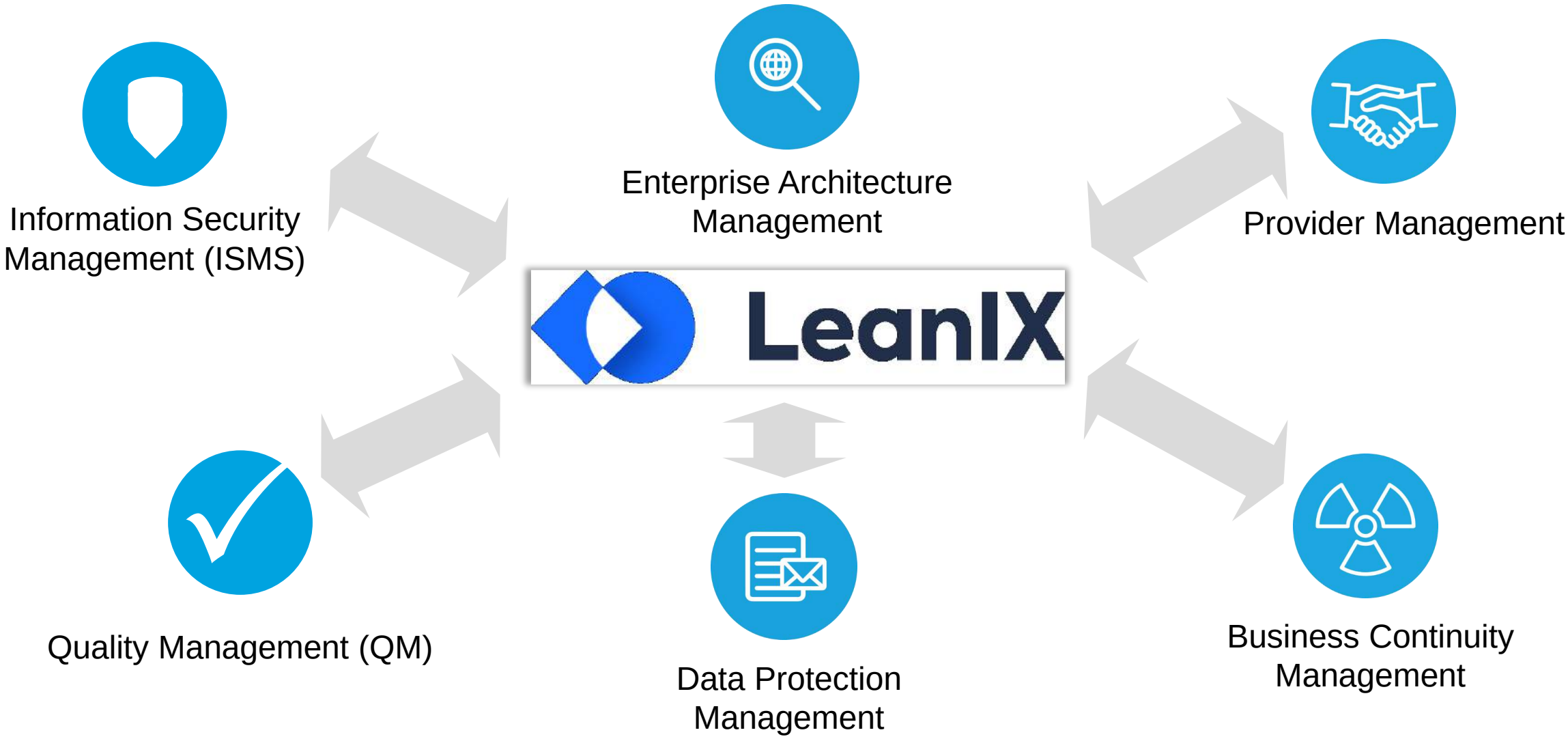
Use **SELF SERVICE PORTAL***

to provide

APPLICATION BLACK- & WHITELISTS

*brand new in LeanIX

Different corporate functions need the same related information



DKMS

WE DELETE BLOOD CANCER

Dennis Endert

DKMS
gemeinnützige GmbH
Kressbach 1
72072 Tübingen
T 0 70 71 9 43 - 1811

endert@dkms.de

Dr. Kai Höfler

DKMS
gemeinnützige GmbH
Kressbach 1
72072 Tübingen
T 0 70 71 9 43 - 1850

hoefler@dkms.de

dkms.de

DKMS

WE DELETE BLOOD CANCER

DKMS

gemeinnützige GmbH
Kressbach 1
72072 Tübingen

T +49 (0) 70 71 9 43-0
F +49 (0) 70 71 9 43-14 99

post@dkms.de

dkms.de