

# Da li znamo kako se čuvaju i štite podaci u bazama podataka?

Mladen Kuzminski, KONTO d.o.o. Požega, Varaždin



## Mladen Kuzminski, mag.inf.

---

- 20 godina iskustva u projektiranju informacijskih sustava
- Voditelj predstavništva Embarcadero / IDERA za Adriatik - Balkan
- IRCA Lead auditor za ISO 27001
- Autor 10 stručnih knjiga i udžbenika
- <https://www.linkedin.com/in/mladen/>

## KONTO d.o.o. Požega, Varaždin

---

- Osnovano 1993. Razvoj poslovnih aplikacija.
- ISO 9001, ISO 27001, aAa bonitet
- Distributer Embarcadero / IDERA za Adriatik - Balkan
- [www.konto.hr](http://www.konto.hr)



# Gdje se nalaze osobni podaci u našoj organizaciji

i koji su to podaci?

## Kako ih štitimo

i kako to dokazujemo?

# Baze podataka

- Sadrže većinu današnjih podataka
- Koje su potencijalne slabosti naše baze?
- Tko može pristupiti podacima?
- Da li legalni korisnici koriste slabe i nesigurne lozinke?
- Kako vidjeti koja su pravila ponašanja na serveru?
- Kako uraditi sigurnosni audit baze podataka i dobiti gotov izvještaj koji ima smisla?
- Da li sve to trebamo sami ručno uraditi ili postoje alati koji nam mogu pomoći?



# SQL Secure

Audit MS SQL baze podataka

# Koje su potencijalne slabosti naše baze?

## Security Report Card :

- Usporedba sigurnosnih postavki svih SQL Servera u organizaciji
- Provjera definirane razine sigurnosti 2 za zaštitu od upada.
- Identifikacija najčešćih sigurnosnih ranjivosti.
- Pravila za procjenu rizika omogućuju provjere pristupa bazama podataka, konfiguracijske provjere i provjere dozvola.
- Svaka sigurnosna provjera kategorizirana je: visoki rizik, srednji rizik ili nizak rizik.

The screenshot displays the 'Server Security Report Card' for a SQL Server instance named 'DESKTOP-4HBCUGR'. The interface is divided into several sections:

- Summary:** Shows the overall security status with a 'High Risk' indicator (red bar) and a score of 2 out of 8. It also displays 'Medium Risk' (6 out of 14) and 'Low Risk' (22 out of 47) counts.
- Server Status:** Provides details about the server, including the name 'DESKTOP-4HBCUGR', the version 'SQL Server 2014 v12.00.4436', and the edition 'Enterprise'.
- Server Security Report Card:** Lists various security checks. A prominent finding is 'Public Role Has Permissions on User Database Objects', which is categorized as 'High Risk'. Other findings include 'Public Server Role Has Permissions' (High Risk), 'Weak Passwords' (High Risk), and 'Audit Data is Stale' (Medium Risk).
- Findings Table:** A detailed table of findings with columns for Risk Level and Findings. The 'Public Role Has Permissions on User Database Objects' finding is highlighted in orange.

# Tko može pristupiti podacima?

## SQL Server User Permissions :

- Otkrivanje svih prava pristupa na SQL Server i Azure SQL bazama podataka.
- Pregled i analiza svih SQL Server objekata od razine servera do razine uloga.
- Pregled svih sigurnosnih svojstava i dopuštenja za sve objekte.
- Povijesni pregled audita i usporedba stanja (traženje promjena)

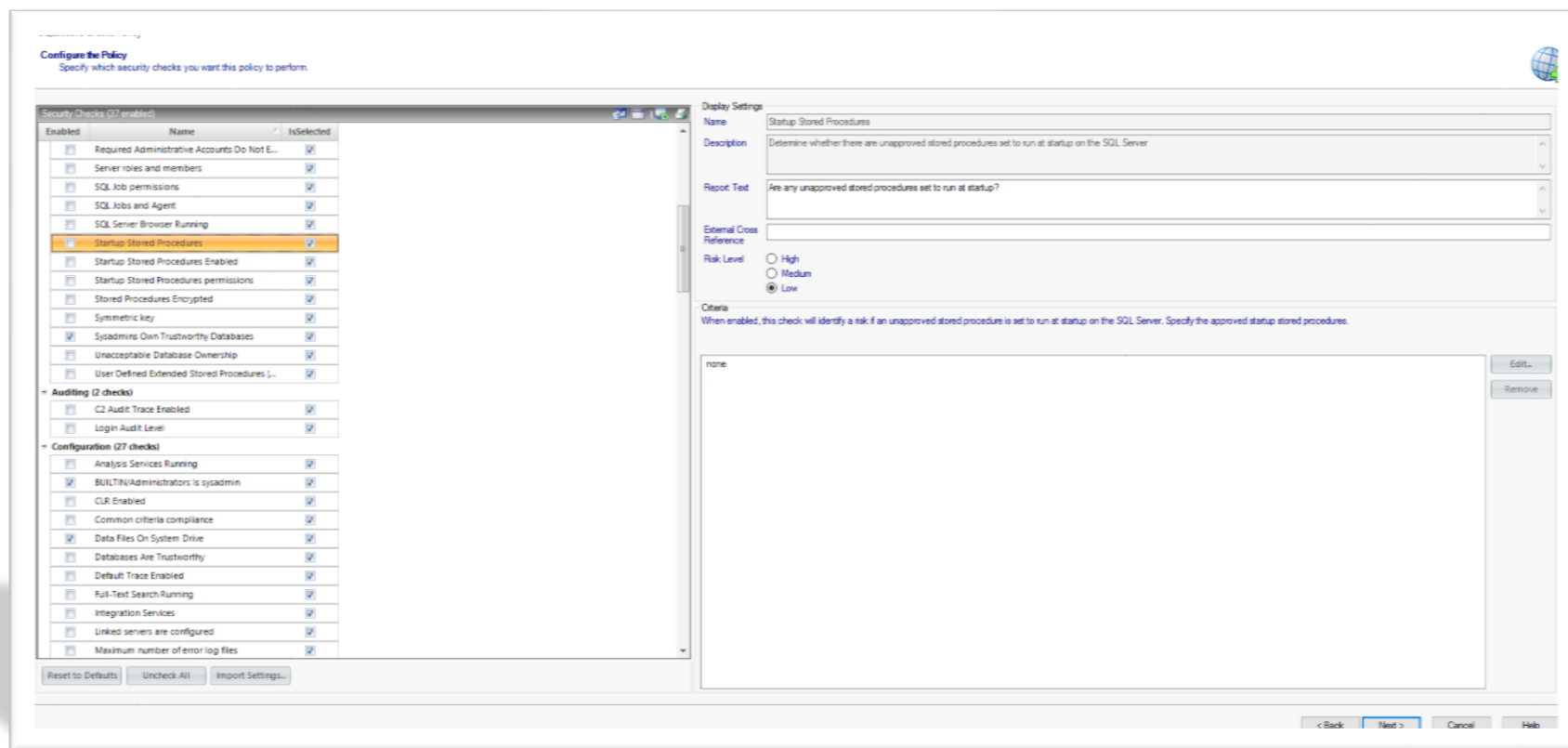
The screenshot displays the SQL Server Enterprise Manager interface. The left pane shows the 'Explore Permissions' tree view, highlighting the 'Financial\_Records' database. The main pane shows the 'Table Properties - Financial\_Records.dbo.employee' dialog box, which is open to the 'Permissions' tab. The 'Permissions' section is set to 'Include fixed role and inherited'. Below this, a table lists all permissions for the table:

Grantee	Permission	Grant	With Grant	Deny	Grantor	Source Permission	Source Object	Source Type
ASLark	SELECT	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	db_datareader	SELECT		
ASLark	DELETE	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	db_datawriter	DELETE		
ASLark	INSERT	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	db_datawriter	INSERT		
ASLark	UPDATE	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	db_datawriter	UPDATE		
BruceC	SELECT	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	db_datareader	SELECT		
BruceC	DELETE	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	db_datawriter	DELETE		
BruceC	INSERT	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	db_datawriter	INSERT		
BruceC	UPDATE	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	db_datawriter	UPDATE		
BulletM	SELECT	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	db_datareader	SELECT		
BulletM	DELETE	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	db_datawriter	DELETE		
BulletM	INSERT	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	db_datawriter	INSERT		
BulletM	UPDATE	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	db_datawriter	UPDATE		
DanC	SELECT	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	db_datareader	SELECT		
DanC	DELETE	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	db_datawriter	DELETE		

# Kako vidjeti koja su pravila ponašanja na serveru?

## SQL Server Policies :

- 80+ provjera ponašanja kroz 7 kategorija
- Import predložaka pravila ponašanja na temelju preporuka autoriteta kao što su DISA SRR, CIS i SNAC, kao i IDERA definirane kategorije zaštite: Osnovna, Balansirana i Jaka.

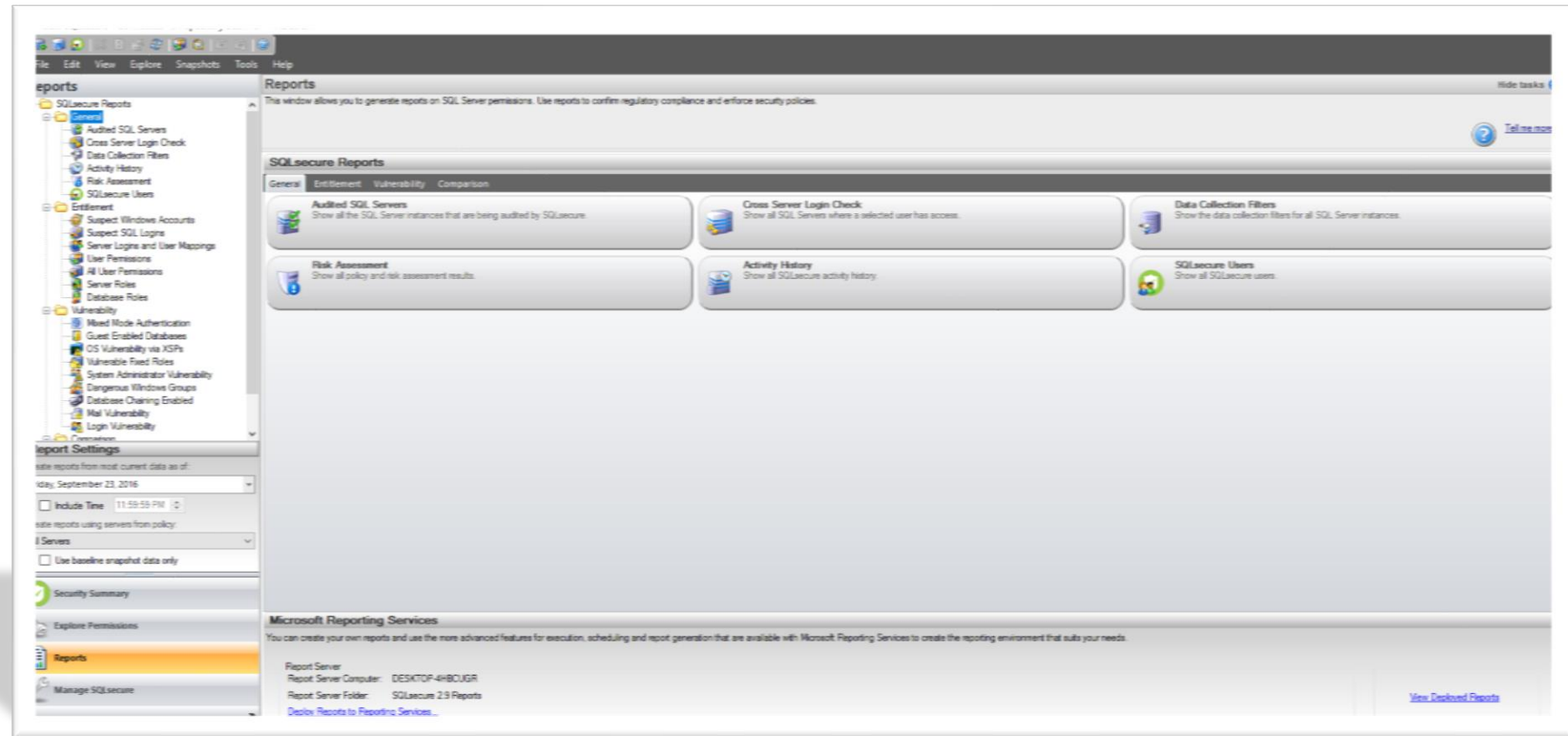




# Kako uraditi sigurnosni audit baze podataka i dobiti gotov izvještaj koji ima smisla?

## SQL Secure Reporting:

- Brzi i pregledni izvještaji. Prijave na više servera, svi serveri na koje je pristupio određeni korisnik, slabosti servera, prava pristupa, uloge na bazama podataka i dr.
- Vremenska usporedba izvještaja i usporedba s predefiniranim modelom.



## **Data Protection by Design and Default**

**GDPR Article 25**

## **Security of Processing**

**GDPR Article 32**

## **Data Protection Impact Assessment**

**GDPR Article 35**



# Što ako dođe do neovlaštenog pristupa i/ili gubitka podataka?

- Tko je radio s podacima i kojim točno podacima?
- Da li postoji dnevnik aktivnosti za forenzičku analizu incidenta?
- Da li postoji mogućnost 24/7 praćenja svih aktivnosti nad bazama podataka?

# SQL Compliance Manager

Praćenje aktivnosti nad MS SQL bazom podataka sa sigurnosnog aspekta

# Tko je radio s podacima i kojim točno podacima?

## Audit SQL Server-a :

- Centralizirani audit svih SQL Server-a i baza podataka
- Praćenje svih aktivnosti korisnika i upozoravanje na promjene podataka u stvarnom vremenu
- Definiranje alarma za pristup osjetljivim podacima
- Praćenje trendova aktivnosti korisnika

The screenshot displays the Idera SQL compliance manager (SQL2012) interface. The main window is titled "SQL2012" and features a menu bar with options like File, Edit, View, Auditing, Alerting, Agent, Tools, and Help. A navigation pane on the left shows a tree view of "Audited SQL Servers" including EARTH, MARS, PROD-CLUST-1, SQL2012, Financial\_Records, Healthcare, and msdb. The main content area is divided into several sections:

- Server Status:** Shows a green checkmark and "OK" status. It includes fields for Last Heartbeat (9/10/2014 4:40 PM), Last Archived (9/10/2014 1:30 AM), Processed Events (818,929), and Recent Alerts (2).
- Server Activity Report Card:** Features a line graph showing "Overall Activity" over time. The graph indicates that "Overall Activity currently has no threshold enabled." The y-axis ranges from 0 to 80,000, and the x-axis shows dates from 8/14 to 9/08.
- Audit Configuration:** Lists "Server - Failed Logins, Security, DDL, Admin", "Privileged Users (1) - Logins, Failed Logins, Security, DDL, Admin, UDE, DML, Select, Capture SQL, Capture Transactions", and "Databases - 2 of 46". It also shows "Event Filters (1) - Application Name, Database, Hostname, Login Name".
- Recent Audit Events:** A table listing events with columns for Category, Event, Time, and Details. The events include multiple "DDL Invalid" entries and "Admin Server alter trace" entries.

At the bottom of the interface, there are navigation buttons for "Explore Activity", "Audit Reports", and "Administration".

# Dnevnik aktivnosti za forenzičku analizu incidenta

## Bilježenje aktivnosti:

- Bilježenje svih aktivnosti korisnika
- Analiza promjena podataka
- Pregled DML-a koji je promijenio podatke, pregled vrijednosti prije i poslije promjene
- Posebna pažnja posvećena pristupu osjetljivim podacima

The screenshot displays the Idera SQL compliance manager interface for SQL2012. The left pane shows the 'Explore Activity' tree with 'SQL2012' expanded to show 'Healthcare'. The main pane shows 'SQL2012::Healthcare' with 'Audit Events' selected. The 'Login' event is expanded, showing a table of events for user 'DEMOSOX\robert'. The table includes columns for Category, Event, Date, Time, Database, and Target Object. Below the main table, detailed views for 'Update' events are shown, including columns for Action, Date, Time, Columns Updated, Audited Updates, Table, and Primary Key. The 'Before Value' and 'After Value' columns show the change in 'MedicalID' from 9 to 2, 2 to 1, and 1 to 2.

Category	Event	Date	Time	Database	Target Object	Details
DML	Insert	9/8/2014	4:29:14:250 P	Healthcare	CustomerDemogr	
DML	Update	8/15/2014	9:20:31:490 A	Healthcare	Prescriptions	
Update		8/15/2014	9:20:32 AM	1	1	Prescriptions <OrderID = 10263
Column			Before Value	After Value		
MedicalID			9	2		
DML	Update	8/13/2014	4:30:01:767 P	Healthcare	Prescriptions	
Update		8/13/2014	4:30:03 PM	1	1	Prescriptions <OrderID = 10256
Column			Before Value	After Value		
MedicalID			1	2		
DML	Update	7/25/2014	9:51:30:257 A	Healthcare	Prescriptions	
Update		7/25/2014	9:51:31 AM	1	1	Prescriptions <OrderID = 10261
Column			Before Value	After Value		
Freight			3.0500	0.0500		

# Regulatorni izvještaji

## Predloži standardnih izvještaja:

- Automatsko stvaranje izvještaja koji udovoljavaju zahtjevima HIPAA, HITECH and PCI DSS I dr. regulative
- 25 gotovih predložaka audita uz stalno proširenje

The screenshot displays the Idera SQL compliance manager (SQL2012) interface. A dialog box titled "SQLcm Configuration Wizard - Apply Regulation" is open, showing the "Regulation Guidelines" section. The dialog box indicates that the selected HIPAA regulatory guidelines are being applied, and the SQLCompliance Agent will automatically collect the following server and database events:

- Failed Logins
- Administrative Activities
- Security Changes
- Database Definition
- Database Modification
- Privileged Users
- Privileged User Events
- Sensitive Column Auditing

To successfully comply with the selected regulation guideline, you will need to configure the following audit settings:

- Privileged Users
- Privileged User Events
- Sensitive Column Auditing

The background interface shows the "Explore Activity" pane with a tree view of audited SQL servers (EARTH, MARS, PROD-CLUST-1, SQL2012, Financial\_Records, Healthcare, msdb). The main pane displays a table of audit events with columns for Time and Details.

Time	Details
8/31:14 PM	DEMOBOX\ideraSQLdm
8/31:14 PM	DEMOBOX\ideraSQLdm
8/31:14 PM	DEMOBOX\ideraSQLdm
8/31:14 PM	DEMOBOX\ideraSQLdm
8/31:14 PM	DEMOBOX\ideraSQLdm
8/31:14 PM	DEMOBOX\ideraSQLdm
9/10/2014 4:31:14 PM	Admin Server alter trace
9/10/2014 4:31:14 PM	Admin Server alter trace
9/10/2014 4:31:14 PM	Admin Server alter trace
9/10/2014 4:31:10 PM	DDL Invalid
9/10/2014 4:31:10 PM	DDL Invalid
9/10/2014 4:31:04 PM	DDL Invalid
9/10/2014 4:31:04 PM	DDL Invalid
9/10/2014 4:31:00 PM	Admin Server alter trace
9/10/2014 4:31:00 PM	Admin Server alter trace
9/10/2014 4:31:00 PM	Admin Server alter trace

## **Notification of Personal Data Breach to the Supervisory Authority** GDPR Article 33

## **Records of Processing Activities** GDPR Article 30

## **Data Protection Impact Assessment** GDPR Article 35



## Are you ready for GDPR? See How IDERA Can Help with your MS SQL and Data Management Directives.

By Sultan Shiffa, Bob Fullam, Stephen Stout

### Overview of GDPR

Today, we live in a digitalized economy where globalization is driving businesses across borders and data management needs more attention than ever.

The European Union's General Data Protection Regulation (GDPR) becomes effective on May 25, 2018. In contrast to older directives and data protection acts, the GDPR will bring new accountability obligations, increased data protection rights for the EU citizens and restrictions on data flows across borders. Organizations that process EU citizens' personal data must comply with the regulations, and this applies to all data owners, who say why and how data is processed, and to data processors, who perform actions on the data.

Also, it introduces obligations to data breach notification, with stricter accountabilities that personal data information is sufficiently managed and protected.

## Are you ready for GDPR? See How IDERA Can Help with your MS SQL and Data Management Directives.

- Stručni dokument koji objašnjava kako razumjeti i dokumentirati kretanje i upravljanje podacima u organizaciji.
- Daje preporuke za provjeru usklađenosti s GDPR regulativom.
- Dostupan na zahtjev slanjem maila na [mladen@konto.hr](mailto:mladen@konto.hr)



# SQL Secure

Dostupan na [www.idera.com](http://www.idera.com) Prvih 14 dana besplatna upotreba.

# SQL Compliance Manager

Dostupan na [www.idera.com](http://www.idera.com) Prvih 14 dana besplatna upotreba.



# IDERA proizvodi

Bogat portfelj alata za nadgledanje, praćenje, optimizaciju i sigurnost MS SQL, Oracle i ostalih vodećih servera. Alati za modeliranje i praćenje sustava.

## Performanse i nadgledanje

SQL Diagnostic Manager  
SQL BI Manager  
SQL Defrag Manager  
SQL Inventory Manager  
SQL Doctor  
DB Optimizer

*Osiguravaju  
raspoloživost i  
performanse servera i  
aplikacija*

## Sigurnost i usklađenost

SQL Compliance Manager  
SQL Secure

*Aktivnosti audita i  
usklađenja s  
regulativama*

## Backup i administracija

SQL Safe Backup  
SQL Enterprise Job  
Manager  
SQL Virtual Database  
SQL Admin Toolset  
SQL Toolbox  
SQL Comparison Toolset  
DB Artisan

*Čuvanje kritičnih  
podataka i  
automatizacija procesa*

## Modeliranje podataka

ER/Studio Data Architect  
ER/Studio Business  
Architect  
ER/Studio Enterprise  
Team Edition

*Aktivnosti audita i  
usklađenja s  
regulativama*



[www.idera.com](http://www.idera.com)  
[idera@konto.hr](mailto:idera@konto.hr)  
+385.42.300.910