

# How security tools can accelerate GRC projects

Lessons learned in SAP projects

Bridging business and IT

## Agenda

- CSI tools: the company
- The goal: Full integrated GRC system
- Implementation approach
- In which faze are security tools used
- Lessons learned

Bridging business and IT





## CSI tools

- Founded in 1997
- Rebranding 2008
- Focus
  - Software development
  - No services
  - Only SAP
    - “ABAP Stack”
  - PC based & C/S
  - Offline & Online

### Development of tools

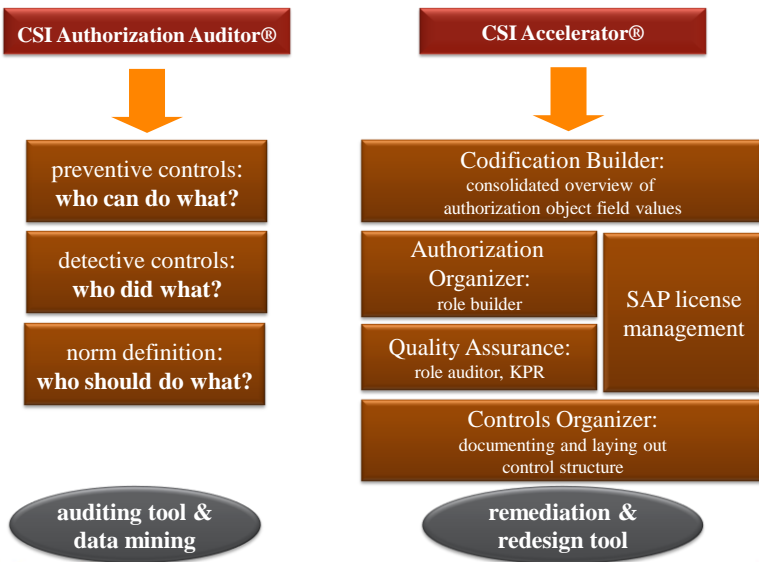
- 1) auditing
- 2) design
- 3) building
- 4) implementing of :
  - SAP authorizations
  - SAP roles
  - SAP users
  - SAP GRC
  - Business Process Controls
  - Risks
  - Controls

Bridging business and IT

© CSI tools. All rights reserved.



## Proven International Recognition

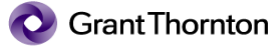


Bridging business and IT

© CSI tools. All rights reserved.



over 250 customers demonstrate the need



Bridging business and IT



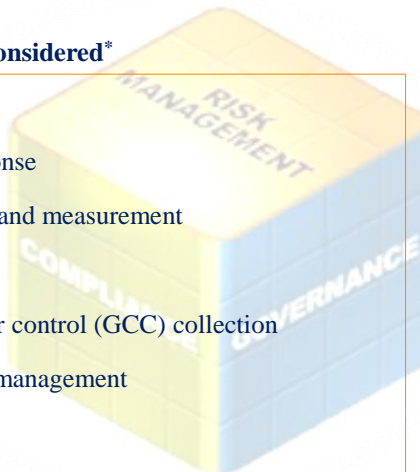
© CSI tools. All rights reserved.



## Governance, Risk & Compliance

### GRC areas/capabilities to be considered\*

- Controls and policy library
- Policy distribution and response
- IT Controls self-assessment and measurement
- IT Asset repository
- Automated general computer control (GCC) collection
- Remediation and exception management
- Reporting
- Advanced IT risk evaluation and compliance dashboards



\* Source: Gartner

Bridging business and IT

© CSI tools. All rights reserved.



## Why GRC projects?

- Efficiency benefits → improve business processes
  - faster report aggregation
  - decreased audit costs
  - faster time to remediate control deficiencies
- Risk reduction benefits
  - fewer incidents
  - fewer regulatory fines
  - lower insurance premiums
- Strategic performance benefits
  - better strategic decisions using risk and compliance information

Source: Chris McClean, a senior analyst at Forrester Research

Bridging business and IT

© CSI tools. All rights reserved.



## How to start a GRC project

- How to eat a big elephant?
  - ...
- Top Down approach
  - Risk Management
  - Project management
  - Vulnerability analysis
  - ...



Bridging business and IT

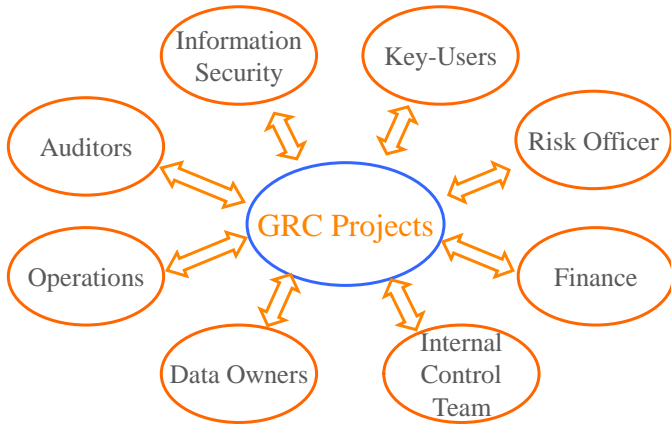
\* Source: Dan Rockwell

© CSI tools. All rights reserved.





## Top Down: Information is critical

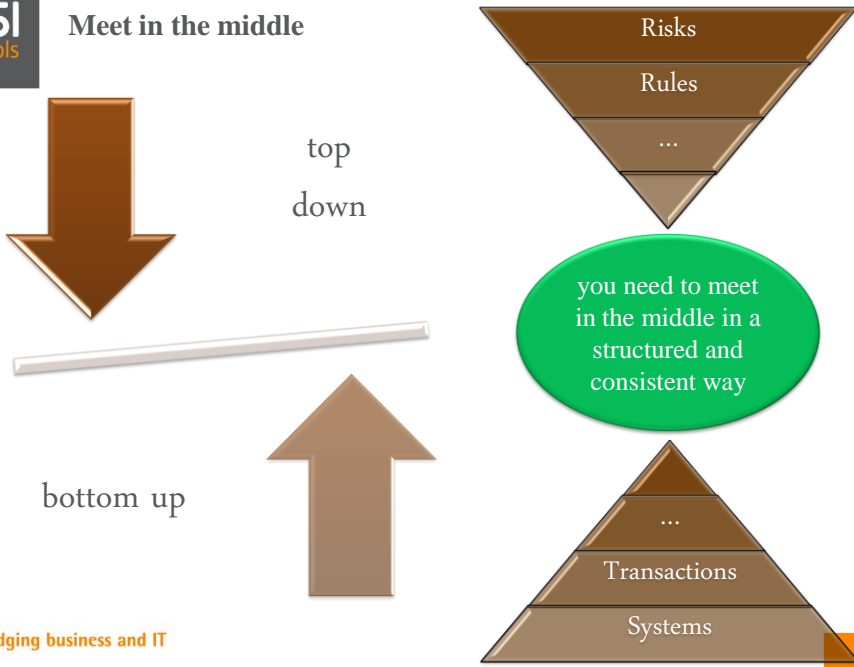


Bridging business and IT

© CSI tools. All rights reserved.



## Meet in the middle

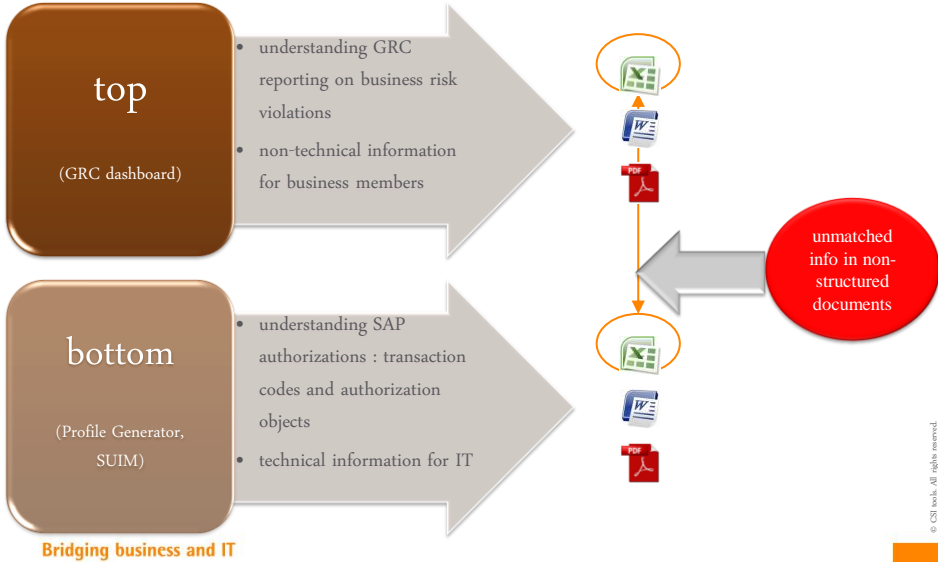


Bridging business and IT

© CSI tools. All rights reserved.



## Inefficient use of text editors; spreadsheets; ...



© CSI tools. All rights reserved.



## Non-structured documents



- difficult to define an project approach
- not clear what to do due to lack of insight
- nightmare for project resource allocation
- does not give any confidence to business members
- are out-dated very fast
- QA is almost impossible
- leads to non-action

**Bridging business and IT**



© CSI tools. All rights reserved.



# Vulnerability analysis is complex: a worthy challenge

- thousands of users world-wide
- business-critical system & process operation
- different processes and configuration in different sites
- multi-dimensional roles and responsibilities
- multi-layer, multi-component security
- interconnectivity, customizing and custom developments
- integrated systems, non-integrated organizations
- SAP is a standard well known application
  - “bad guys” can have more knowledge than the “good guys”

Bridging business and IT

© CSI tools. All rights reserved.



## Step 1: Data mining for vulnerability analysis

#### 4. user-ids overview

user status	active system	password	service	effective
(A)	(B)	(C)	(D)	(E)
locked	475	0	0	0
locking in the future	1	0	0	0
password to be reset	293	0	0	0
password	7	0	0	0
total users	776	0	0	0

total users analysed: 664 / 449

#### 5. authorization concept role assignment

#### 5. authorization concept authorization status - organizational levels

authorization status	nr. of fields	% fields
unchanged	4850	49%
changed	2481	25%
standard	4494	45%
recovered	229	3%
<b>total</b>	<b>9854</b>	<b>100%</b>

#### 6. access rights to critical functionality graphical overview

#### 7. segregation of duties distribution of SoD conflicts: user-single

#### 7. segregation of duties distribution of SoD conflicts: user - single - composite

#### 7. segregation of duties distribution of SoD conflicts: user-composite

Bridging business and IT

© CSI tools. All rights reserved.

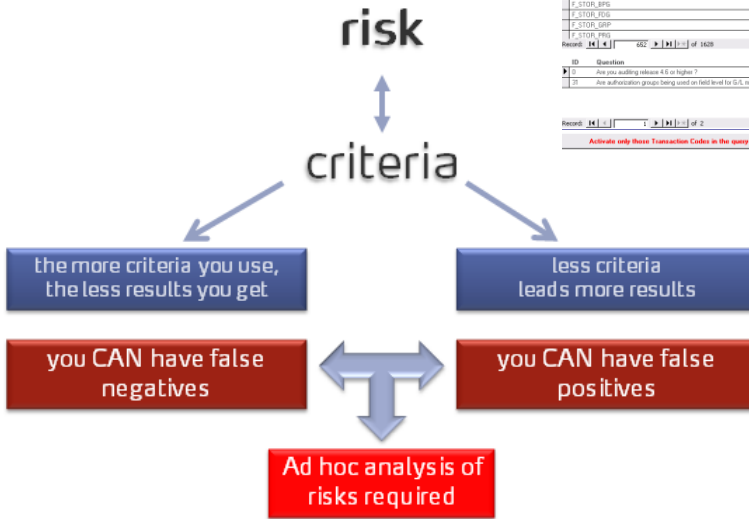


## Step 2: Rule set accuracy

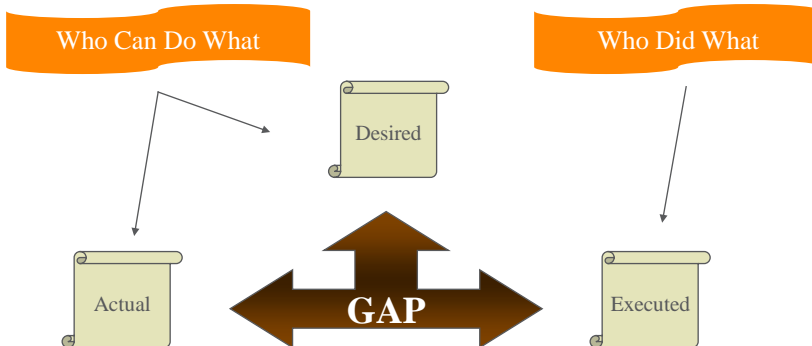
Object	Description	Result
F_RTP_BPA		NO
F_RTP_BPA		NO
F_RTP_BPA		NO
F_RTP_GSP		NO
F_SKAL_ABT	GL Account Change Authorization for Certain Fields	NO
F_SKAL_ABT	GL Account Change Authorization for Certain Fields	NO
F_STOR_ACS	GL Account Account Authorization	NO
F_STOR_ACS	GL Account Account Authorization	NO
F_STOR_ACS	GL Account Account Authorization	NO
F_STOR_ABT		NO
F_STOR_ABT		NO
F_STOR_BKA		NO
F_STOR_BKA		NO
F_STOR_BKA		NO
F_STOR_BPA		NO
F_STOR_BPA		NO
F_STOR_BPA		NO
F_STOR_GSP		NO
F_STOR_GSP		NO
F_STOR_PYS		NO

ID	Question	Answer
0	Are you auditing release 4.0 or higher?	YES
21	Are authorization groups being used on field level for GL master records?	NO



## Step 3: Closing the gap

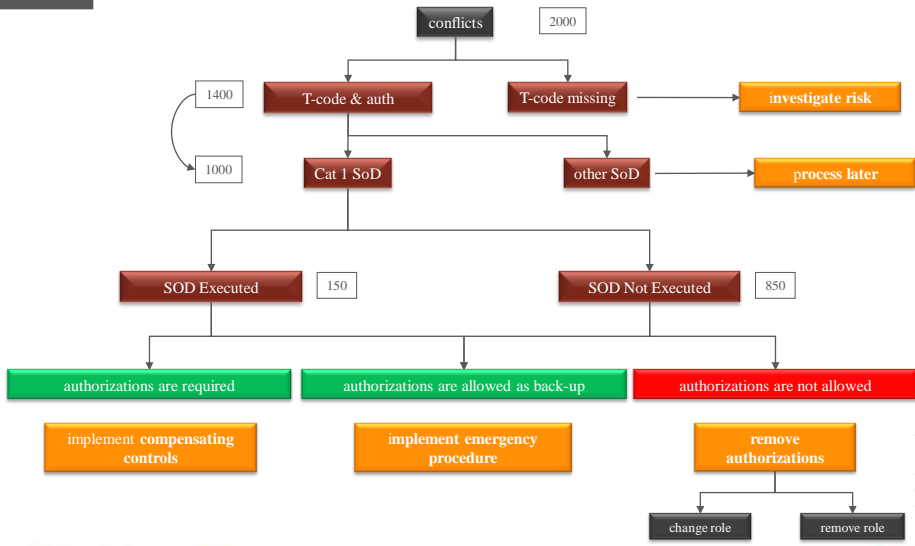


Bridging business and IT

© CSI tools. All rights reserved.



## Step 4: Remediation decision tree



Bridging business and IT

© CSI tools. All rights reserved.



## Step 5: Remove or change the role

The screenshot shows a window titled 'The Ultimate Remediation for B\_SAP\_ALL - Generated partial profile for SAP\_ALL'. It includes a 'Hide Legend' button and a 'Queries' section with a table for user 'SUPER\_20001'. Below is a 'Legenda' table with 9 rows of query information.

Nbr	Query ID	Variant	Query description
1	AAAMPFA	<NA>	Maintain Asset Manual Postings
2	AAAMPFA	<NA>	Maintain Asset Sales, Donation, Scraping
3	AAAMPFA	<NA>	Maintain Depreciation Run
4	AAAMPFA	<NA>	Maintain Asset Revaluation Activities
5	CBOMKA	<NA>	Maintain Bill of Materials
6	CRUTA	<NA>	Maintain Routings
7	CRORFA	<NA>	Maintain Production Orders
8	DWES_A	<NA>	Maintain Work Breakdown Structures
9	DESDFA	<NA>	Maintain Project Budget

Row contains all 'N':  
= user should not have any of the functionality granted by role/profile  
→ Remove role from user

Column contains all 'N':  
= all users should not have the functionality granted by role/profile  
→ Remove authorizations from role

Note: especially useful when Norm info is used

Column contains a BLANK:  
Indicates that role gives only partial access to functionality (Accumulation of Access Rights)  
→ Focus on other roles/profiles

Bridging business and IT

© CSI tools. All rights reserved.



## Step 6: Analysis Role inconsistencies

### Analysis authorization

Analysis cockpit | Derived roles, objects with differences

Drag a column header here to group by that column.

Derived role	Derived description	Master role	Master description	Object
S99FCAMPAPIVA	F-AP: Maintain A/P Invoice Verificati...	S99F000APIVA	F-AP: Maintain A/P Invoice Verificati...	F_BKPF_BUK
S99FCAMPAPIVA	F-AP: Maintain A/P Invoice Verificati...	S99F000APIVA	F-AP: Maintain A/P Invoice Verificati...	K_TP_VALU
S99FCAMPAPIVA	F-AP: Maintain A/P Invoice Verificati...	S99F000APIVA	F-AP: Maintain A/P Invoice Verificati...	M_BEST_EKO
S99FCAMPAPIVA	F-AP: Maintain A/P Invoice Verificati...	S99F000APIVA	F-AP: Maintain A/P Invoice Verificati...	M_BEST_WRK
S99FCAMPAPIVA	F-AP: Maintain A/P Invoice Verificati...	S99F000APIVA	F-AP: Maintain A/P Invoice Verificati...	M_RAHM_EKO
S99FCAMPAPIVA	F-AP: Maintain A/P Invoice Verificati...	S99F000APIVA	F-AP: Maintain A/P Invoice Verificati...	M_RECH_BUK
S99FCAMPAPIVA	F-AP: Maintain A/P Invoice Verificati...	S99F000APIVA	F-AP: Maintain A/P Invoice Verificati...	M_RECH_WRK
S99FCAMPAPIVA	F-AP: Maintain A/P Invoice Verificati...	S99F000APIVA	F-AP: Maintain A/P Invoice Verificati...	S_WFAR_OBJ

Added / changed authorizations in deriveds

- Roles with differences: 1
- Role objects added: 0
- Role objects different: 8
- Role object fields different: 8
- Role object field values different: 9

Double-click on the role

Bridging business and IT

© CSI tools. All rights reserved.



## Step 7: Reverse Engineering build all roles automatically based on documentation

Store role authorization values back in codification sheets.  
Use template roles and update other roles for the same domain according to the template.

CSI Accelerator - [Development Concept]

File Edit Codification Organize Simulation QA Control View Custom Views Library Info center Tools Window Help

Workbook: Domain workbook

Drag a column header here to group by that column.

Module	Field	Description	Objects	Comes	Modules	Taskcodes	Actions	Master	Belgium	Netherlands	USA	New York	Texas
								BOOK	BOOK	BOOK	BOOK	BOOK	BOOK
F	HTORL	Chart of Accounts											
F	BUORG	Company Code											
F	BROGRU	Authorization Group	F_LFA1_BSEK										
K	KDIRGS	Controlling Area											
M	WENGS	Plant											
M	ENORG	Purchasing Organization											
V	VDIRGS	Sales Organization											
V	SPART	Division											
V	VTRGS	Contribution Channel											
S	CLASS	User group in user-master mai...	S_USER_GRP										
C	CSWRK	Plant											
B	ISAPTRVCI	ISAPTRVCI											
B	GCOSMP	Company Code											

Large question mark in the authorization restrictions area.

Bridging business and IT

© CSI tools. All rights reserved.



## Final project step: after care

- Once everything is documented and cleaned tools can be used
  - upload all documentation / rules into GRC
  - for ad-hoc monitoring
  - change management
  - rule simulation
  - automated role maintenance
  - optimize license management



Bridging business and IT

© CSI tools. All rights reserved.



## Lesson Learned: What goes wrong?

- No responsibility split in the three major security processes
  - rule set maintenance
  - role set maintenance
  - user – role assignment
- Rules that were not accepted by the organization
- Process view instead of data centric view
- People do not understand who does what and no ownership with regard to data
- Maturity level of the organization not taken into account
- The description does not map the content of the role
- Role = WHAT & WHERE vs SoD = WHAT only

Bridging business and IT

© CSI tools. All rights reserved.



## Good practice: Roles

- Standard roles can be used
- SOD is not the only criteria for a role
- Isolate always critical data
- Do not fine tune roles on non-critical data (exaggerate on WHERE)
- Ownership is key
- Description of the role is extremely important

Bridging business and IT

© CSI tools. All rights reserved.



## Good practice: Rules

- Work risk-based
- Ensure business involvement
- So do not use internet SOD rules
- Establish Ownership again
- Avoid theoretical conflicts – take materiality into account
- Take statistics into account

Bridging business and IT

© CSI tools. All rights reserved.



## Food for thought: Mitigating controls

- Can only be implemented if SoD – Risk is a 1-1 relation
- Non-executed SOD's cannot be solved with controls !
- Are executed SOD's a real risk?

Bridging business and IT

© CSI tools. All rights reserved.



## The presentation ends here but GRC never ends ☺

- “It is cost effective to automate repetitive tasks; it is expensive and complicated to automate everything.”
- Monitoring solution to be checked yearly
  - New transaction codes used
  - Optional objects no longer used
- Ensure that changes in ERP or organizations will trigger change management in GRC
- *“Security is a process not a product” - Bruce Schneier*

Bridging business and IT

© CSI tools. All rights reserved.



Common Sense by Innovation



**Johan Hermans - Partner**  
Tel. +32 16 308 000 - Mob. +32 495 24 63 98  
Fax +32 16 311 001  
[www.csi-tools.com](http://www.csi-tools.com)  
Geldenaaksebaan 329 B-3001 Heverlee  
Bridging Business and IT



IT bridging business and IT  
Geldenaaksebaan 329 B-3001 Heverlee  
[www.csi-tools.com](http://www.csi-tools.com)  
Tel. +32 16 308 000 - Mob. +32 495 24 63 98  
Fax +32 16 311 001

Bridging business and IT