



# Top Control and Security Risks in SAP

And How to Overcome Them

17 December 2008

ISACA WINCHESTER CHAPTER IN FORMATION

# Top Security and Control Risks...

On the First Day of Christmas my consultant gave to me  
A “World Class Methodology”...



# The first day...

## ASAP

- Business interaction
- Change management
- Security & Control

## How to solve it

- Controls workstream
- Programme governance  
(monitor change management and control)

# Top Security and Control Risks...

---

**On the Second Day of Christmas my consultant gave to me**

**Project Management**

# The second day...

## What's not in the project plan?

- Interfaces
- Data clean-up
- Change management
- Benefits realisation
- Controls

## How to solve it

- Don't make assumptions about what the consultants will provide
- Control and security are your responsibility

# Top Security and Control Risks...

---

**On the Third Day of Christmas my consultant gave to me**

**First Class Skills**

# The third day...

## Skills in what?

- UK consultants with business knowledge but no SAP
- Low cost outsource programming with no business knowledge

## How to solve it

- keep on top of the design
- consider security and controls throughout the project and not build on them after the event

# Top Security and Control Risks...

---

**On the Fourth Day of Christmas my consultant gave to me**

**Vanilla SAP**

# The fourth day...

## Vanilla SAP

### RICEFs and FRICEs

Controls become “extras”  
and you have to pay more  
for them

## How to solve it

- consider control in the contract negotiations
- align controls to SAP functionality; don't try and apply your legacy controls

# Top Security and Control Risks...

---

**On the Fifth Day of Christmas my consultant gave to me**

**A Business Case**

# The fifth day...

**To win a contract every consultant will price keenly...**

**...to deliver the contract you and they will come under cost pressure...**

**...Security and Controls are often forgotten**

**As a rule of thumb 5% of the project budget should be on controls and security**

# Top Security and Control Risks...

---

**On the Sixth Day of Christmas my consultant gave to me**

**A Detailed Design**

# The sixth day...

## Detailed design

- Does this take advantage of SAP controls
- How do you transform a business and build a new system at the same time?

**Involve SAP Controls specialists in the design – people who know how controls work in SAP**

# Top Security and Control Risks...

---

**On the Seventh Day of Christmas my consultant gave to me**

**Testing plans**

# The seventh day...

## Testing plans

- End to end scenarios?
- The swivel chair test (dealing with exceptions)
- Testing controls?
- Testing security?

Ensure that controls are an integral part of your design so that they are tested as part of the system.

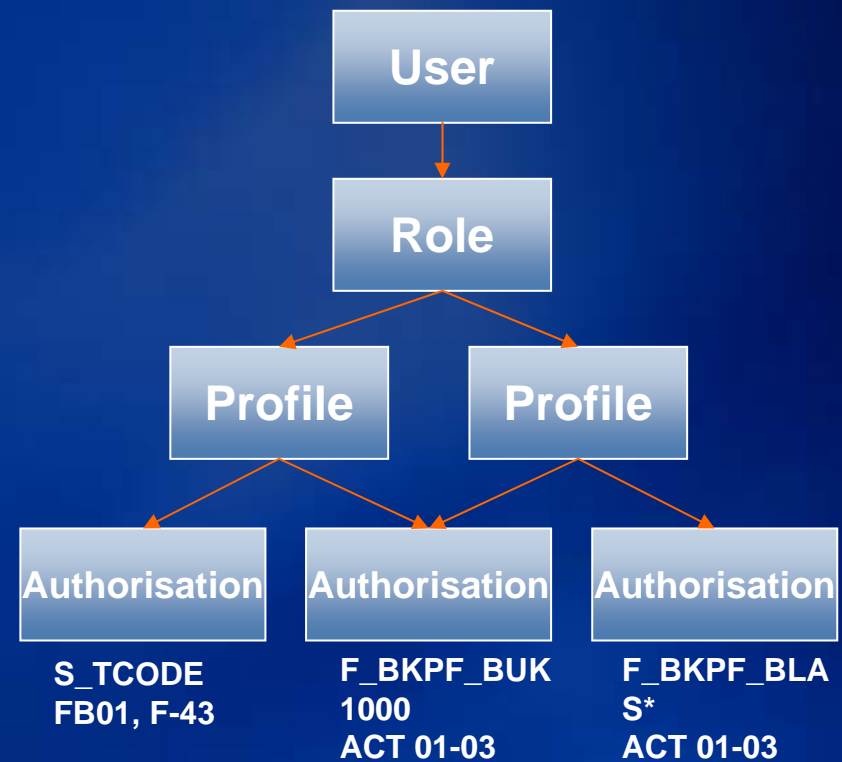
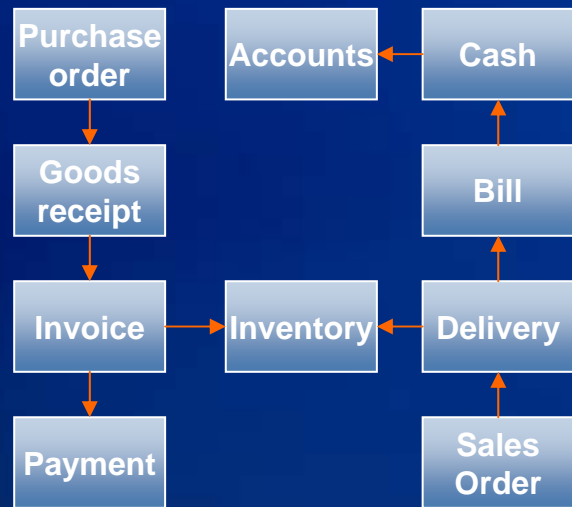
Do work on security – authorisations and profiles early so that they can be tested.

Test exceptions and errors as well as the straight-through processes

# Top Security and Control Risks...

On the Eighth Day of Christmas my consultant gave to me

## Segregated Duties



# The eighth day...

## Segregation of duties

- Roles built late
- Consultant doesn't understand segregation of duties
- Super-users
- Support roles

**Do organisation design in parallel with role design and process design**

**Test segregation of duties early**

**Use preventive software (such as SAP-GRC, Approva, or SecurityWeaver)**

# Top Security and Control Risks...

---

**On the Ninth Day of Christmas my consultant gave to me**

**Management Reporting**

# The ninth day...

## Management reporting

- Management information needs not understood
- Replication of legacy reports (which become expensive RICEFs)
- Quality of consultants?
- 50% of code written for SAP is NEVER USED

Management information starts on day 1 of the project

Focus on data requirements and data sources

BW/BI can meet control requirement and continuous monitoring....(but that's another presentation)

# Top Security and Control Risks...

---

**On the Tenth Day of Christmas my consultant gave to me**

**Managed changes**

# The tenth day...

## **Solution Manager?**

**- a large SAP system can have up to 1000 transports a month – changes to roles, programmes, configuration, and other system settings**

## **Rigid change control**

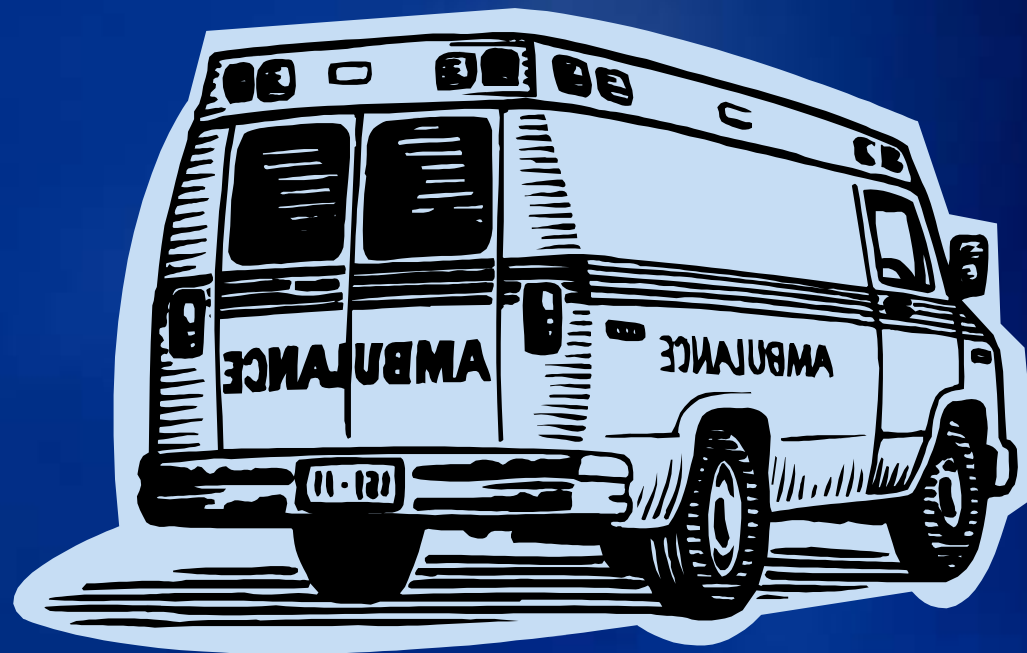
**Automated regression tests**

**Testing covers key control functionality (if you're really smart it tests your application embedded controls)**

# Top Security and Control Risks...

On the Eleventh Day of Christmas my consultant gave to me

Go-live support



# The eleventh day...

## Go-live support

- Its not the car that matters  
but the driver...

Day 1 KPIs – how to spot  
where processes are not  
working / not followed

# Top Security and Control Risks...

---

**On the Twelfth Day of Christmas my consultant gave to me**

**A painless transition**

# The twelfth day...

## Who owns controls and security

- User administration
- Shared services?
- Role of internal audit

## Review your control and governance functions

### Source controls alongside processes

**Audit needs to embrace SAP  
– it is the company's DNA**

# 12 Days of SAP

---

**Painless transition**

**Go-live support**

**Managed Changes**

**Management Reporting**

**Segregated Duties**

**Testing plans**

**Detailed design**

**A business case**

**Vanilla SAP**

**First Class Skills**

**Project Management**

**A World Class Methodology**



## Presenter's contact details

**Colin Bezant**

**KPMG LLP (UK)**

**+44 (0)20 7311 4548**

**[colin.bezant@kpmg.co.uk](mailto:colin.bezant@kpmg.co.uk)**

**[www.kpmg.co.uk](http://www.kpmg.co.uk)**