ISACA 2013 NORDIC CONFERENCE

SOX TODAY AND YESTERDAY

ASSURANCE TRACK

2013-04-23 10:15-11:00

cicc

2013-03-27

AGENDA

What is SOX?

SOX implementation yesterday

Changes

SOX implementation today

SOX legacy, how is it used today

HARALD CARLSSON

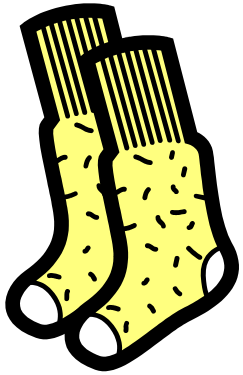
Independent Internal Control Consultant

Formerly IT-auditor and Information Security Consultant at Ernst & Young

SOX experience:

- Documented SOX processes for Volvo and Ericsson (2005)
- Project Leader of SKF SOX IT Management test (2006-2009)
- SAS-70 and ISAE 3402 specialist (2006-2012)
- Advisor to Elfa Group, currently in the process of being SOX-compliant. (2012-2013)

WHAT IS SOX?



SOCKet Secure (**SOCKS**)

WHAT IS SOX?

Sarbanes–Oxley Act of 2002, A United States federal law.

Reduce risk for fraud like Enron and Lehman Brothers

Section 404, Requirements on Assessment of Internal Control

Corporate Management shall attest to

- The design of internal control
- The operating effectiveness of the internal control

Requirements on IT departments to develop internal control

MANAGEMENT IS RESPONSIBLE

YESTERDAY (2005-2007)

Uncertainty

- How much is good enough
- Checklist approach based on COBIT
- Same set of IT-controls fits all

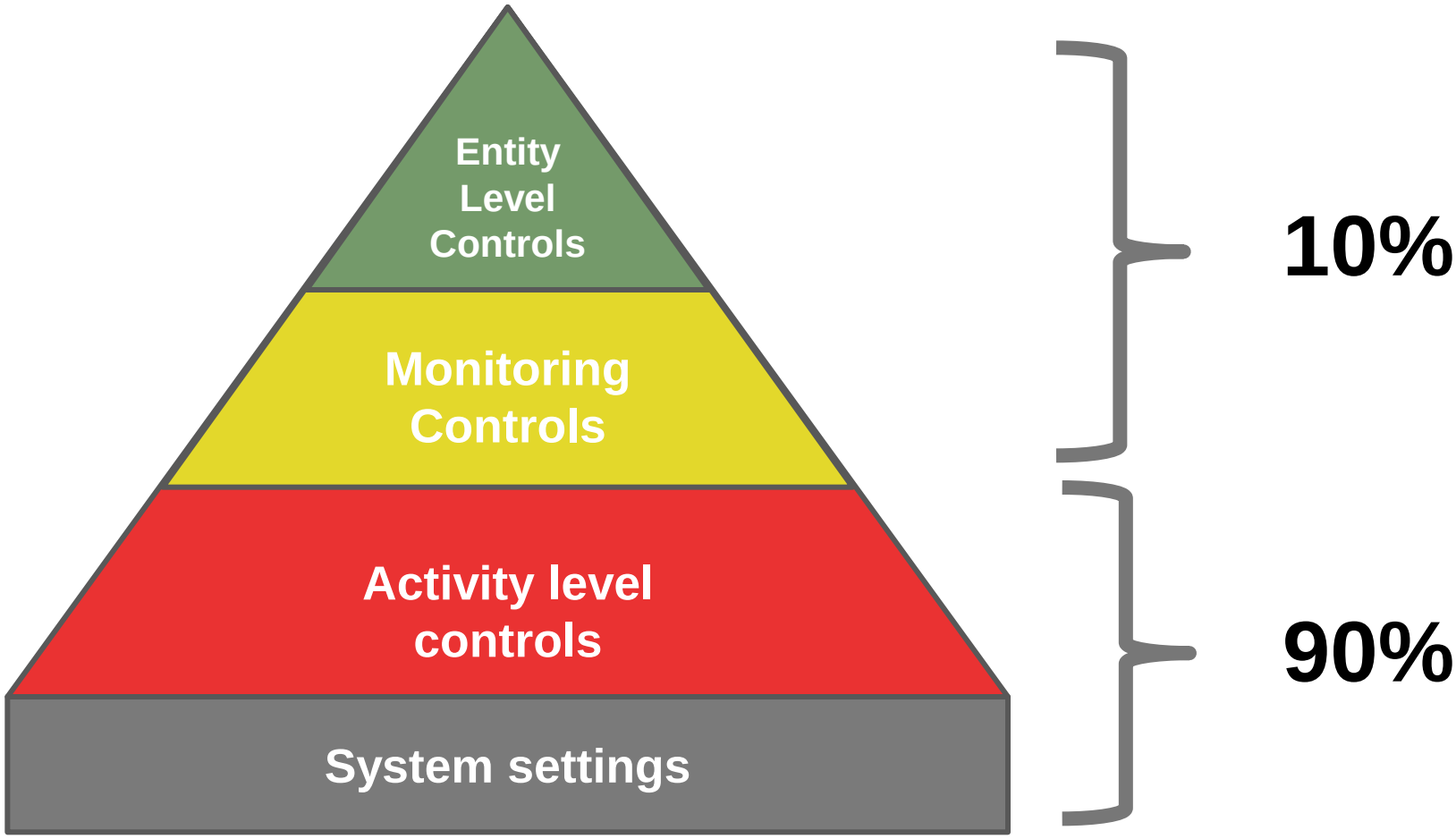
Management buy in 100% - no compromise

Compliance focus – cost/benefit not in focus

Focus on activity controls with evidence of control activity

Strict requirements on evidence of performed controls

FOCUS ON DETAILS



REDUCTION IN COST

High initial cost to implement SOX

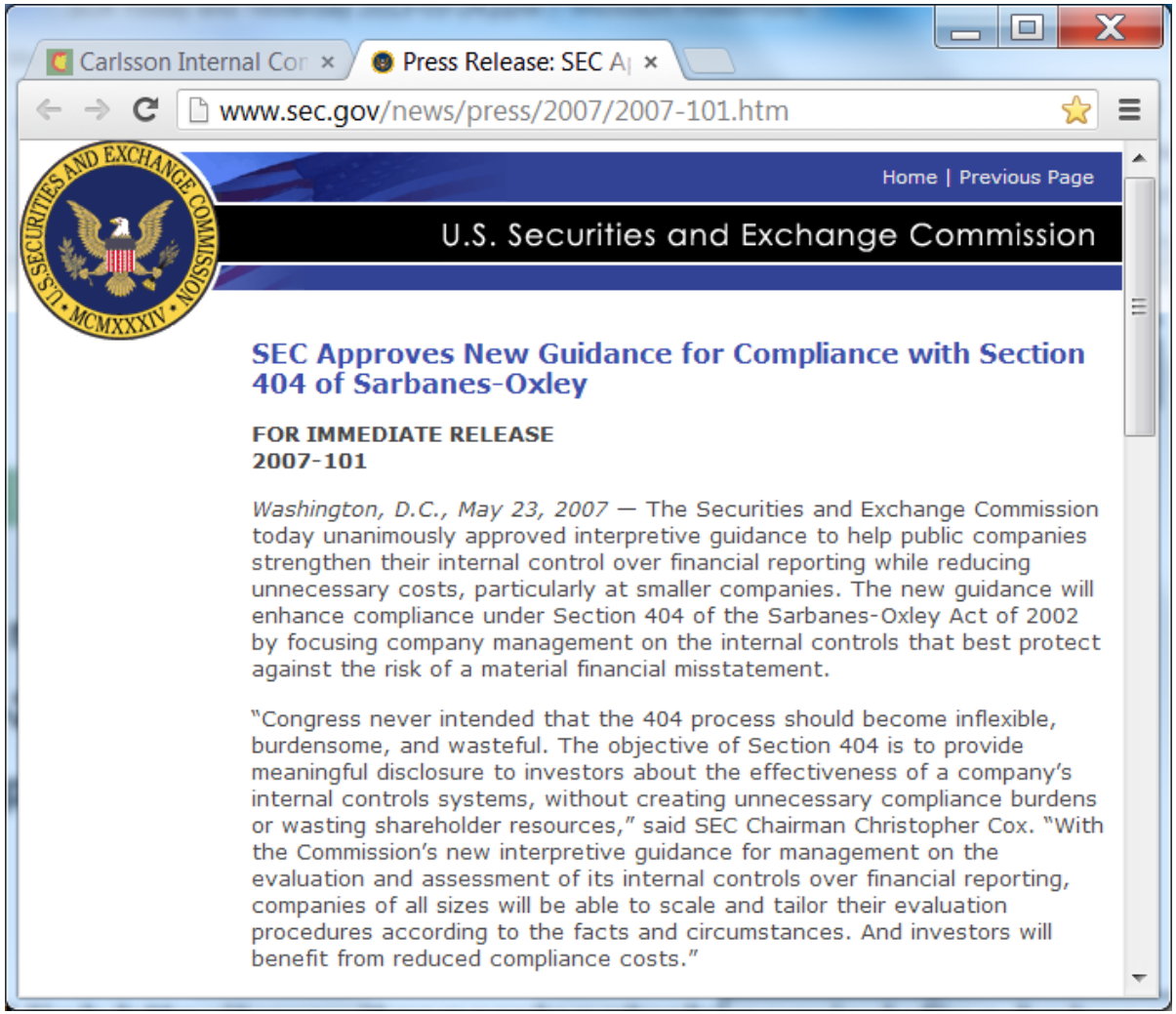
Cost reduced to maintain SOX compliance

Increased knowledge

Year	% of Revenue
2005	0,056%
2006	0,043%
2007	0,036%

Source: Finance Executives International (FEI)

NEW GUIDANCE



CHANGES

SOX requirements

- 2007 new guidance, top-down risk assessment based
- 2007-2010 exemption for smaller public companies

"With the Commission's new interpretive guidance for management on the evaluation and assessment of its internal controls over financial reporting, companies of all sizes **will be able to scale and tailor their evaluation procedures according to the facts and circumstances**. And investors will benefit from reduced compliance costs."

Maturity

- IT departments are more aware of internal control
- ITIL is introduced in many organizations

IMPLEMENTING SOX TODAY

SOX audit not very different from normal Swedish audit of larger organizations

Companies have better understanding of internal control

Availability of expertise and know-how

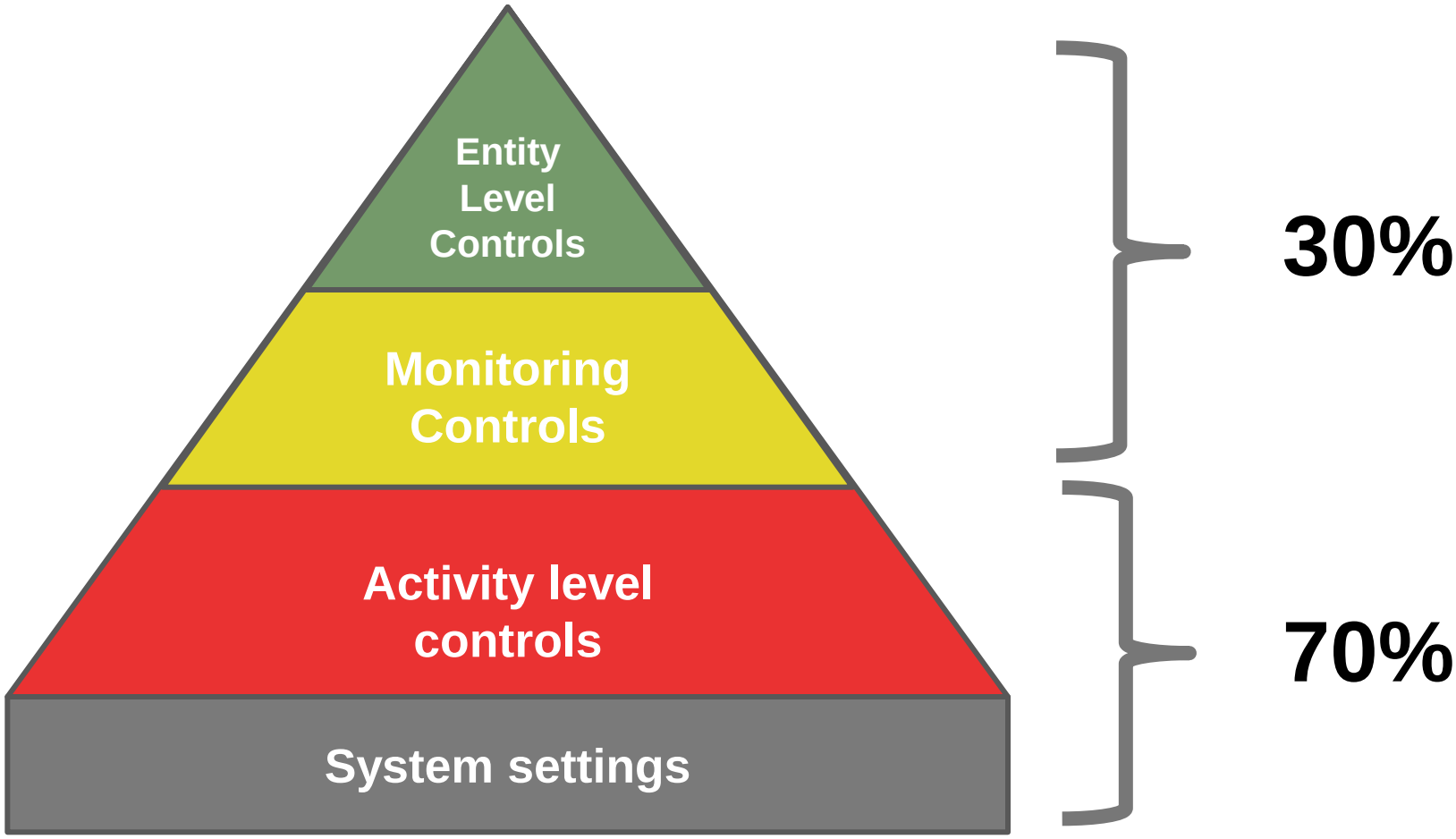
SOX compliance has high priority, but cost/benefit and risk is taken into account

Cobit is still the primary guidance for scope, control objectives and controls

No history of prosecuted management

More relaxed, sensible SOX projects

SHIFT IN FOCUS



SOX LEGACY

Based on experience from SKF

SOX requirements 2005-2007

Built SOX IT control framework covering systems and organizations in SOX scope

SOX IT controls covered central SKF Group IT, Local business units and the IT outsourcing partner.

Yearly management test was performed by an external party

POSITIVE EFFECTS OF SOX

Implementation of IT Internal Control

Increased transparency with suppliers

Increased transparency with local business units

Clarified responsibilities

More effective ways of handling IT Governance, Local Units started to communicate with each other

Common systems better utilized due to common SOX Financial processes and control over local adaptations

Simplified contract negotiations with suppliers of IT services

SKF INTERNAL CONTROL STANDARD (SICS)

No external requirement to keep SOX controls and SOX management test

New control framework, SICS, based on SOX controls

- Keep the benefits of SOX control framework
- Remove or reform inefficient/ non value add controls and testing
- Scope extended to business critical systems and not only systems critical for financial reporting
- Scope extended to more business units
- Regulate the responsibility split with outsourcing partner

SCOPE CHANGE

Business units

- Medium and smaller units included in the scope of management test
- Increase with 40% number of business units tested

Systems in scope

- Systems critical for financial reporting are in scope (SOX)
- Systems that are critical for the operations
- Systems that are critical for legal compliance

RISK BASED TESTING

High risk business units

- Full management test
- On site test

Medium risk business units

- Not always tested or only some aspects are tested
- Remote test team
- Self test with auditor follow-up

Units that are doing well are tested less often

Remote test works well with IT-suppliers especially IT Operations

COST SAVINGS

Off-site testing for units that are doing well (60-65%)

Information for testing prepared and gathered before test

- Selected sample to test is sent to local units in advance
- Local units collect information
- Auditor may collect additional samples at time of test

Focus on objectives of testing

- Removed formalities around signoffs
- Email etc are acceptable as evidence

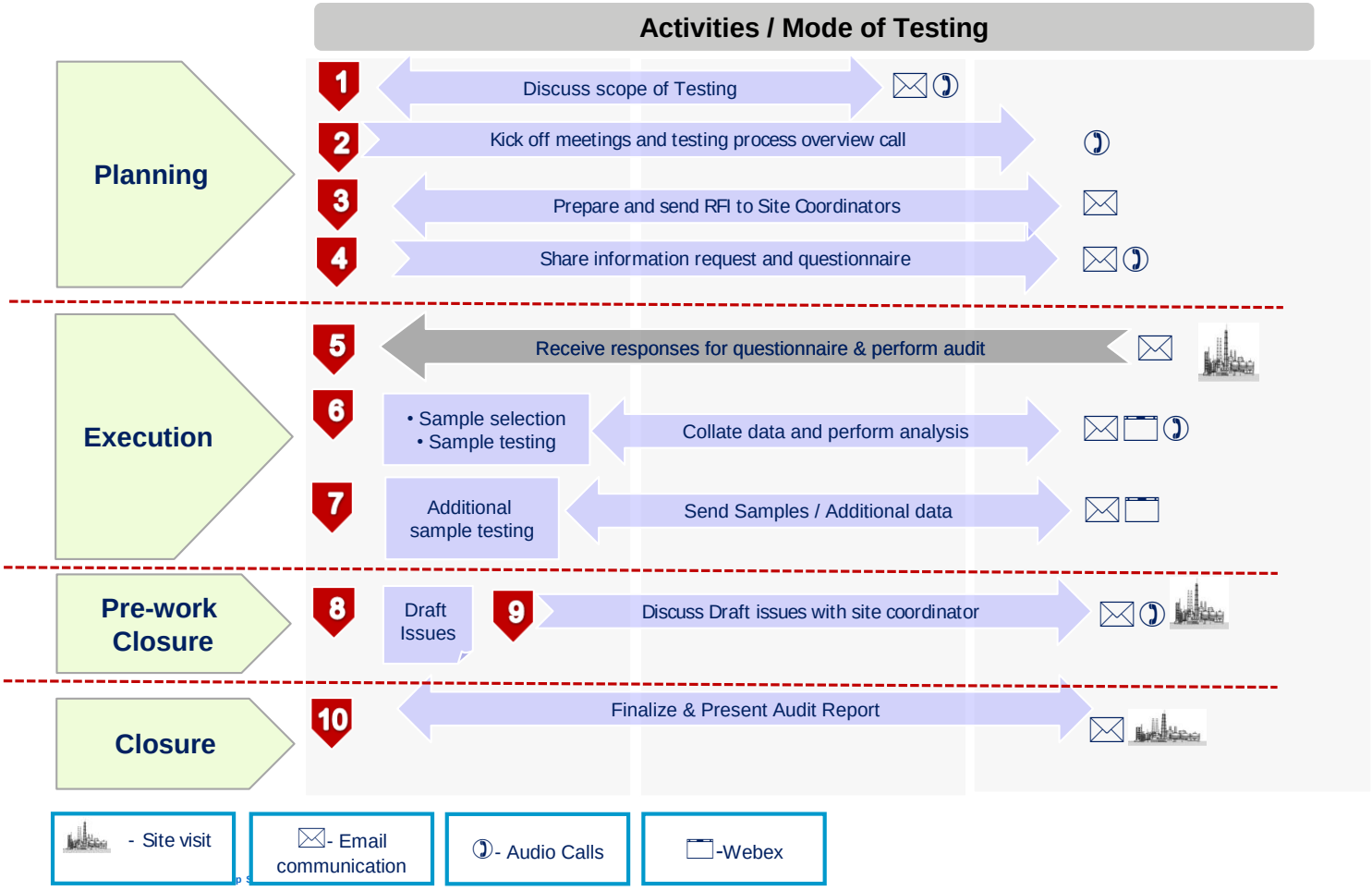
Removal of technology specific tests of IT operational controls in favor of more generic controls and tests.

Fine tuned the budgeting and planning of annual testing.

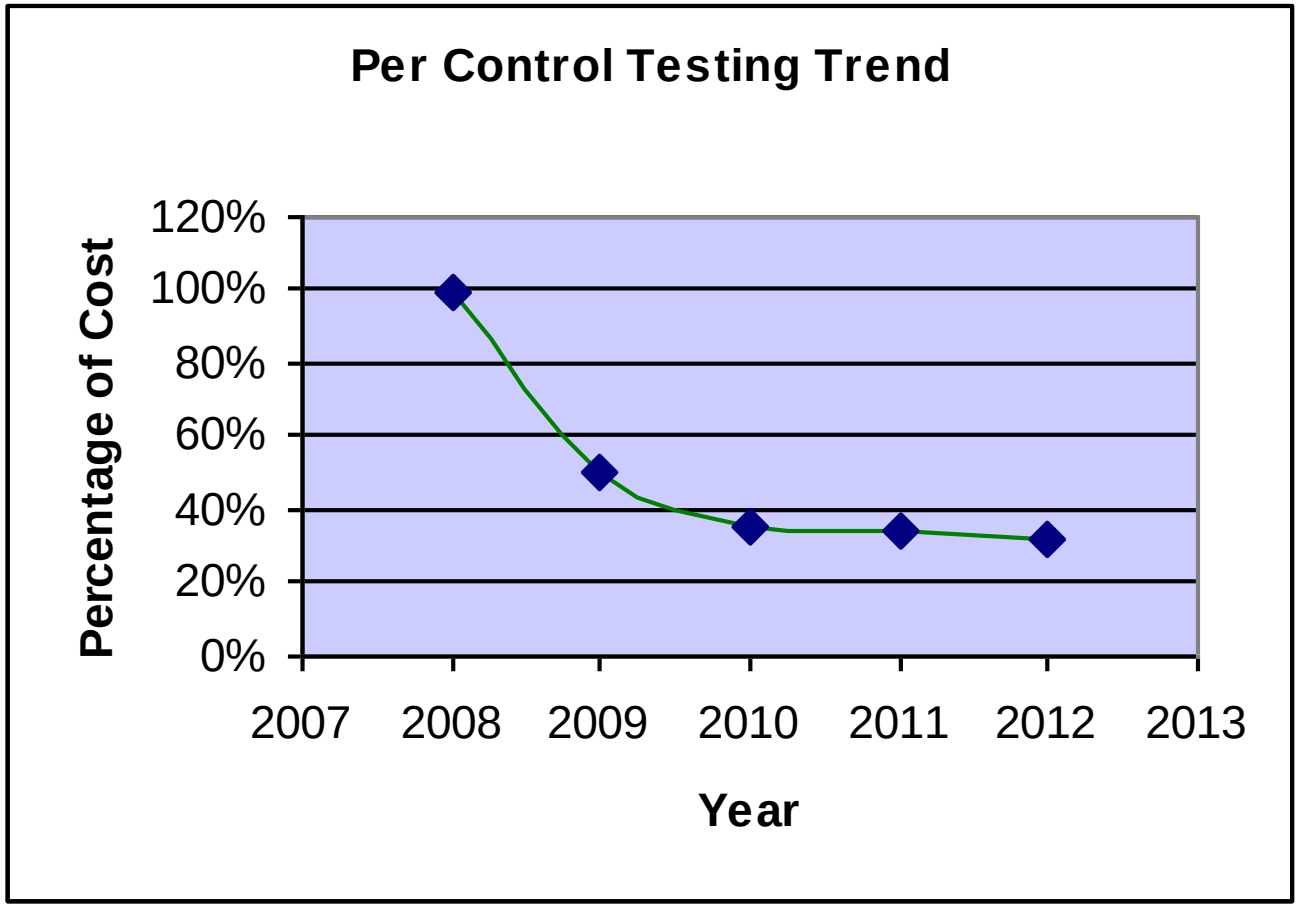
Global resources used, leading to lower cost of testing.

Controls have simplified contract negotiations with suppliers of IT services.

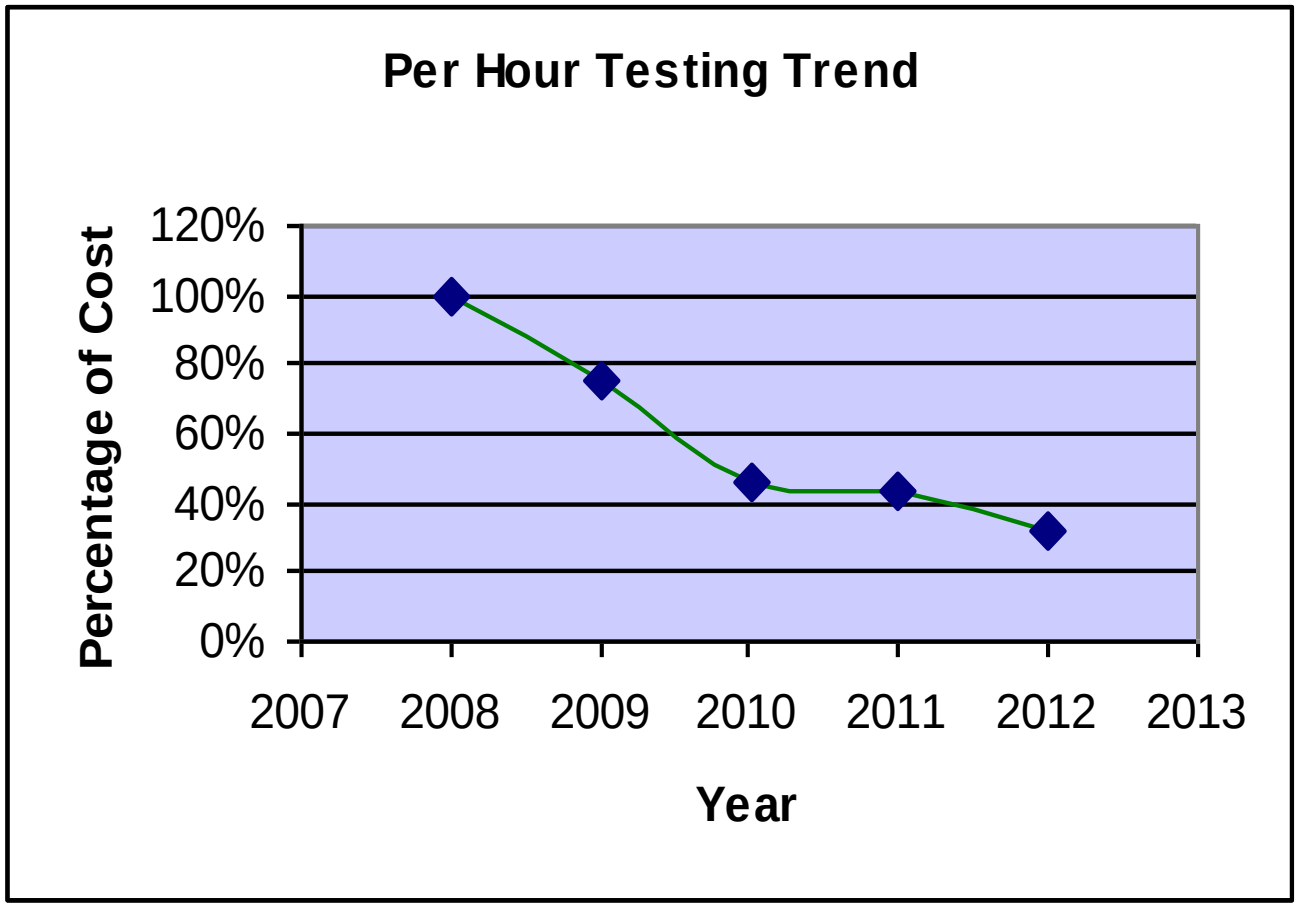
TESTING APPROACH



DECREASING COST (1/2)



DECREASING COST (2/2)



CONCLUSION

SOX does not cost as much today

It is not as painful as before

An internal control framework has benefits beyond SOX compliance

MY THANKS TO

Rudragouda Patil
Compliancy Manager SKF

&

Anette Alsteryd
CIO Elfa Group

Who made this presentation possible.

THANK YOU

Harald Carlsson

Carlsson Internal Control Consulting AB

+46 707-293131

harald.carlsson@cicc.se

www.cicc.se