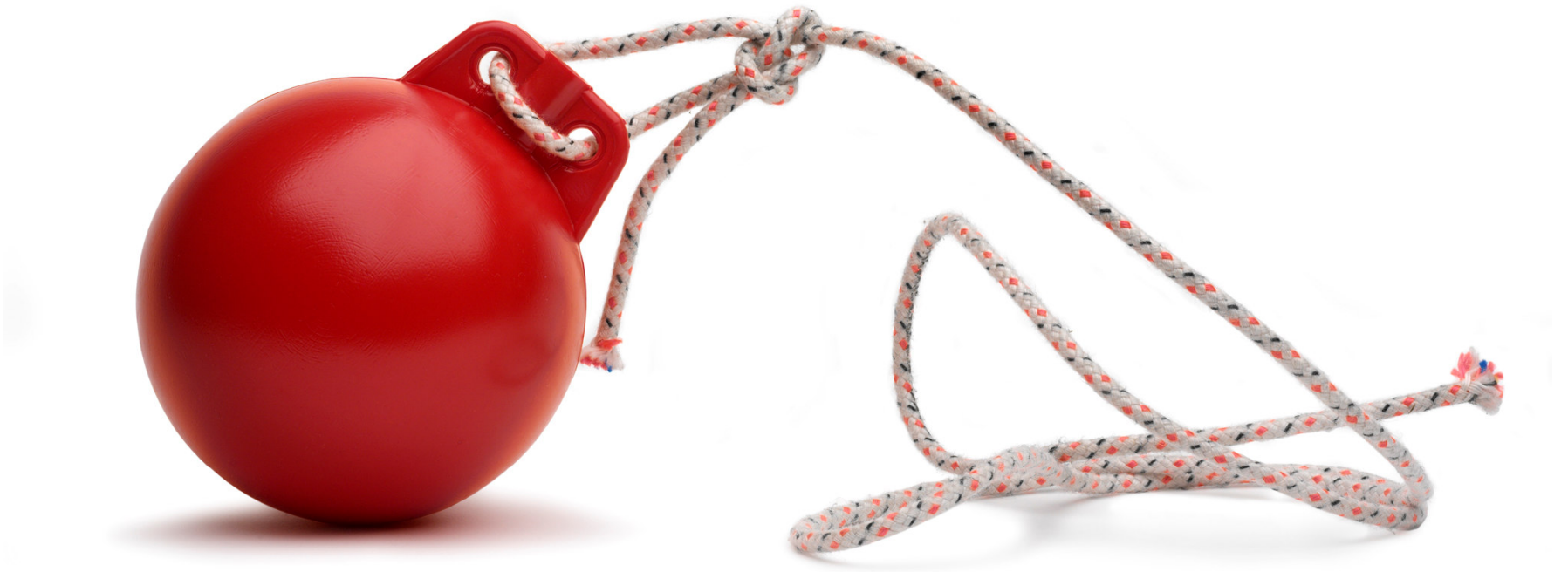
Technology Security and Risk Services



Information Technology and Security Governance

Internetdagarna 2006-10-25

Andreas Halvarsson

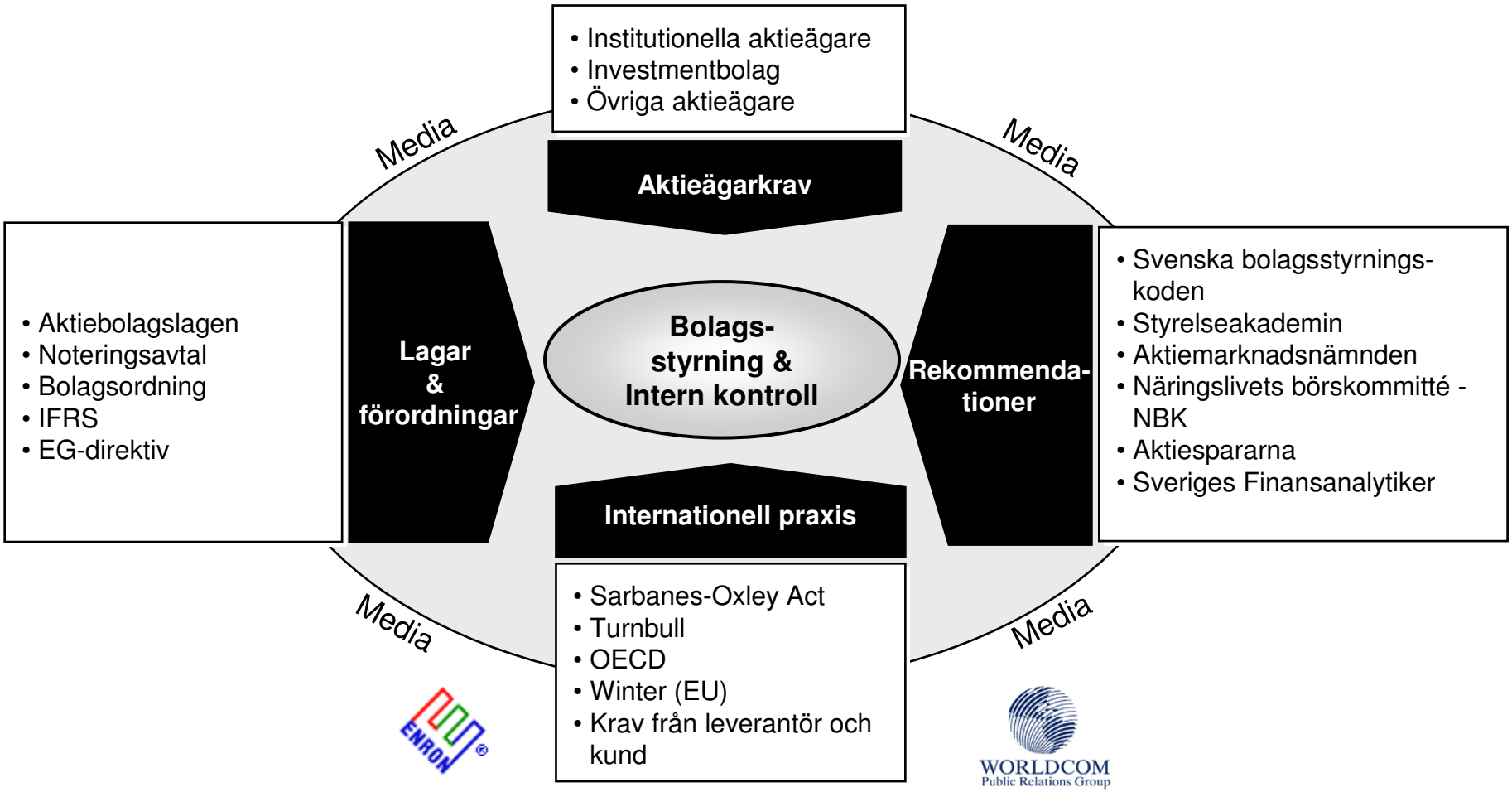
ERNST & YOUNG

Quality In Everything We Do

Lapp på anslagstavlan hos IT-leverantör

Förr	**Nu**
Prästen	Ekonomen
Kyrkan	Börsen
Exekutionen	Revision
Alkohol	Losec

Utmaningarna för IT-governance är inte vad de varit…..



ERNST & YOUNG
Quality In Everything We Do

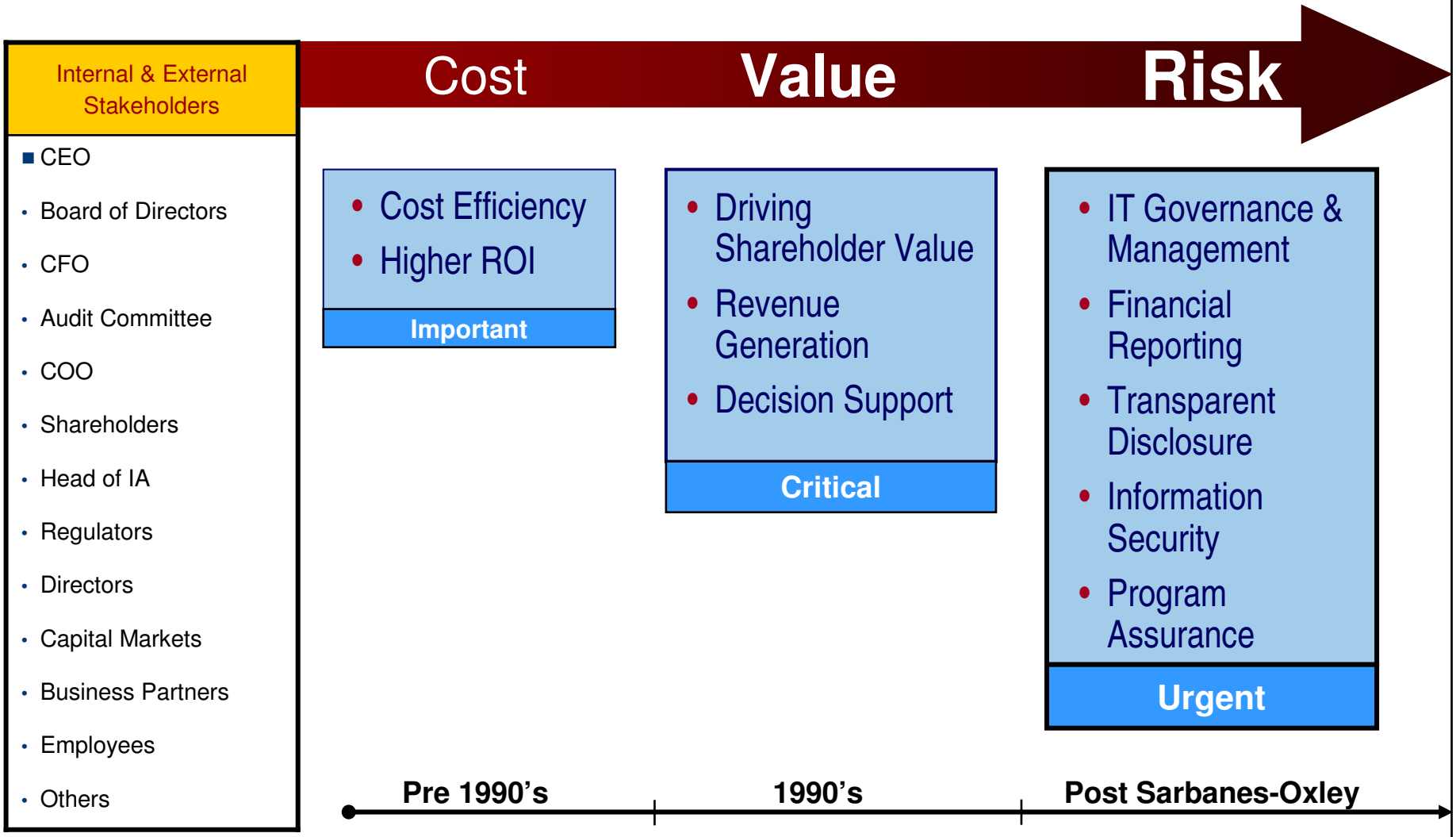
Sarbanes-Oxley Act

- **Congressman Mike Oxley:**
  - "Sarbanes-Oxley compliance is an investment in every company, it is an investment in our financial system, and it is an investment in the strength of the United States capital markets"
- **Federal reserve Chairman Alan Greenspan**
  - "(The Sarbanes-Oxley Law) importantly reinforced the principle that . . . corporate managers should be working on behalf of shareholders to allocate business resources to their optimum use."
- **Effektiv implementering av Section 404 är till fördel för den investerande allmänheten**
  - Mer trovärdiga och transparanta ekonomiska rapporter
  - Ökat investerar förtroende
  - Reducerade kapitalkostnader för utfärdare
  - Reducerad risk för bolagsbedrägeri

SOX och den Svenska Bolagsstyrningskoden

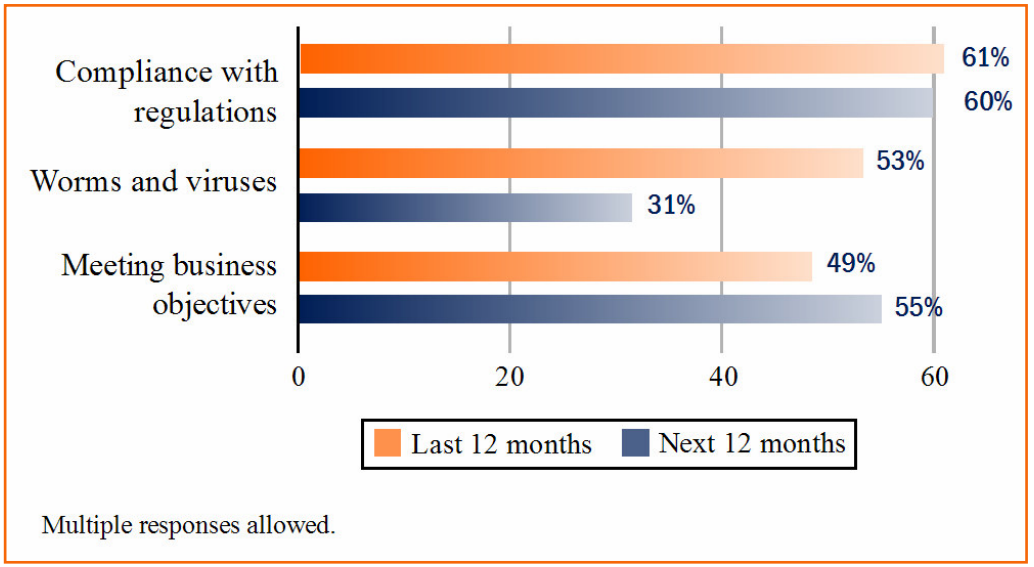
	Svenska Bolagsstyrningskoden ”Intern kontroll över finansiell rapportering”	SOX 404
Grund	Kod & rekommendation	Lagar & förordningar
Ansvar	Styrelsen	Ledningen
Bolagets redovisning	Beskrivande	Avvikelser
Bekräftelse	Styrelsens beslut	Ledningens beslut
Sanktion	Förteckning över slutsatser	Betydande enskild bestraffning
Krav på kontroll dokumentation	Inga formella krav	PCAOB krav
Revision	Ja	Ja

Increasing Expectations of IT Function



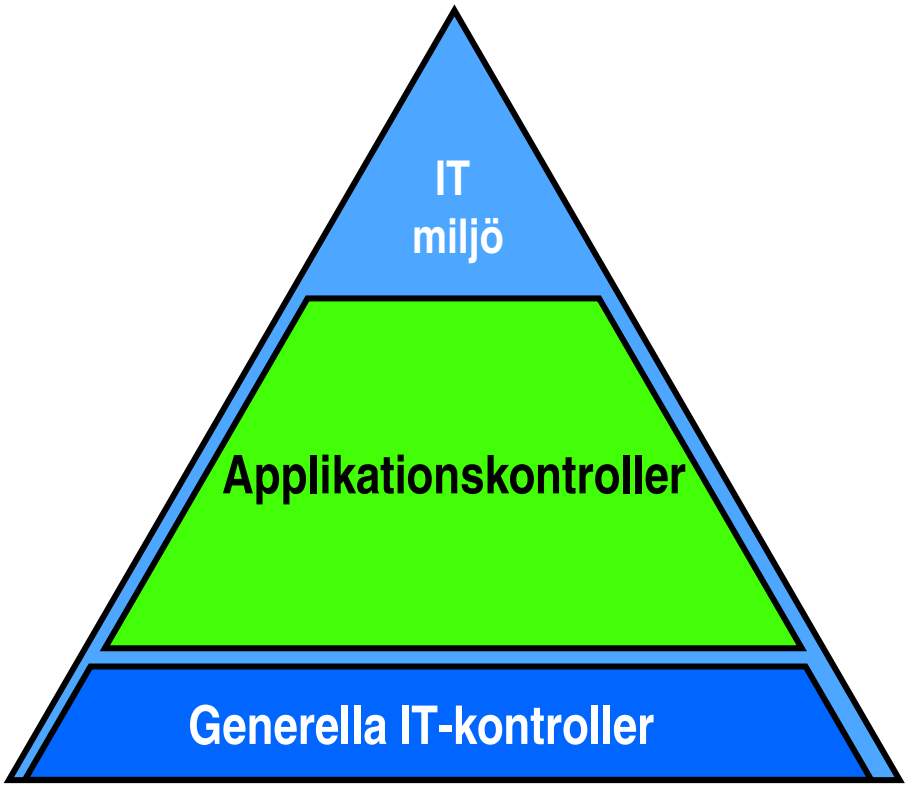
Compliance leder i prioritet

- Nästan 2/3 av respondenterna säger att compliance är topp och att det överskuggar maskar och virus.



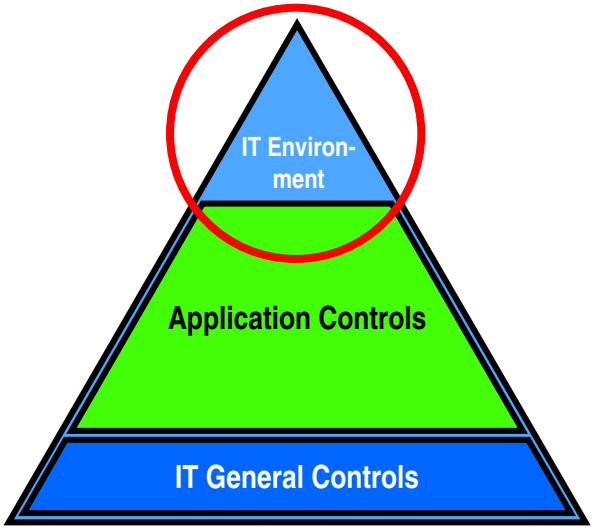
Källa: Ernst & Young Global Information Security Study 2005

Kontrollstruktur



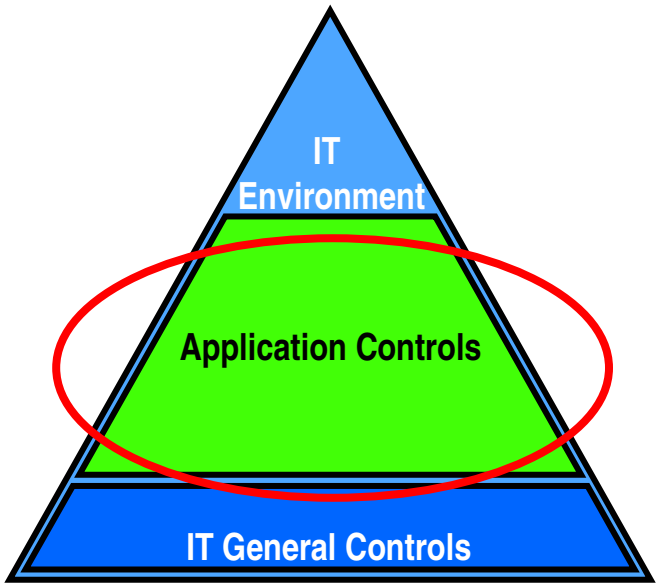
Vad påverkar IT miljön?

- IT-beroende och komplexitet
- IT- organisation
- Strategi och styrning avseende IT
- Förekomst av policy och riktlinjer
- Riskanalyser
- IT-resursernas ändamålsenlighet
- Övervakning av kapacitet och kontroller
- Uppföljning och granskning
- ...



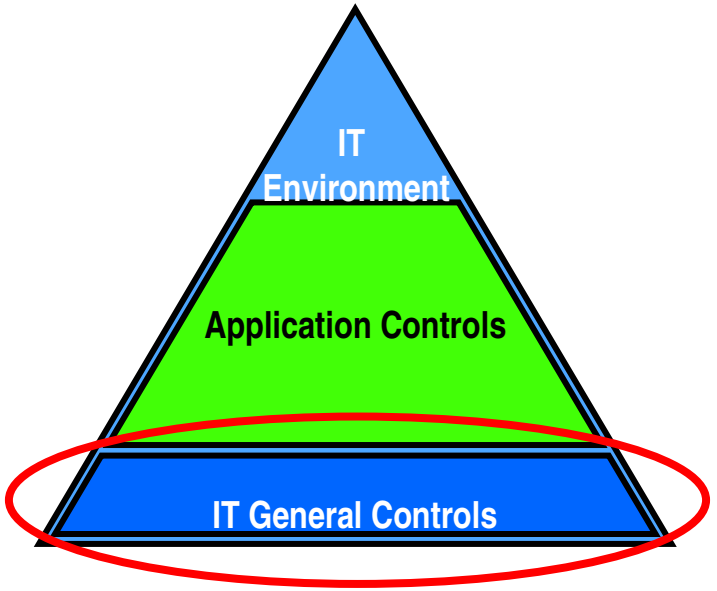
Applikationskontroller

- Kontroller relaterade till specifika applikationer eller transaktioner.
- Syftar till att säkerställa integritet, fullständighet och riktighet.
- Exempelvis indata-, bearbetnings- och utdatakontroller.



Generella IT-kontroller

- IT kontroller som är gemensamma för hela IT-verksamheten
- Utgör basen för fungerande applikationskontroller över tiden
- Exempelvis behörighetsrutin och rutin för programuppdateringar



Frågor som borde ställas

- I vilken utsträckning är IT riskerna som företaget står inför allmänt kända?
- Hur väl känner dina leverantörer till de ökade kraven?
- Vilka aktieägare är involverade i bedömning och överenskommelse av risk? Externa revisorer, revisionskommittée, CIO, internrevision, annan företagsledning, ledning, andra företagsövergripande risker, betydande tredje man?
- Hur svarar din riskbedömningsprocess på nya företag och IT strategier?
- Kan du effektivt och konsekvent bestämma följden och sannolikhet av dina IT risker, skulle företaget hålla med om IT utvärderingen?
- Använder du dig av oberoende rådgivare? Gör skillnad på produkt, tjänst och kopplingar dem emellan.
- Har din organisation torrt på fötterna?

Lärdomar av utförda governance arbeten, läs Bolagsstyrningskoder

1: IT spelar en betydande roll i detta initiativ
2: Identifiera IT processen som är väsentlig för bolagets verksamhet
3: Förståelse av relationen mellan IT och manuell kontroll är väsentlig
4: Adressera frågor lägligt med tanke på outsourcad 3de part
5: Fastställ en metod för att på ett korrekt sätt identifiera och reagera på kontroll undantag
6: Inverkan på Ansvarsfördelning
7: Viktiga projekt skall ALLTID innehålla en Program Assurance, dvs att projektet granskas av en tredje part.

Tack!

Andreas Halvarsson
08-520 594 55, andreas.halvarsson@se.ey.com