Deloitte.

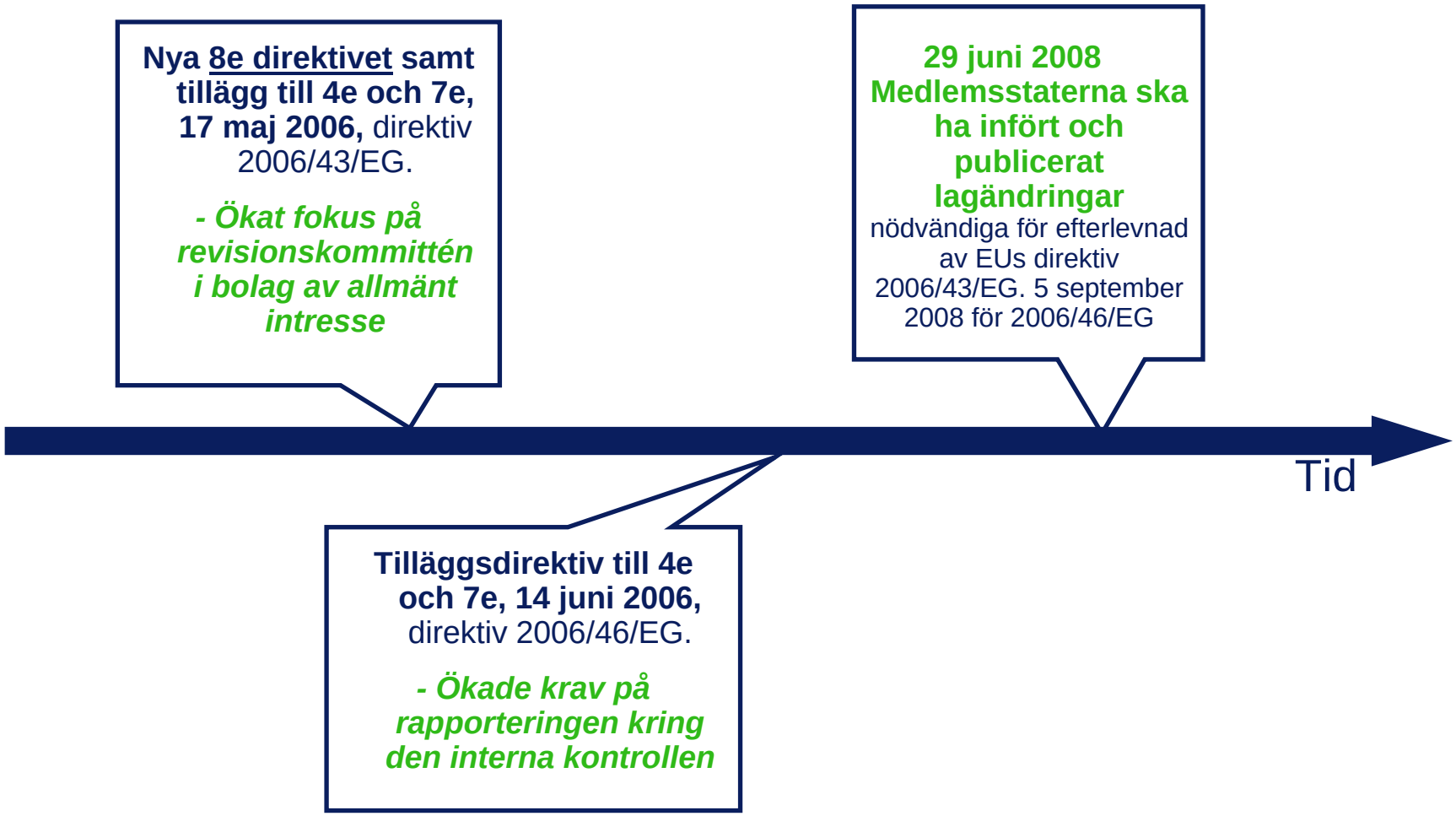
Kontroll över IT –
för efterlevnad och framgång

Johanna Wallmo
Peter Tornberg

Agenda

- Direktiv från EU - tidsplan
- EU:s 8:e direktiv: syfte och innehåll
- Hur kommer svenska bolag att påverkas?
- Utmaningar vid övervakning av den interna kontrollen
- IT:s betydelse för intern kontroll
- Krav på utformning kontrollaktiviteter

Direktiv från EU - tidsplan



EU:s 8:e direktiv - syfte

- Harmonisering av arbete avseende revision och intern kontroll
- Minimera finansiella och förvaltningsmässiga risker
- Höja kvaliteten på den ekonomiska rapporteringen

EU:s 8:e direktiv – innehåll om intern kontroll

- Företag av **allmänt intresse** ska ha en revisionskommitté
- Revisionskommittén övervakar effektiviteten i:
  - Företagets interna kontroll
  - Internrevision
  - Riskhanteringssystem
  - Finansiella rapporteringen
- Den valde revisorn rapporterar viktiga iakttagelser med särskilt fokus på materiella svagheter i den interna kontrollen över finansiell rapportering
- Styrelsen har yttersta ansvaret för god intern kontroll

Påverkan på svenska bolag

No more excuses

Påverkan på svenska bolag, forts.

Tillämpning	***Det nya EU-direktivet kommer att omfatta fler bolag, såsom börsnoterade bolag och bolag av allmänt intresse***
Styrelse & Ansvar	***Ansvaret för en god internkontroll ligger liksom tidigare på styrelsen som helhet. Skillnaden blir att ett särskilt organ ska inrättas, d v s revisionskommittén, för att arbeta med internkontroll***
Intern kontroll	***Alla omfattade bolag skall ha en revisionskommitté som skall övervaka den finansiella rapporteringen och effektiviteten i företagets internkontroll, eventuella internrevision samt riskhanteringssystem.***
Rapportering	***Alla noterade bolag omfattas av rapporteringskravet och förväntas avlägga en rapport om vilken kod som tillämpas samt hur den interna kontrollen är organiserad och vilka avvikelser som förekommit från tillämpad kod.***

Viktigt att notera…

“Det är viktigt att notera att exakt hur den svenska lagtexten kommer att utformas, till följd av EU:s 8:e direktiv, ännu inte är fastställt. Klart är dock att frågor rörande intern kontroll får en allt större betydelse för företag och dess intressenter.”

Utmaningar för företag vid övervakning av intern kontroll

- Tillgång till resurser (tid, pengar och personal)
- Ansvarsfördelning
- Förankring hos ledningen
- Riskfokusering
- Rätt risk och kontrolldefinitioner
- Förändrade arbetssätt
- Varaktig fokus – ej ett ”engångsprojekt”
- IT-stöd

Ansvarsområden för IT

- Kartläggning av IT system som stödjer den finansiella rapporteringen
- Identifiering av risker relaterat till IT system
- Utformning och implementering av kontroller för att hantera risker
- Dokumentering och testning av IT kontroller
- Kontinuerlig uppföljning av kontroller

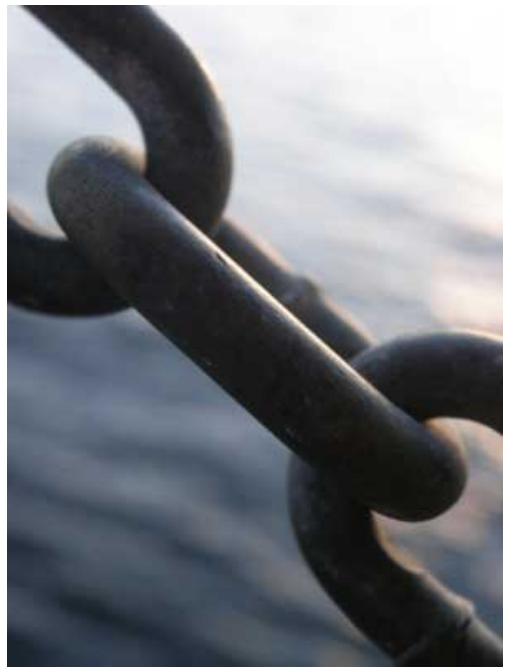
De kritiska applikationerna och infrastrukturen

Väsentliga poster

Affärsprocesser

Finansiella applikationer

IT Infrastruktur

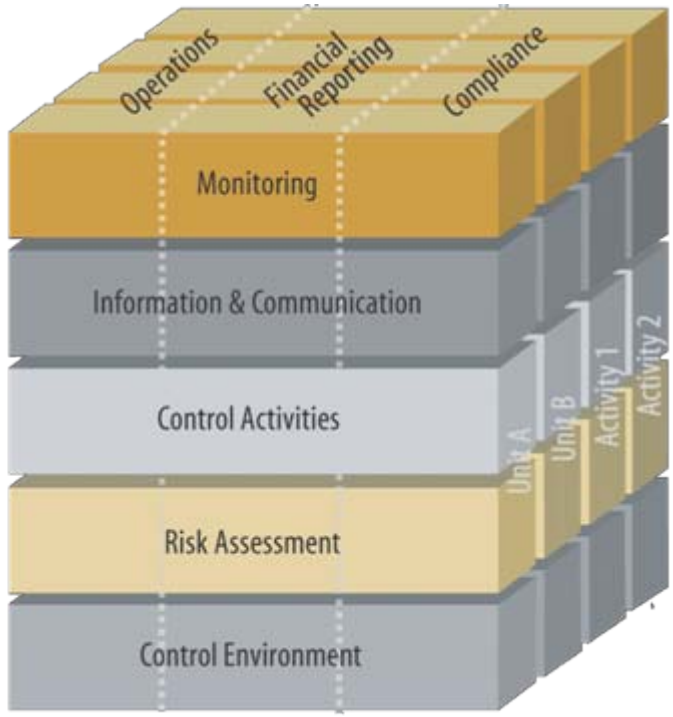


Kritiska IT-områden

- Informationssäkerhet
  - Integritet
  - Konfidentialitet
  - Tillgänglighet
- Fokus på finansiell rapportering
  - 3 kontrollområden specifikt identifierade
  - Programförändringar, drift och åtkomstkontroll
- Hur uppnå detta?
  - Tydlig och kommunicerad strategi
  - God identitets- och accesskontroll
  - Business Continuity Plan
  - Change Management
  - Configuration Management
  - Patch Management
  - ...

Områden

- Uppföljning
- Riskbedömning
- Information och kommunikation
- Kontrollaktiviteter
- Kontrollmiljö

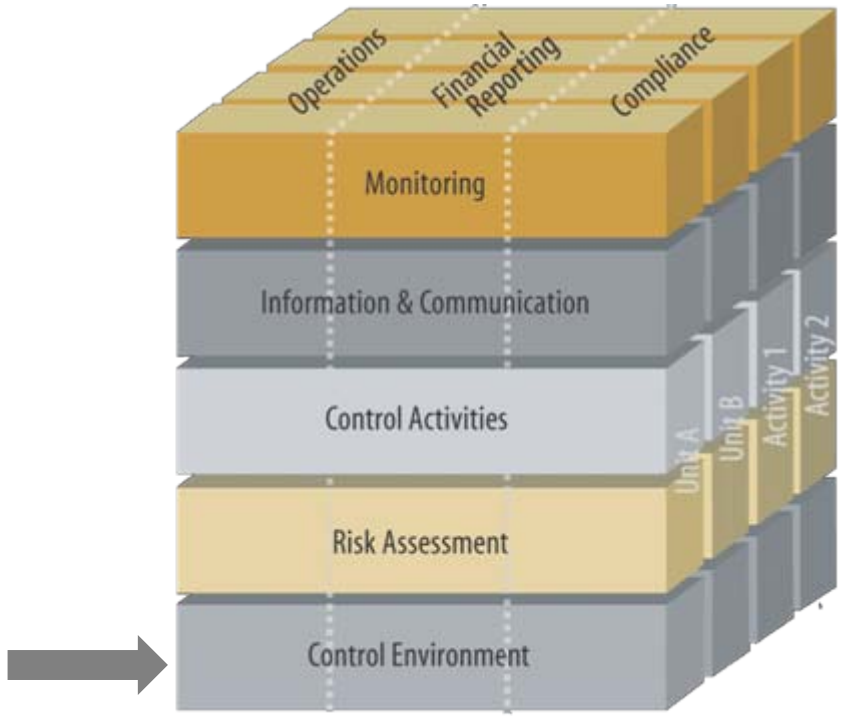


Kontrollmiljö

Den interna kontrollmiljön innefattar det arbetsklimat som finns i organisationen och som bestämmer utgångspunkten för hur organisationens medarbetare ser på och förhåller sig till risker.

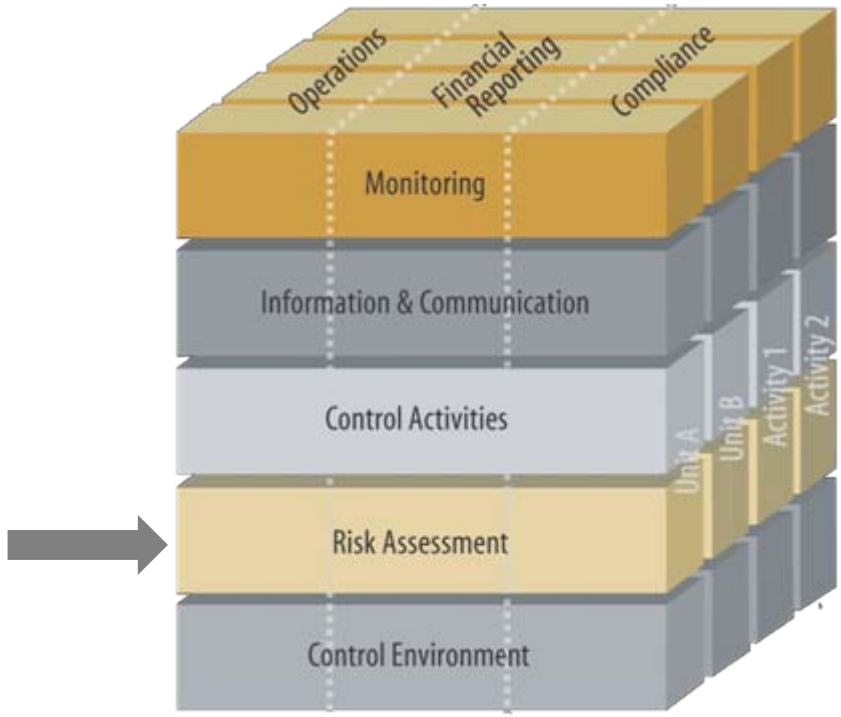
Exempel:

- IT ingår i den övergripande kontrollmiljön
- Dokumenterade policys och procedurer
- Definierat ansvar för IT-kontroller



Riskbedöming

Risker analyseras, med utgångspunkt från deras sannolikhet och konsekvenser, för att få ett underlag för hur de ska hanteras. Risker bedöms både före och efter hantering, dvs. både som ursprungliga och återstående risker.



Exempel:

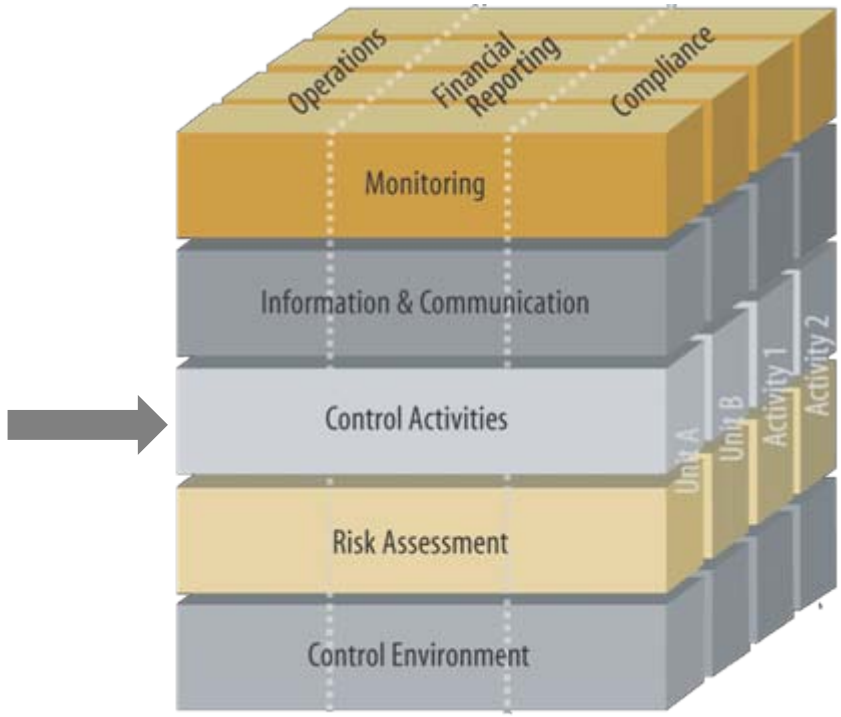
- En riskbedöming för IT är upprättad
- IT-risker behandlar säkerhet, drift, tillgänglihet etc.
- Ledningen har en förståelse för innebörden av IT-risker och de kontrollaktiviteter som hanterar dessa risker

Kontrollaktiviteter

Riktlinjer och rutiner fastställs och genomförs för att säkerställa att riskåtgärderna genomförs på ett effektivt sätt.

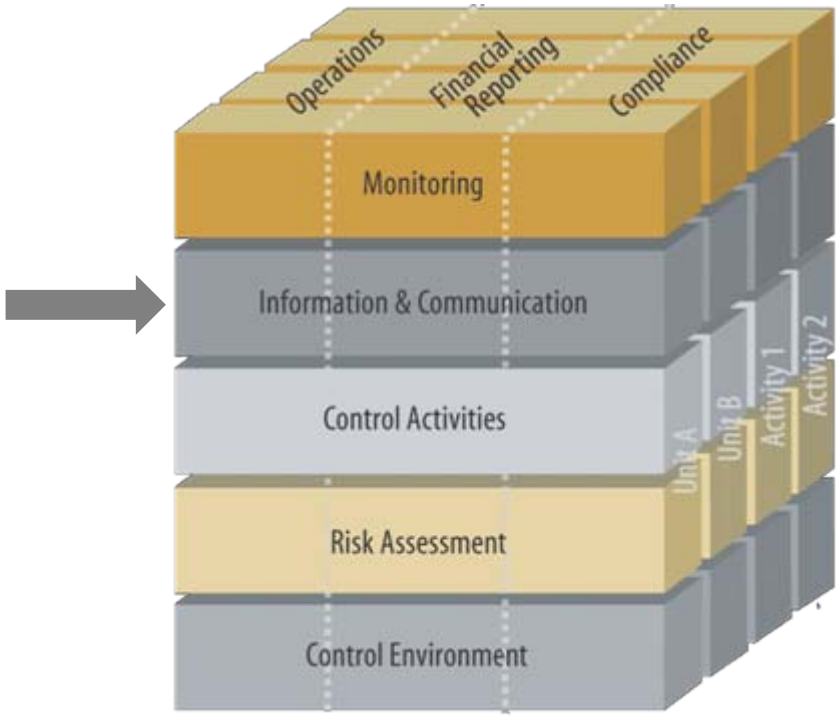
Exempel:

- Segregation of duties
- Auktoriseringar
- Utvärderingar



Information och kommunikation

Relevant information identifieras, samlas in och förmedlas i en form och inom en tidsram som gör det möjligt för de anställda att utföra sina åtaganden.

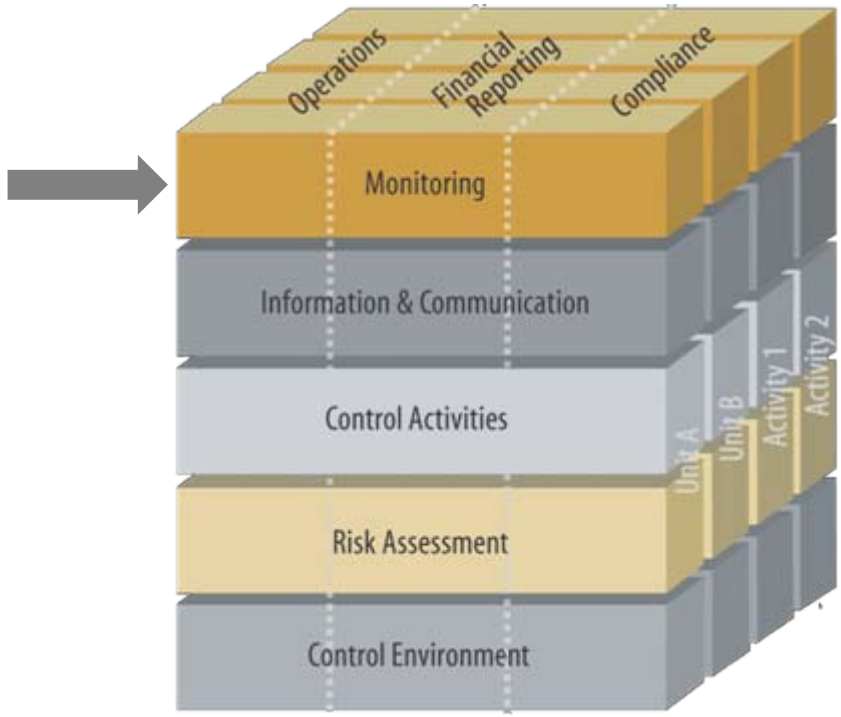


Exempel:

- Utbildning
- Möten
- Kvartalsbrev
- Rapporter

Uppföljning

Hela den företagsövergripande riskhanteringen övervakas och modifieras när det behövs. Övervakning sker genom löpande ledningsaktiviteter inklusive uppföljningar, separata utvärderingar, eller bådadera.



Exempel:

- IT kontroller följs upp för att säkerställa att de är lämpliga och fungerande
- Brister i kontroller åtgärdas på lämpligt sätt
- Löpande säkerhetsövervakning


Deloitte.