The Institute of Internal Auditors

Vad är Internrevision?

Ett material framtaget av
Advocaykommittén februari 2020

Syfte

- Syftet med denna presentation är att ge dig som internrevisor ett material för att beskriva Internrevision.
- Den är framtagen av medlemmarna och kan ses som en inspiration och ett hjälpmedel, snarare än ett officiellt dokument.
- Presentationen är en föreslagen struktur som kan anpassas efter behov och vilka intressenter som presentationen vänder sig till. Bilder ska tas bort eller läggas till.
- I slutet av presentationen finns ett appendix med några alternativa bilder.
- På IIA Globals hemsida finns mycket material att ladda ner t.ex.
  - Internal Auditing -Adding value across the board
  - Internal Auditing –Assurance, Insight and Objectivity
  - All in a days work

Innehåll

1. **Vad är internrevisionens uppdrag**
2. **Vad är internrevision**
3. **Vad gör internrevisionen**
4. **Vad styr internrevisionen**
5. **Internrevisionens spelplan** - vad är intern styrning och kontroll?
6. **Revisionsprocessen** – hur bedriver internrevisionen sitt arbete?
7. **Internrevisionens värdeskapande roll**
8. **Specifika regelverk per sektor** – privata och offentliga verksamheter

1. Vad är internrevisionen uppdrag?

Uppdraget

Internrevisionens definierade uppdrag är:

”Att utveckla och skydda organisatoriska värden genom att tillhandahålla riskbaserad och objektiv försäkran, råd och insikt”.

Internal auditing = Assurance, Insight and Objectivity

2. Vad är internrevision?

The Institute of Internal Auditors (The IIA)

- Finns en yrkesorganisation för internrevisorer
- Är världsledande inom utbildning, utveckling, forskning och teknisk rådgivning för internrevisorer över hela världen
- Certifierar yrkesverksamma internrevisorer
- Tillhandahåller principbaserad normgivning
- Grundades 1941 och har ca 200 000 medlemmar i mer än 170 länder
- Läs mer på www.globaliia.org

Definition av Internrevision

Internrevisionens grundprinciper:

- Har integritet
- Har kompetens och professionellt omdöme
- Är objektiv och fri från otillbörlig påverkan (oberoende)
- Arbetar i linje med organisationens strategier, mål och risker
- Har rätt placering i organisationen och har tillräckliga resurser
- Levererar med kvalitet och ständiga förbättringar
- Kommunicerar effektivt
- Tillhandahåller riskbaserad försäkran
- Är insiktsfull, proaktiv och framåtsiktande
- Främjar organisatorisk förbättring.

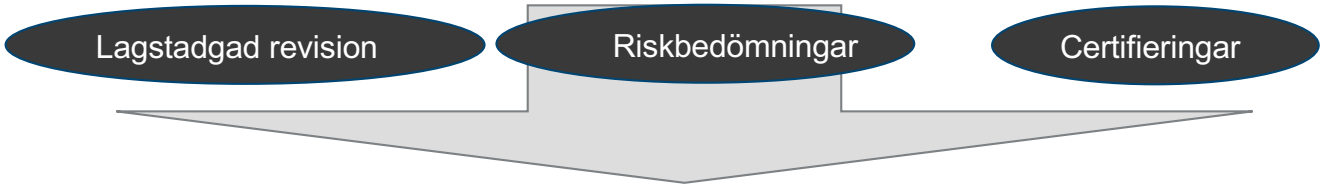
Dessa principer avser både en internrevisionsfunktion och den enskilde internrevisorn. Enligt IIA ska samtliga dessa principer vara beaktade och aktivt efterlevas om en internrevisionsfunktion ska anses agera i linje med det definierade uppdraget. Hur detta tar sig uttryck kan emellertid variera beroende på vilken typ av organisation det handlar om.

Definition av Internrevision

- Internrevisionen hjälper organisationen att nå sina mål genom att utvärdera och bidra till förbättringar av styrprocesser och riskhantering.

- En förutsättning och ett övergripande mål är att Internrevisionen har organisationens förtroende och i det avseendet har kompetens att internt agera som en betrodd/tillförlitlig rådgivare (Trusted Advisor).

Likheter och olikheter
IR, andra revisionsroller och liknande aktiviteter



	Externrevision	Tredje part -bedömningar	"Blue Surveys"	Internrevision	Interna bedömningar
På uppdrag av	Aktieägare (oberoende av styrelse och ledning)	Verksamhetsledning (Baserat på externa verksamhetsrelaterade krav exempelvis ISO certifieringar)	Externa försäkringsaktörer och verksamhetens riskansvariga funktioner.	Styrelsen (oberoende av verksamhetsledningen)	Verksamhetens linjeorganisation. (syfte att säkerställa effiektivitet, styrning och måluppfyllelse)
Huvudsaklig uppgift	Verifiering av extern rapportering exempelvis årsredovisningar, verksamhetsrapporter …..övriga rapporter-	Certifieringar och liknande.	Verifiering av standarder för riskhantering vid specifika fysiska platser och förslag till förbättringar, om nödvändigt.	Validering av riskhantering och intern styrning.	Behovsbaserade operationella bedömningar.
Fokus	Intern styrning av finansiell rapportering. Finansiella uttalanden i externa rapporter. Legal efterlevnad. Segregation of duties	Efterlevnad av standarder och verksamhetskoder. Efterlevnad av styrdokument.	Efterlevnad av försäkringsgivares standarder och verksamhetens egna relevanta instruktioner.	Revisioner av prioriterade verksamhetsrisker baserade på reguljära konsoliderade verksamhetsriskbedömningar.	Efterlevnad av standarder och verksamhetskoder. Efterlevnad av styrdokument.
Risk bedömning	Verksamhets- och operationell finansiell förvaltning med fokus på den legala externa rapporteringens korrekthet.	Operationell förvaltning.	Operationell förvaltning.	Förvaltningen av huvudsakliga och verksamhetsväsentliga risker.	Förvaltningen av lokala och enhetsrelaterade risker.
Dimension	Legal & koncernstrukturer	Operationell (ibland i perpektivet av legal enhet).	Operationell (ibland i perpektivet av legal enhet).	Operationell & legal	Operationell (ibland i perspektivet av legalt bolag eller enhet).
	Externa aktörer			Interna aktörer	

3. Vad gör internrevisionen?

Vad gör internrevisionen?

- Bedömer risker
- Utvärderar kontroller
- Förbättrar verksamheten
- Granskar processer och arbetssätt
- Kommunicerar resultat och rekommendationer

Internrevisorers värde

- Ser vad som fungerar resp. inte fungerar.
- Ser på organisationen objektivt.
- Har ett brett perspektiv på verksamheten.
- Identifierar “red flags”.
- Säger som det är.
- Agera förebyggande i riskhanteringen samt identifiera problem och föreslå förbättringar.
- Bidra till att väsentliga tillgångar skyddas.
- Trygghet för ledning och styrelse.

4. Vad styr internrevisionen?

Internationella regelverk och yrkesstandard
för Internrevision

Internationella regelverk och yrkesstandard

- **I**nternational **P**rofessional **P**ractices **F**ramework (**IPPF**)

  IPPF är yrkesstandards som är formulerade, fastställda och underhållna av IIA.
  IPPF utgör internrevisionsbranschens internationellt accepterade ramverk.
  Indelas i två huvudområden:

  Attribute Standards
  Standarder för egenskaper
  Performance Standards
  Standarder för genomförande

  Det är inte tvingande att följa IPPF men en internrevisionsfunktion som anser sig efterleva IPPF måste verifiera det genom att vart femte år genomgå en oberoende extern kvalitetsbedömning.

Komponenter i IPPF

Internrevisionens uppdrag

Att utveckla och skydda organisato-riska värden genom att tillhandahålla riskbaserad och objektiv försäkran, råd och insikt.

Obligatorisk vägledning

- **Grundprinciper för professionellt utövande av internrevision**
- **Definition of internrevision**
- **Yrkesetisk kod**
- **Internationella standarder för yrkesmässigt utförande av internrevision**

Rekommenderad vägledning

- **Implementerings vägledning**
- **Kompletterande vägledning**

En annan bild av IPPF

Internationella regelverk och yrkesstandard

Yrkescertifieringar för internrevisorer

- **C**ertified **I**nternal **A**uditor (**CIA**)

  IIA:s internationellt accepterade yrkestitel motsvarande auktorisation för externa revisorer. Erhållande av certifieringen kräver en kombination av utbildningsnivå och praktisk yrkeserfarenhet samt specifika teoretiska studier som bekräftas genom att avlägga ett antal prov. Certifieringen måste sedan fortlöpande underhållas genom aktivt yrkesutövande och regelbunden relevant vidareutbildning som årligen intygas till IIA.

  Det finns även andra områdesspecifika certifieringar för internrevisorer som exempelvis:

  CRMA – **C**ertification in **R**isk **M**anagement **A**ssurance

  QIAL – **Q**ualification in **I**nternal **A**udit **L**eadership

  CPEA – **C**ertified **P**rofessional **E**nvironmental **A**uditor

  CPSA – **C**ertified **P**rocess **S**afety **A**uditor

- **C**ertified **I**nformation **S**ystems **A**uditor (**CISA**)

  Certifiering för IT/IS - specialiserade revisorer. Utges och förvaltas av The **I**nformation **S**ystems **A**udit and **C**ontrol **A**ssociation (**ISACA**).

5. Internrevisionens spelplan

Vad är intern styrning och kontroll?

Vad är intern styrning och kontroll?
Innebörden av begreppet ”Internal Control”

Svenska språkets ”Intern styrning” och engelska språkets ”Internal control” betyder samma sak. ”Internal control” syftar således inte enbart på enskilda kontroller utan inbegriper alla komponenter i verksamhetsstyrningen.

Några centrala komponenter: Fastställda strategier och mål, Riskbedömningar, Processer, Styrdokument, Mandat, Process- och systemkontroller, Organisationsstruktur, Kommunikations- och rapporteringsstrukturer, Monitoreringsfunktioner.

Vad är intern styrning och kontroll?
COSO

- COSO (Committee of Sponsoring Organizations of the Treadway Commission) är det globalt sett mest etablerade ramverket för att beskriva och åskådliggöra intern styrning.

- COSO:s definition: "A process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives"

- COSO:s grundläggande internstyrningsmål och dess komponenter:

  Mål: Strategihantering, Operationella verksamheten, Verksamhetsrapportering, Efterlevnad av lagar och regler.

  Komponenter (verksamhetens förutsättningar): Verksamhetens allmänna kontrollmiljö, Riskhantering, Styrnings- och kontrollaktiviteter, Kommunikation, Monitorering

Vad intern styrning och kontroll?
COSO Enterprise Risk Management

COSO Enterprise Risk Management (2016)

"value is maximized when management sets strategy and objectives to strike an optimal balance between growth and return goals and related risks, and efficiently and effectively deploys resources in pursuit of the entity's objectives."

- Verksamhetens effektivitet och ändamålsenlighet
- Tillförlitligheten i finansiell rapportering och
- Efterlevnad av gällande lagar och förordningar"

Vad är intern styrning och kontroll?
Andra etablerade principer och ramverk förutom COSO

- **G**overnance**, R**isk management and **C**ompliance (**GRC**)

  "the integrated collection of capabilities that enable an organization to reliably achieve objectives, address uncertainty and act with integrity.“

- **3 Lines Model**

  Ett generellt sätt att åskådliggöra och beskriva strukturen och de olika rollerna/ansvaren för intern styrning och kontroll inom en organisation.

- **Combined Assurance**

  Syftar till att samordna olika aktörer inom intern styrning och kontroll för att optimera effektivitet och samordning i utvärdering, analys, slutsatser, kommunikation och rapportering.

Ramverk för styrning och kontroll

- **ISO -** International Organization for Standardization

  Exempel : ISO 9001 – Kvalitetscertifiering, ISO 14001 – Miljöcertifiering, ISO 27001 - Informationssäkerhet och CSR 2000:2012 - CSR Certifiering

- **COBIT -** Control Objective for Information and Related Technology Standards (ISACA)

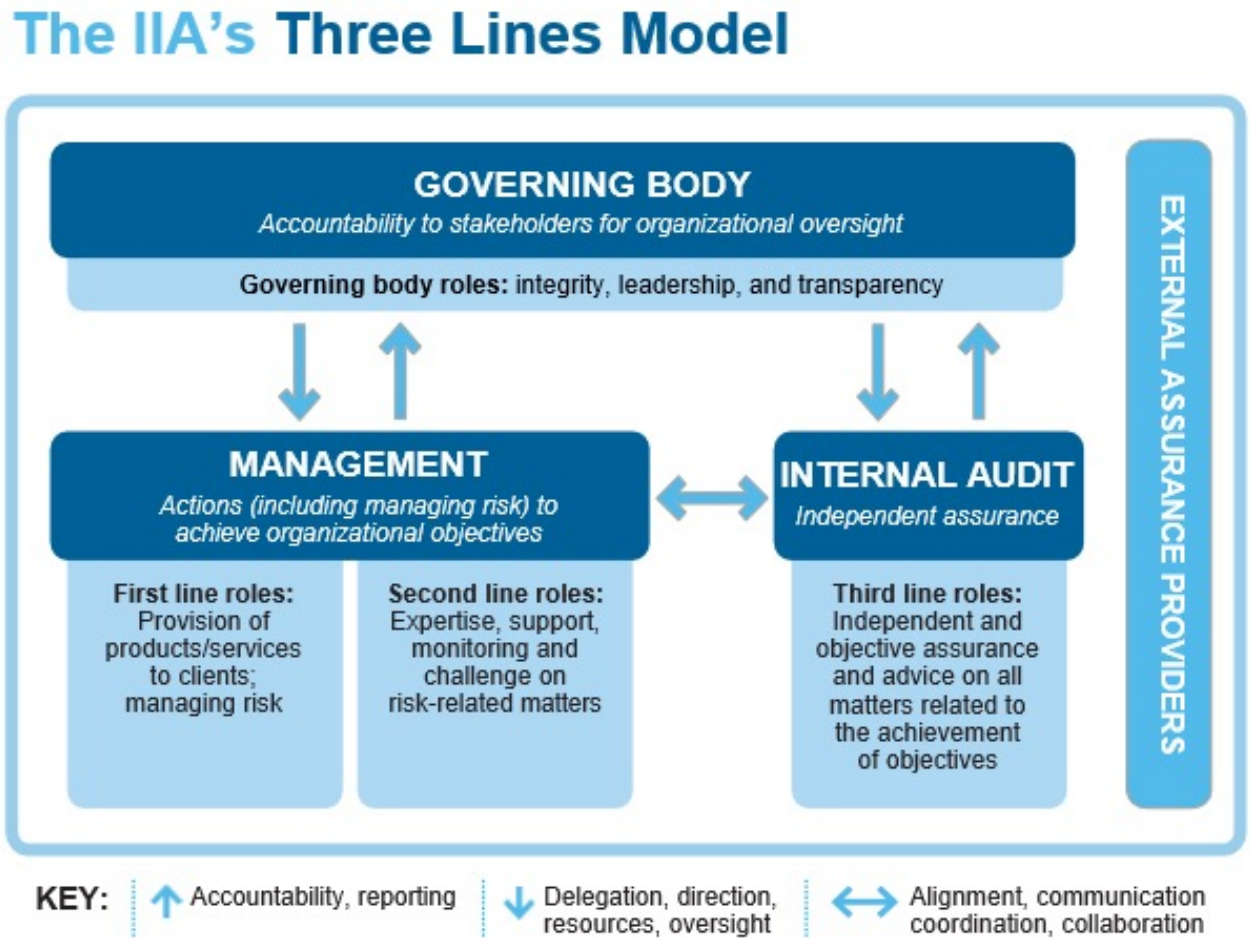
  Ramverk för IT – styrning och ledning med avseende på informationsteknik i relation till affärsrisker och kontrollkrav.

- **Combined Assurance**

  Syftar till att samordna organisationens olika aktörer inom intern styrning och kontroll för att optimera effektivitet och samordning i utvärdering, analys, slutsatser, kommunikation och rapportering.

Vad är intern styrning och kontroll?
De tre ansvarslinjerna

Ansvarsfördelning mellan olika aktörer i organisationen vad avser riskhantering och intern styrning



Vad är intern styrning och kontroll?
Combined Assurance

Parties Involved in the Combined Assurance Framework

With combined assurance, there will be a number of parties involved in providing assurance, and their activities require coordination and alignment.

Huibers, S., CBOK Report *Combined Assurance: One Language, One Voice, One View* (2015). *Source:* adapted from *King Code of Governance for South Africa 2009* (Institute of Directors in Southern Africa) and *Combined Assurance: Case Studies on a Holistic Approach to Organizational Governance* by G. Sarens, Decaux, L., & Lenz, R.

The IIA Research Foundation | CBOK
The Global Internal Audit Common Body of Knowledge

Vad är intern styrning och kontroll?
Organisationens mognadsgrader

Opålitlig	Informell	Standardiserad	Övervakad	Integrerad
• Oförutsägbar miljö där den interna styrningen inte fungerar eller inte existerar	• Intern-styrningen existerar och brukar fungera, men är inte tillräckligt dokumenterad • Stort personberoende	• Intern styrning existerar och är tillräckligt dokumenterad • Avvikelser upptäcks inte eller upptäcks för sent	• Standardiserad miljö som löpande utvärderas i fråga om sin utformning och tillämpning • Ledningen informeras regelbundet	• Integrerad intern styrning som övervakas i realtid av ledningen • Ständiga förbättringar införs fortlöpande

6. Revisionsprocessen

Revisionsprocessen

Riskanalys

- Övergripande riskanalys
- Kategorisering och klassificering av identifierade risker
- Bedömning av identifierade risker gentemot verksamhetens strategiska mål
- Prioritering av vilka risker som ska ligga till grund för revisionsaktiviteter

Revisionsplan

- Upprättande av förslag till revisionsplan baserat på riskanalysen
- Godkännande av revisionsplan

Genomförande av revisioner

- Förberedande analyser/ Öppningsmöte/ Revision/ Slutrevisionsmöte/ Resultatanalyser ”root cause”/ Kommentarer och åtgärdsförslag från representanter för den reviderade verksamheten.

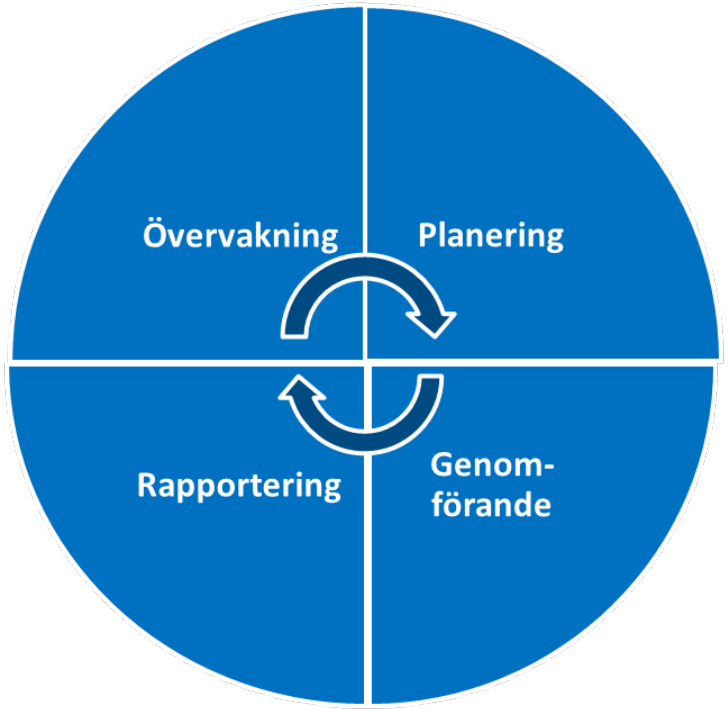
Rapportering

- Skriftlig och muntlig gentemot uppdragsgivare och relevanta representanter för den reviderade verksamheten.

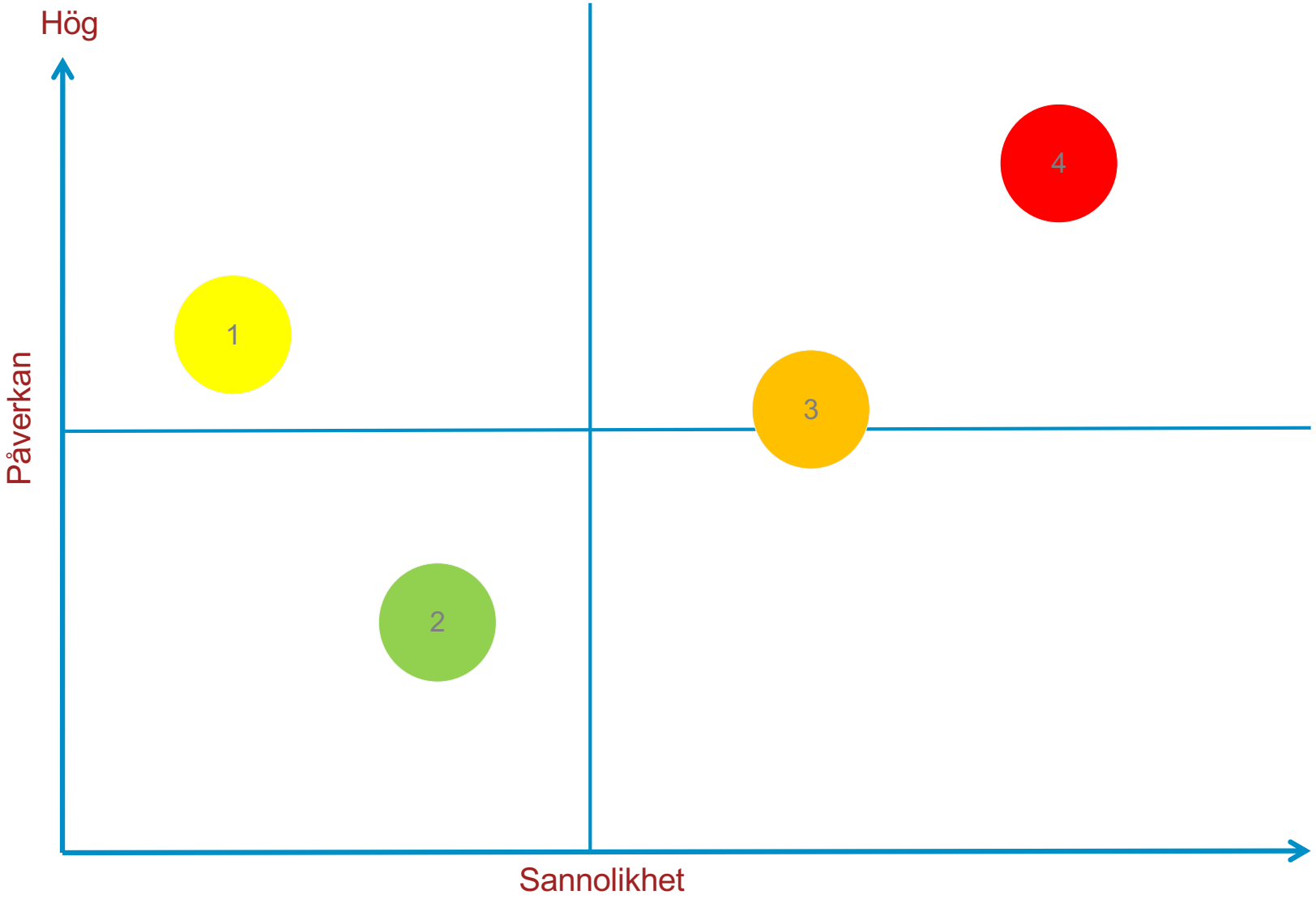
Uppföljning

- Monitorering av genomförandet av överenskomna och beslutade åtgärder i dialog med verksamheten.

Revisionsprocessen

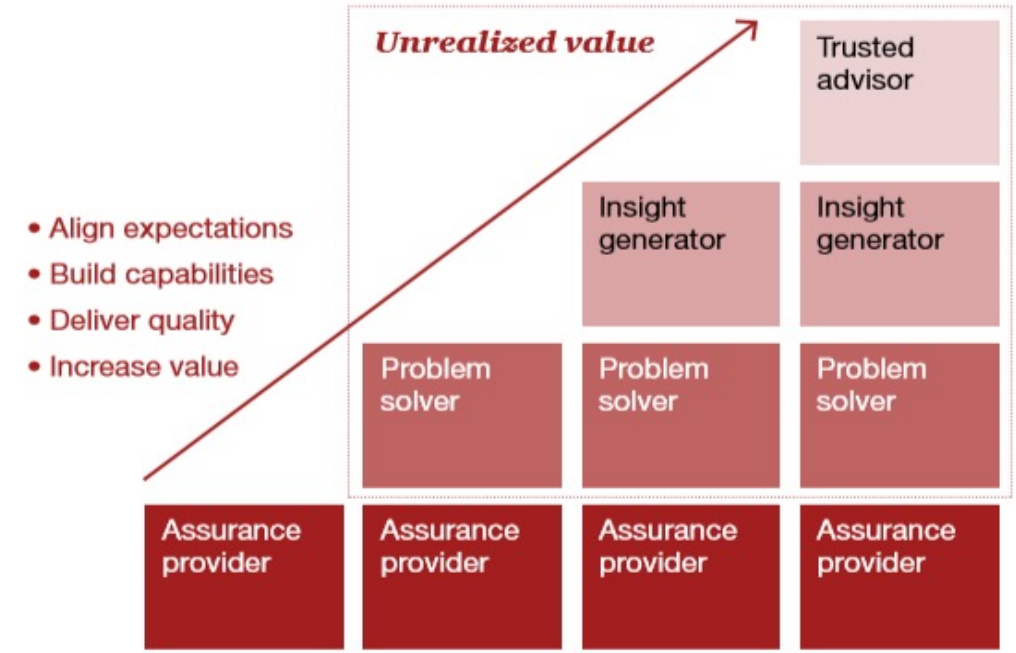


Klassificering av identifierade risker



7. Internrevisionens värdeskapande roll

Internrevisionens värdeskapande roll



Providing value-added services and proactive strategic advice to the business well beyond the effective and efficient execution of the audit plan

Taking a more proactive role in suggesting meaningful improvements and risk assurance

Bringing analysis and perspective on root causes of issues identified in audit findings to help the business take corrective action

Delivering objective assurance of the effectiveness of an organization's internal controls

Source: 2014 PwC State of the Internal Audit Profession Study

Internrevisionens värdeskapande roll

Internrevisionen kan:

- genom sin position utgöra en rapporteringsmässigt oberoende och organisatoriskt objektiv informationskälla
- genom revisioner och andra bedömningar vara validerande/**assurance**
- vara en objektiv och betrodd rådgivare /**consultancy**
- bidra med både övergripande och specifika insikter som strategiskt och operationellt har betydelse för framtiden
- generellt bistå verksamheten i egenskap av ”Trusted advisor”

8. Specifika regelverk per sektor

Specifika regelverk per sektor

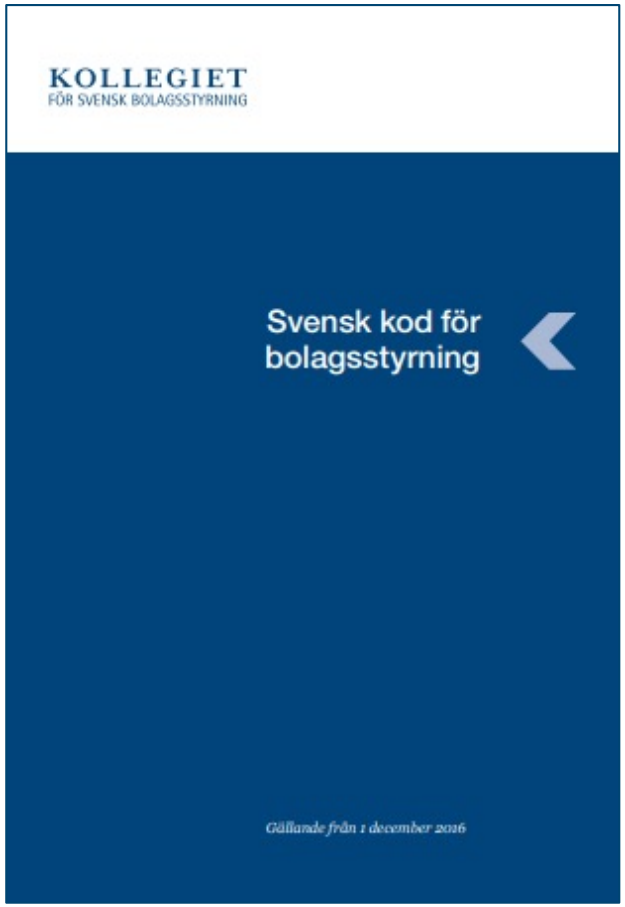
- Offentlig sektor
- Privat sektor
- Finansiell sektor
- Myndigheter som reglerar finansiella företag

Specifika regelverk per sektor
Offentlig sektor

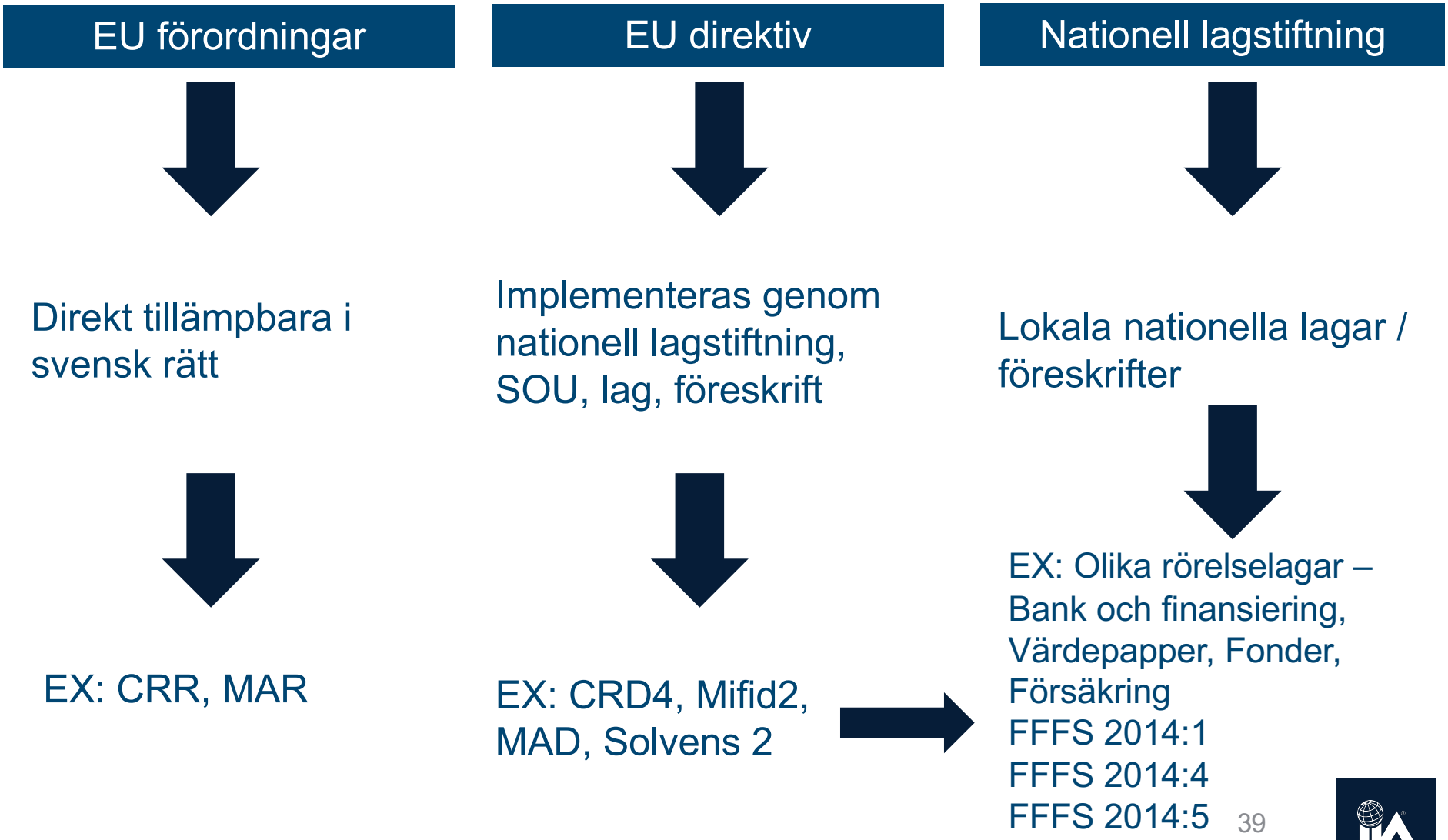
- Myndighetsförordningen (2007:515)
- Internrevisionsförordningen (2006:1228)
  - Fastställer vilka myndigheter som ska ha internrevision
- Förordning om intern styrning och kontroll (2007:603)
- Ekonomistyrningsverket har samordningsansvar för internrevisionen i staten
- Inom staten har vi dessutom den statliga värdegrunden och statstjänstemannarollen att ta hänsyn till.

Specifika regelverk per sektor
Privat sektor: Svensk kod för bolagsstyrning

- Koden är ett led i näringslivets självreglering (följ eller förklara) för att främja god bolags-styrningen i svenska börsnoterade bolag
  - att säkerställa att bolag sköts hållbart, ansvarsfullt och så effektivt som möjligt
- Vad innebär god bolagsstyrning?
  - bolagen drivs med sina ägares intresse som ledstjärna.
  - främja förtroendet för bolagen hos allmänheten och den svenska och internationellt kapitalmarknaden,
  - vilket i sin tur skapar bättre förutsättningar för det svenska näringslivets kapitalförsörjning.



Specifika regelverk per sektor
Finansiell sektor - Övergripande regelverkskarta



Specifika regelverk per sektor
Myndigheter som reglerar finansiella företag

EUROPEISKA MYNDIGHETER

- EBA - Bank
- ESMA – Värdepapper och marknadsuppförande
- EIOPA - Försäkring
- ESRB - Makrotillsyn

SVENSKA MYNDIGHETER

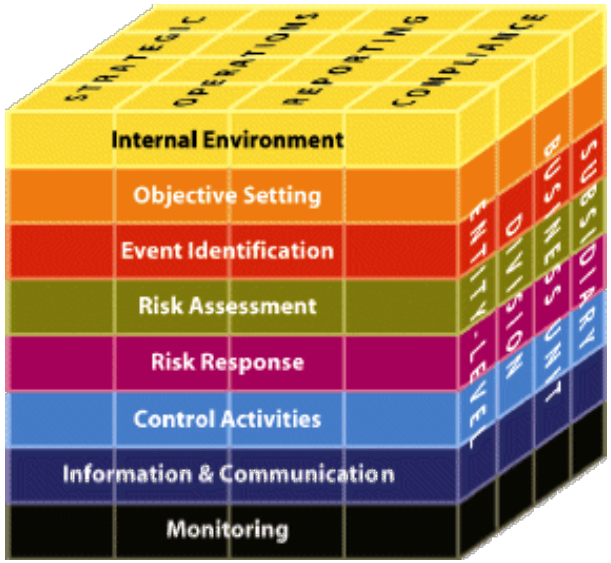
- Finansinspektionen (FI)
- Riksbanken
- Riksgälden

Appendix
Alternativa bilder per område

1. **Vad är internrevisionens uppdrag**
2. **Vad är internrevision**
3. **Vad gör internrevisionen**
4. **Vad styr internrevisionen**
5. **Internrevisionens spelplan** - vad är intern styrning och kontroll?
6. **Revisionsprocessen** – hur bedriver internrevisionen sitt arbete?
7. **Internrevisionens värdeskapande roll**
8. **Specifika regelverk per sektor** – privata och offentliga verksamheter

Appendix
Alternativa bilder per område

5. Internrevisionens spelplan - vad är intern styrning och kontroll?


STRATEGIC
OPERATIONS
REPORTING
COMPLIANCE
Internal Environment
Objective Setting
Event Identification
Risk Assessment
Risk Response
Control Activities
Information & Communication
Monitoring

COBIT

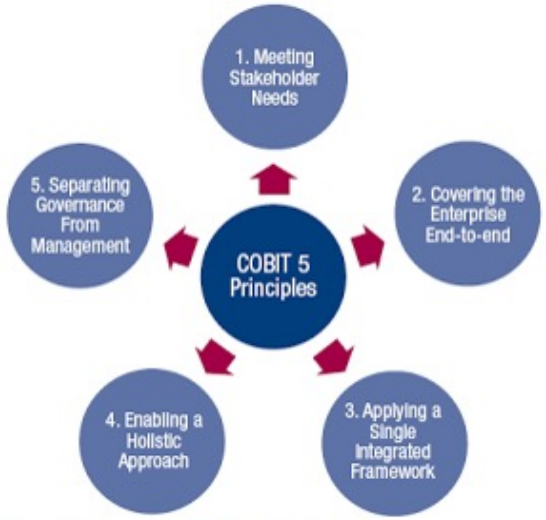
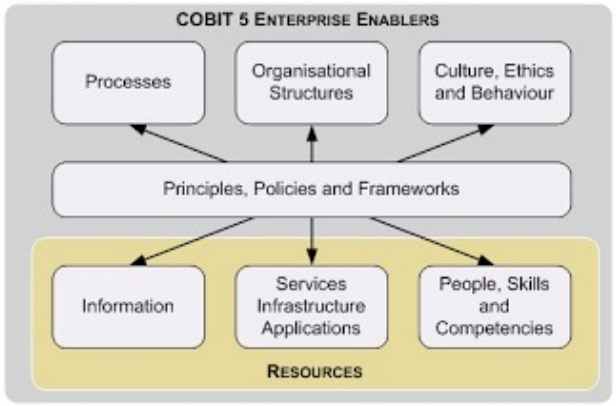


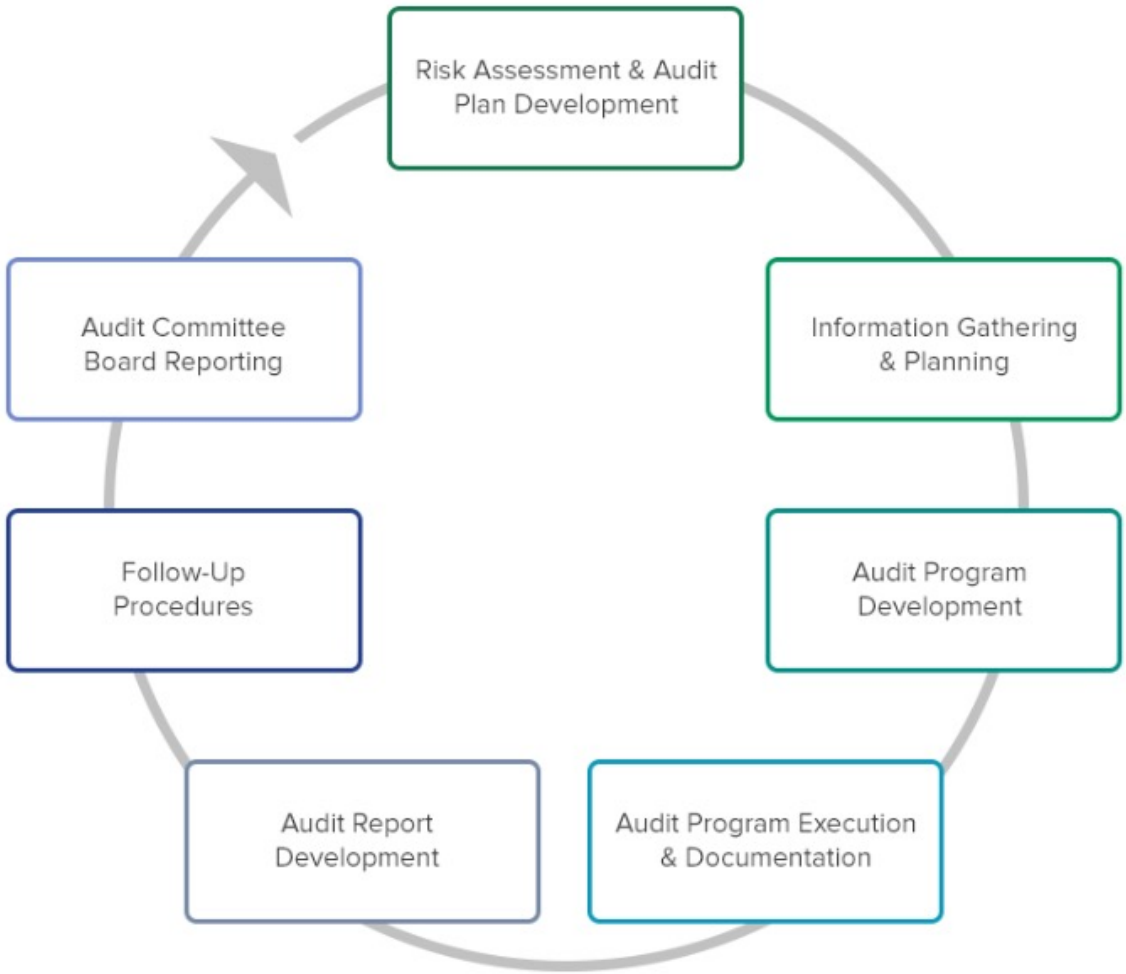
Figure 1: The COBIT 5 Principles



Source: www.vanhaaren.net

Appendix
Alternativa bilder per område

6. Revisionsprocessen – hur bedriver internrevisionen sitt arbete?


Risk Assessment & Audit Plan Development
Information Gathering & Planning
Audit Program Development
Audit Program Execution & Documentation
Audit Report Development
Follow-Up Procedures
Audit Committee Board Reporting