Sikkerhed og Revision

# 3 Lines of Defence

5. September
2019

Kim Stormly Hansen

# Præsentation

1. Statsautoriseret revisor, CISA
2. Medlem af det rådgivende revisionsudvalg i:
   - BEC
   - Nets
   - Finanstilsynet
3. Ekstern lektor, CBS
4. Medlem af FSRs Cypersikkerhedsudvalg
5. Ansvarlig for revision af IT og Governance i Nykredit

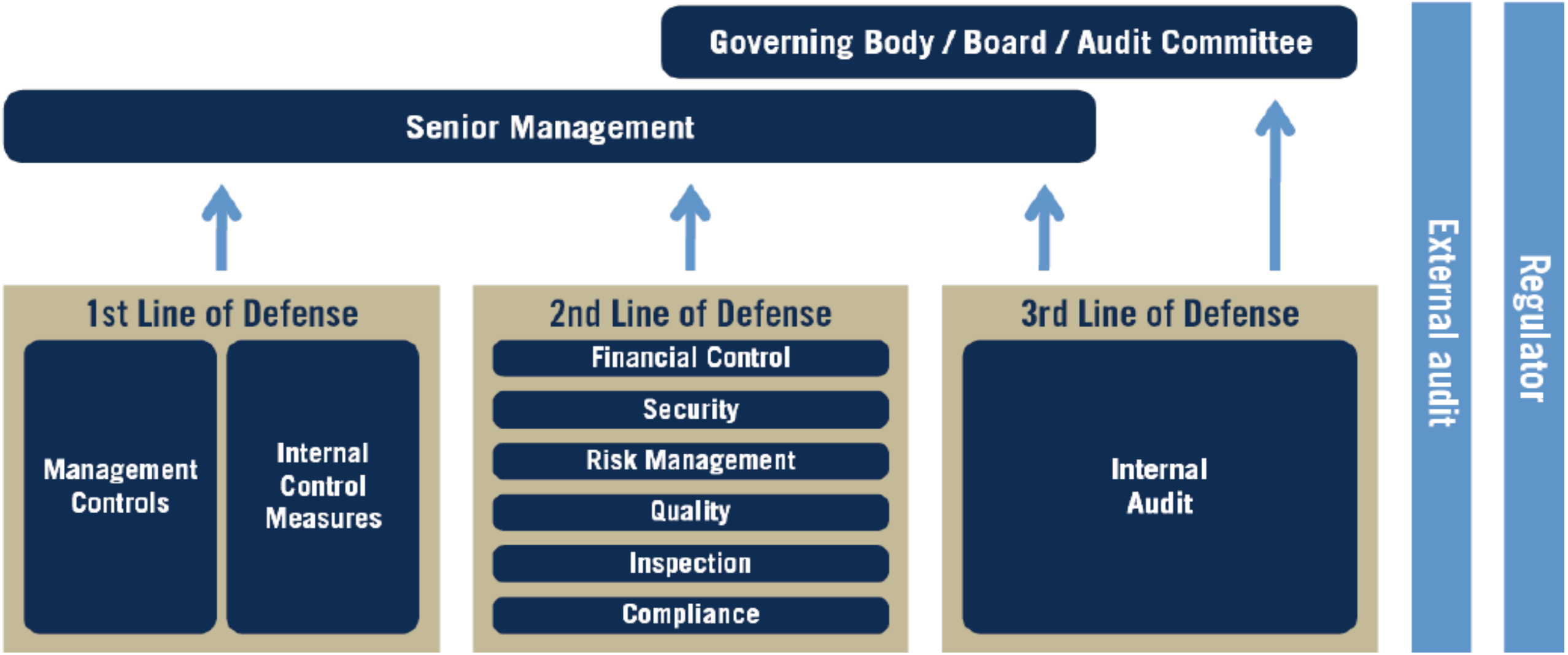
# Agenda

- Hvorfor skal vi tale om 3LOD?
- 1st Line, 2nd og 3rd Line, udfordringer
- Udfordringer på tværs af 1st og 2nd Line, 2nd og 3rd Line, 3rd og 4th Line og 3rd og 5th Line
- Forslag til løsninger
- 3LOD i relation til IT-outsourcing
- IIA Exposure Document

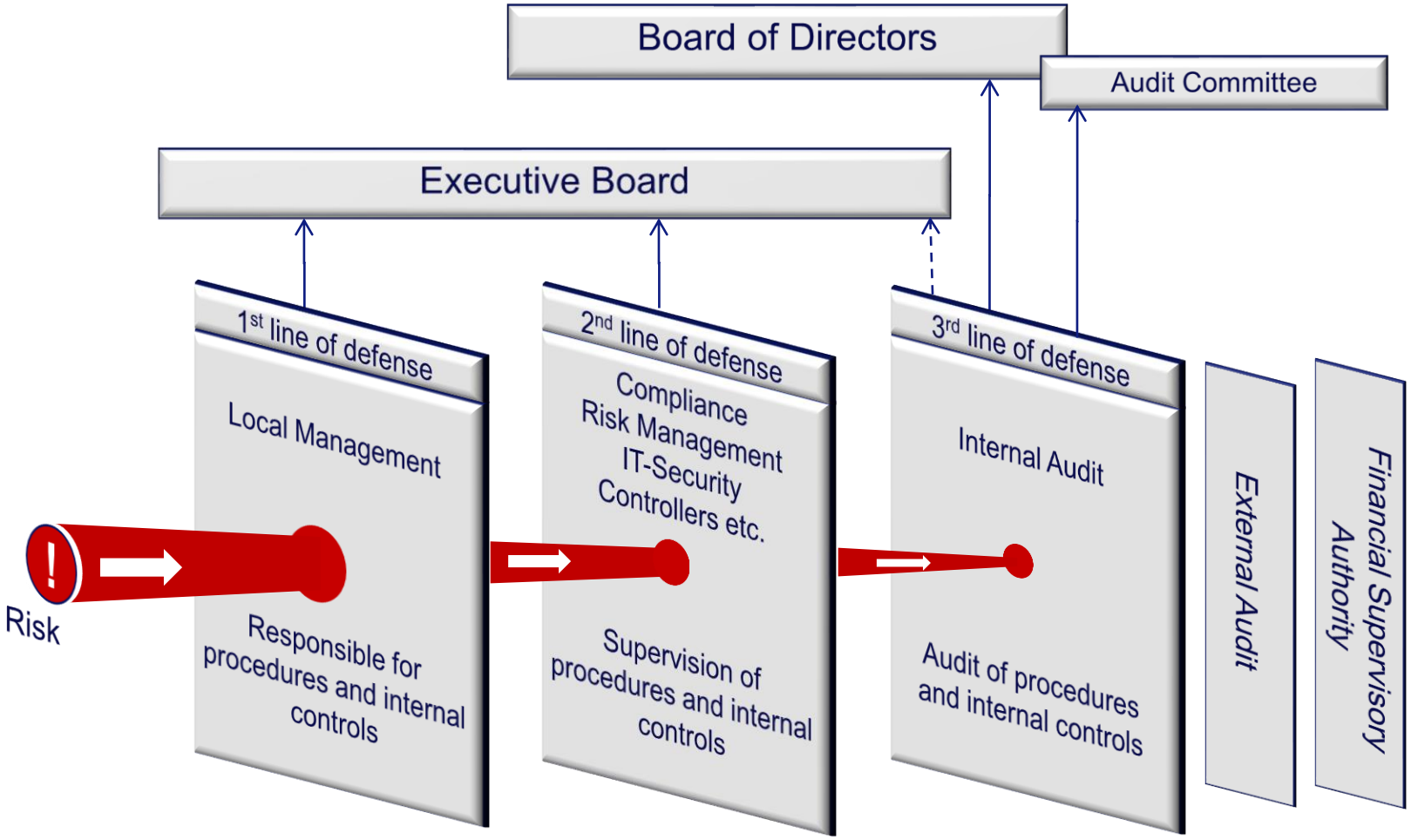
# Hvorfor skal vi tale om 3LOD – Modellen er jo 20 år gammel!!!

Within the basic model, there is plenty of scope for flexibility and choice. How to assign, separate, and combine roles must be a decision that the governing bodies of each organization make, taking full account of stakeholder desires and direction as well as regulatory expectations and legal requirements.

# The Three Lines of Defense Model



# Three Lines of Defense Model



# 1st Line, udfordringer

- Har ikke forstået deres rolle og det ansvar der ligger heri
- Kultur
  - Outsourcing
  - Produktion ctr. kontrol
  - Bekvemmelighed ctr. sikkerhed
- Forståelse af risiko, herunder risikoappetit, iboende risiko, mitigering og restrisiko
- Manglende overblik over risiko og mitigerende tiltag, herunder kontroller

# 2nd Line, udfordringer

- Definition
- Sammenblanding af 1st og 2nd line opgaver
- Manglende / utilstrækkelig regulering, retningslinjer og vejledninger
- Compliance
  - Fortolkning af virkefelt og behandlingsdybde
  - Arbejdsmetoder
  - Finanstilsynet
  - 2½LOD
- Forståelse af risiko, herunder risikoappetit, iboende risiko, mitigering og restrisiko
- Manglende fælles taxonomi, samarbejde / koordinering og rapportering
- Manglende fokus på rådgivning og undervisning

# 3rd Line, udfordringer

- Italesættelse af forskel til 2nd Line enheder
- EBA
- Samarbejdsmodel med ekstern revision

# Udfordringer på tværs af linjerne

- 2nd og 3rd (Compliance) – IR light
- 3rd og 4th – Samarbejdsmodel
- 3rd og 5th – Revisionsvirksomhed ctr. Tilsynsvirksomhed
- 4th og 5th – Forventningskløft (AML)

# Udfordringer på tværs af linjerne

- 2nd og 3rd (Compliance) – IR light
- 3rd og 4th – samarbejdsmodel
- 3rd og 5th – Revisionsvirksomhed ctr. Tilsynsvirksomhed
- 4th og 5th – Forventningskløft (AML)

# Forslag til løsninger

- Information og test (1st line)
- Governance eftersyn (1½ line)
- Retningslinjer og holdningsændring, Finanstilsynet
- End to end GRC proces, herunder systemunderstøttelse
- Assurancemapping og integrated assurance and reporting?

# 3LOD irt. IT

- Kan 3LOD anvendes irt. outsourcing?
  - Ja, men hvem gør hvad?
  - 1st – 1st, 2nd - 2nd, 3rd – 3rd
  - Er intern systemrevision 2nd eller 2½?
- Finanstilsynspåbud
- Risikovurdering
- Egenkontrol ctr. erklæring
- ISAE 3402
  - Regnskab ctr. System-, Data- og Driftssikkerhed
  - Carve out ctr. Inclusive
  - SOC?
- Integrated reporting
  - Eksempel
- EBA retningslinjer

# Vurdering af delområder

Nedenfor har vi anført vores vurdering af det interne kontrolsystem for hvert delområde, der er berørt af revisionen, samt kort beskrevet de områder, hvor procedurer og kontroller kan forbedres. En beskrivelse af anvendte måleskalaer fremgår af bilag 1.

| Delområde | | Vurdering – interne kontrolsystem | Svagheder som kan henføres til Datacentral | Svagheder som kan henføres til Compliance-rapport | Observationer, Intern revision |
|---|---|---|---|---|---|
| **Sikkerhedskrav til informations-systemer** |  | Tilfredsstillende | 1. Ingen forhold | 1. Ingen forhold | 1. Ingen observationer |
| **Sikkerhed i udviklings- og hjælpe-processer** |  | Tilfredsstillende, men med svaghedstegn | 1. Manglende xxxxxxxxxx – *Deadline maj 2019* | 1. Manglende xxxx – *Løst* | **1. Procedure for xxx (Høj risiko):** Manglende xxxxx |

# IIA Exposure document

- Beyond value protection to embrace value creation
- Blurring the lines
- The objective of the working group is the creation of a fit-for-purpose model that is adaptive enough to apply to the wide variety of organizational models and the rapidly changing environments in which they operate. To this end, dynamic governance, risk management, and control processes are required with coordination, collaboration, and alignment across the model being of vital importance.
- The aim of this review is to enable those charged with governance to draw from the Three Lines of Defense model to help them deploy the most appropriate structure and resources within their organizations to preserve and enhance value.

| Strengths of the Three Lines of Defense Model | Opportunities for Development |
| --- | --- |
| Is simple, easy to understand, and easy to communicate. | To maintain these qualities. |
| Provides focus on the importance of effective risk management and control. | To contextualize risk management and control as part of governance, supporting organizational success and value creation. |
| Supports an organization's efforts in responding to opportunities and threats. | To encourage both a proactive and a reactive approach to advancing the goals of an organization. |
| Offers a basis for clarity and efficiency when organizing the activities and resources of risk management and control. | To emphasize the importance of coordination and collaboration aligned to strategic priorities and operational needs. |
| Describes the roles played by each of the key functions and relevant external stakeholders with respect to risk management and control. | To provide additional clarity to the roles and responsibilities of individual functions and to their joint contribution to governance, organizational success, and value creation. |

| Strengths of the Three Lines of Defense Model | Opportunities for Development |
| --- | --- |
| Describes a means of structuring key functions. | To highlight the opportunities for a more flexible and agile adoption of the model. |
| Has been widely adopted, especially by organizations and regulators in financial services. | To take account of organizational differences, especially with respect to size, sector, and maturity; demonstrate relevance; and enable ready adoption by any organization. |
| Recognizes the roles of external auditors and regulators in risk management and control. | To consider other external stakeholders and their contribution to governance, organizational success, and value creation without over-complicating the model. |
| Allows for a ready explanation of the role of internal audit as the "third line of defense." | To expand this description to embrace the role of internal audit as a strategic partner and trusted advisor. |

| Strengths of the Three Lines of Defense Model | Opportunities for Development |
| --- | --- |
| Allows for a ready explanation of the role of internal audit as the "third line of defense." | To expand this description to embrace the role of internal audit as a strategic partner and trusted advisor. |
| Provides a useful framework for discussions about independence, objectivity, and assurance. | To account for and explain "blurring of the lines" and describe appropriate safeguards. |
| Is illustrated by a well-known and simple graphic. | To evolve the graphical representation to reflect evolution and enhancement of the model itself. |

# GRC and Integreting

Regular communication is often the key to effective coordination. Greater integration can also be fostered by:

- Ensuring individual, team, and departmental goals are aligned with the strategic priorities and operational needs of the organization.
- Ensuring a common understanding of the purpose and roles of each part of the organization.
- Establishing a common vocabulary for describing aspects of governance, risk management, and control.
- Using common rating or measurement systems across all functions.
- Sharing resources, including subject matter experts, among functions.
- Leveraging data and technology to facilitate insight capture, analysis, and communication.

Internal audit can play an important role in leading efforts toward a more integrated approach. This includes assurance mapping

# Blurring the lines - IA role

- The Internal audit function can deliver a mix of assurance and nonassurance services according to the needs of the organization. Advisory and other nonassurance services may include:
- • Agreeing management decisions.
- • Making recommendations.
- • Consulting on current circumstances and future actions.
- • Participating in change initiatives.
- • Delivering training in risk-related topics.
- • Leading control self-assessment sessions with management.
- • Assuming managerial responsibilities from time to time.