Internal Control: A COSO framework

Professor Dr. Anatoli Bourmistrov

Nord University Business School, Bodø (Norway)

anatoli.bourmistrov@nord.no

November 28th 2017

Kyiv

Why IC seminar? (1)

- Corruption scandals and increasing pressure on listed companies to improve their internal control
- In Norway, series of scandals with stated owned enterprises
- The Norwegian state and reputation risk
- MFA requirement to international development projects

Why IC seminar? (2)

- September 2016: anti-corruption Conference “Universities of Ukraine as subjects of anti- corruption activities of the state” in Kyiv
- Lunch the idea of an online competence improvement course connected to anti-corruption
- Project CPEA-ST/10022 (2017 – 2019) “Internal Control and the COSO framework: Application to the university sector in Ukraine”
  - Joint application with Taras Shevchenko National University of Kyiv, Ternopil National Economic University and Yuriy Fedkovych Chernivtsi National University
- Seminar gives us opportunity to test ideas

Objectives of the seminar

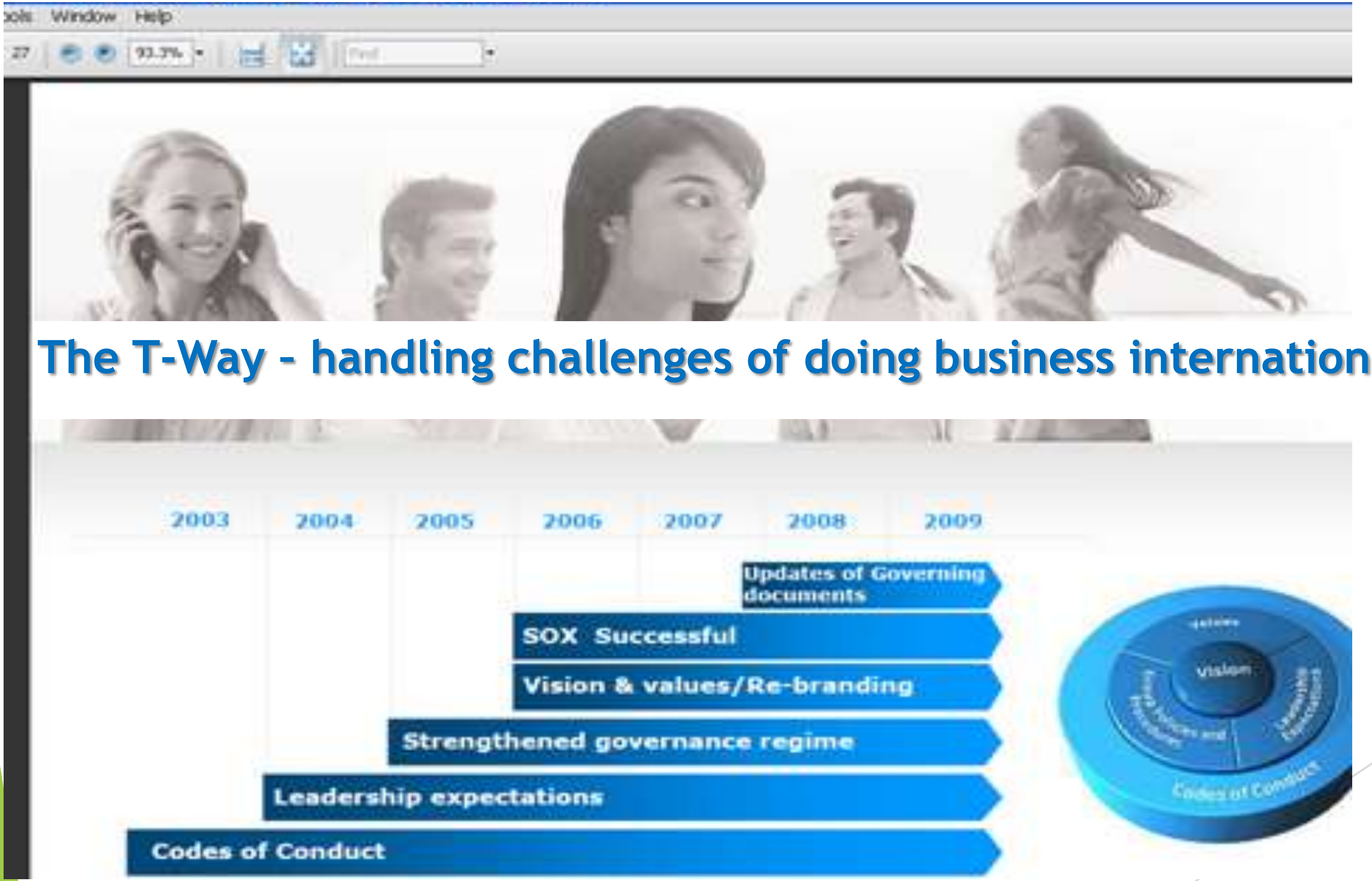
- The learn about the COSO framework for internal control
- To apply two components of the framework, i.e. Control Environment and Risk Management, to access the status in own organizations
- To use this knowledge to develop a strategic plan for how to improve internal control in own organizations

A preamble

A short story of internationalization: A Norwegian MNC «T»

- T is a telecommunication state owned and controlled company (state owns 54% of shares)
- Established in 1855 as a state operated monopoly/agency for telegraphy
- 1993 - started internationalization activities by investing in North-West Russia and expanding to other countries
- 1998 - T invested in an international company VIP (25%) and with years expanded its position to 33% of shares (43% of votes in BoD)
- 1999 - Consolidation of “the planted flags” into an international portfolio with a clear strategy
- 2004 – Different companies - one group

The T-Way – handling challenges of doing business internationally



2003 2004 2005 2006 2007 2008 2009

Updates of Governing documents

SOX Successful

Vision & values/Re-branding

Strengthened governance regime

Leadership expectations

Codes of Conduct

The corruption scandal unveils

- 2012: the Swedish journalists investigation claims that VIP has a case of corruption in a country X-stan
- 2013: VIP is under investigation in USA and Netherlands
- 2014: The Minister of trade and communication discuss the situation with the Chairman of the Board and CEO
- Media in Norway digs deeper and finds the facts that T's executives were informed about the payments

The consequence: a vicious circle?

- 2015: The Norwegian parliament hearings – the CEO denies any knowledge
- The Minister dismiss the Chairman of the Board
- 2016: Norwegian authority arrested the former CEO of VIP
- VIP formally admits the corruption in X-stan and pays a gigantic penalty of 7 billion NOK
- 2016 – 2017: T totally divest from VIP
- …

The case illustrates

- SOE and huge reputational risk (for the public/central government)
- How to achieve influence when you don’t have financial control?
- International cooperation with emerging markets
  - New opportunities but also new types of risks?
- Individual(s responsibility) vs. (internal control) system
- Design vs. real functioning of the internal control
- The significant role of the top managers to prevent the fraud/corruption by designing and implementing well-functioning system
- Significant economic consequences having “skeletons falling out of the closet”
  - Importance do it right from the first time?

The brief history of COSO framework

Why internal control frameworks on «the rise»?

- Initial definitions of internal control focused mostly on perspectives of financial reporting
- Definition was a subject to changes in 70s and 80s due to increasing number of fraud and corporate failures
- 1977: the Foreign Corrupt Practices Act (FCPA) was important
  - Held managers responsible for having and maintaining internal control system
  - Encouraged managers to start thinking about internal control system (even though no standards existed)
- Still many US enterprise failures
- 1985: Formation of the National Commission on Fraudulent Financial Reporting (so called the Treadway Committee)
- 2004: the Sarbanes-Oxley Act (SOX)

The lessons from Enron

DON'T FEED THE ACCOUNTANTS

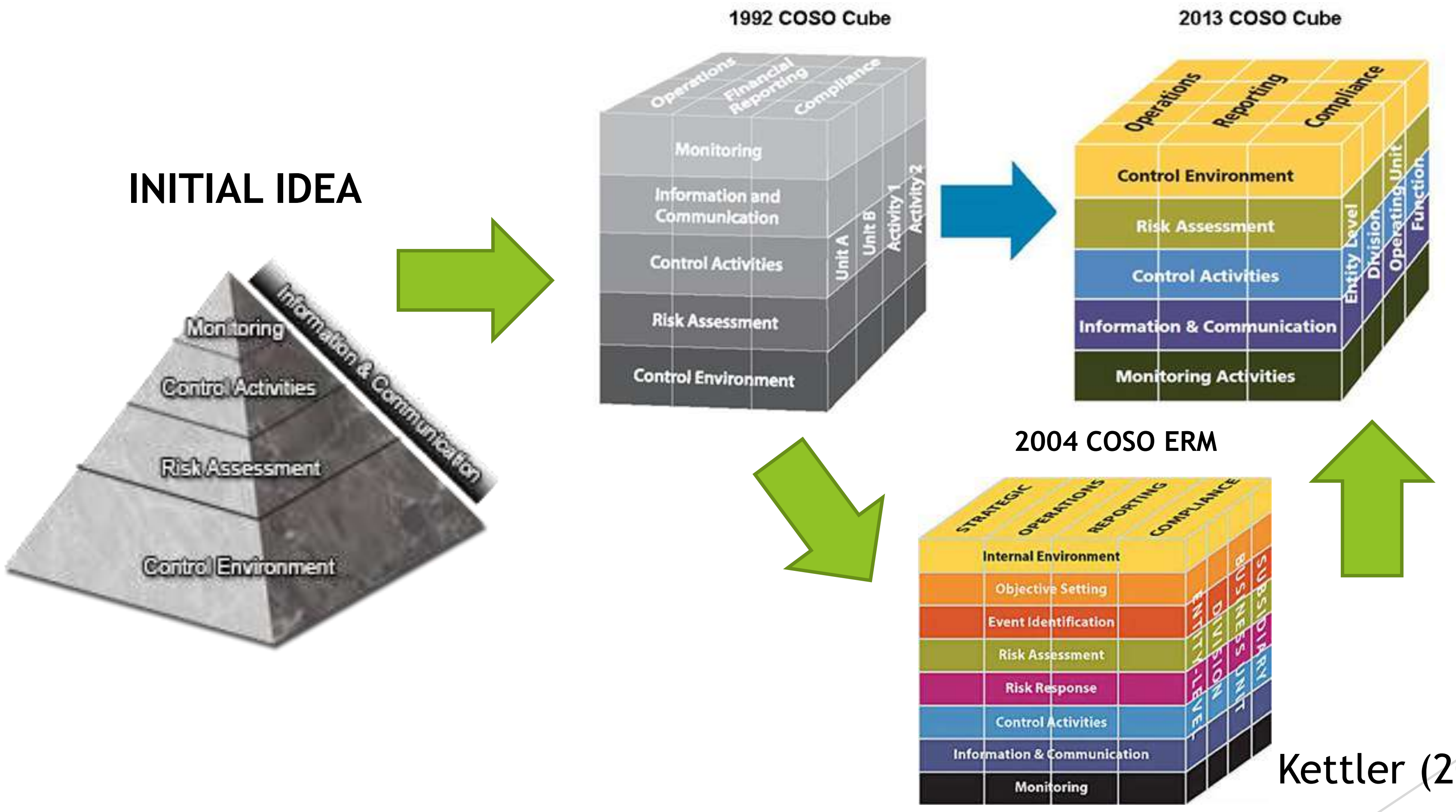
Developments in Norway

- Changes in the Norwegian central government
  - The need to strengthen internal control was emphasized already in 2003
  - Responsibility of the Directorate for the State Management Control (DSØ)
  - Mapping the need for compulsory internal audit based on OECD recommendations (Value fro Money in Government, 2013)
    - ✓ All state organizations with the income of more then NOK 300 mill should access whether they need to use systems of internal audit (May 1st 2016)
    - ✓ Criteria:
      - Complexity and size
      - Risks and materiality
      - Quality of management and control
  - Importance of securing internal auditors' independence

What is a COSO and COSO framework?

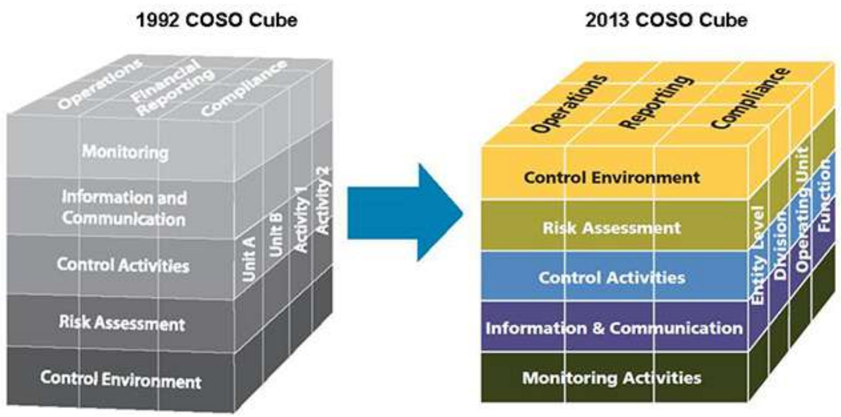
- COSO = the Committee of Sponsoring Organizations
  - Established in 1985 to sponsor the National Commission on Fraudulent Financial Reporting
  - 5 sponsors: AAA, AICPA, FEI, IIA, IMA
  - “COSO’s mission is to provide though leadership through the development of comprehensive frameworks and guidance on enterprise risk management, internal control, and fraud deterrence designed to improve organizational performance and governance to reduce the extent of fraud in organizations” (2008)
  - Created and filled demand for risk management framework: risk could be managed!

THE COSO FRAMEWORK: EVOLUTION - NO REVOLUTION



Kettler (2014)

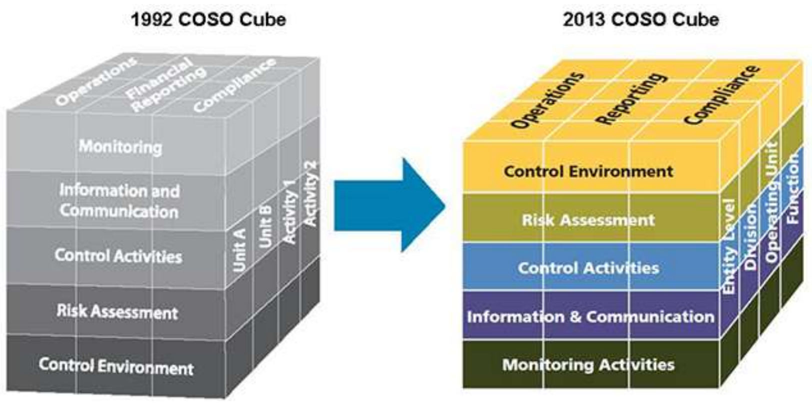
Main similarities between 1992 and 2013 COSO frameworks



- Not changed:
  - Core definition of internal control is the same:
    - ✓ "Internal control is a process, effected by an entity's board of directors, management, and other personnel, designed to provide *reasonable assurance* regarding the *achievements of objectives* relating to *operations, reporting, and compliance*"
  - Three dimensional cube
  - Criteria to assess the effectiveness of an internal control system
  - The exercise of judgement is still important

(Protiviti, 2014; Kettler, 2014)

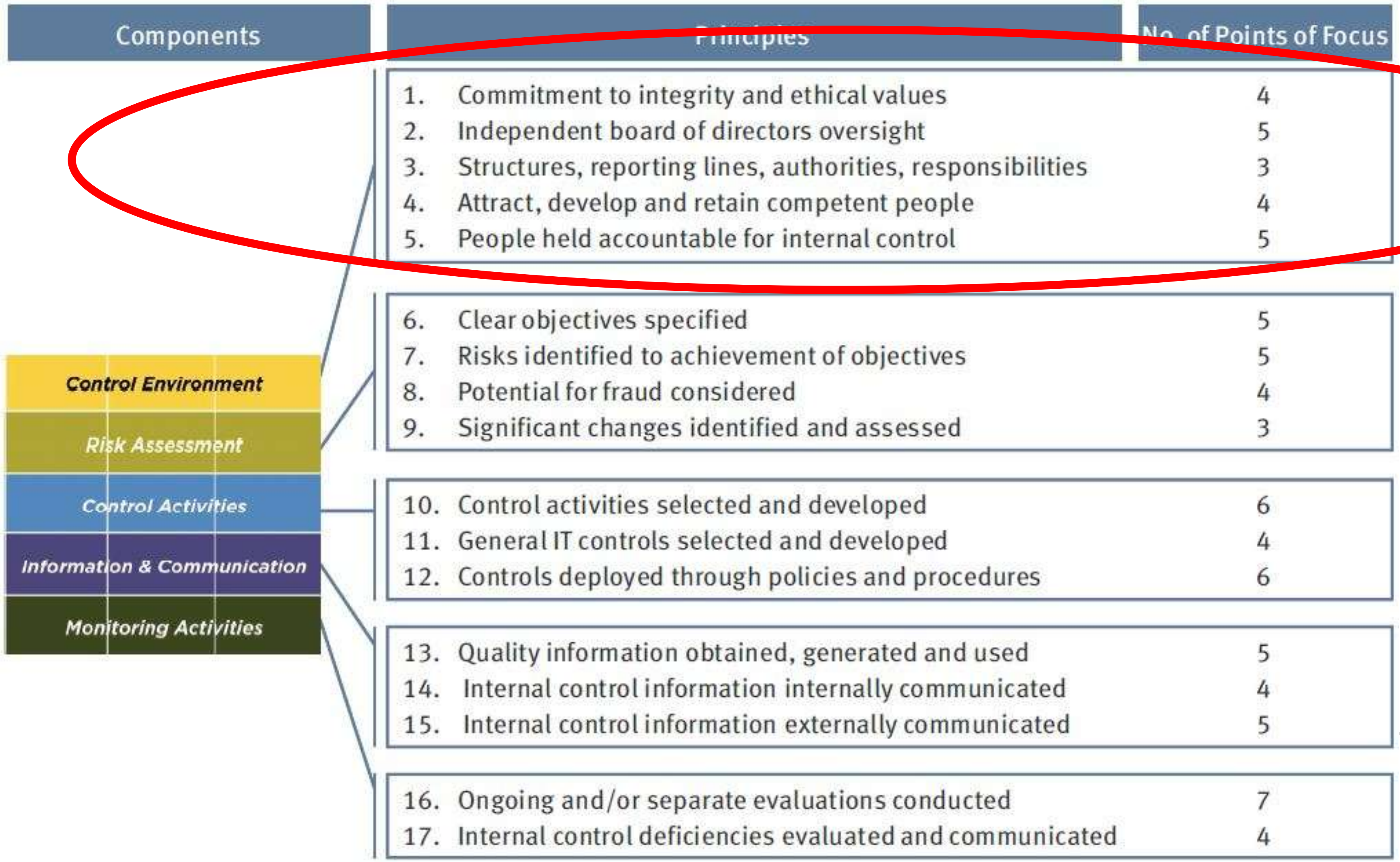
Main differences between 1992 and 2013 COSO frameworks



- New elements in COSO 2013:
  - Flipping the side – the Control Environment on the top
  - 17 explicit principles are codified to support the five elements of internal control system
  - 77 points of focus are developed to represent characteristics of principles
  - Expanding reporting categories
  - More attention to importance of technology
  - An enhanced discussion of governance concept

(Protiviti, 2014)

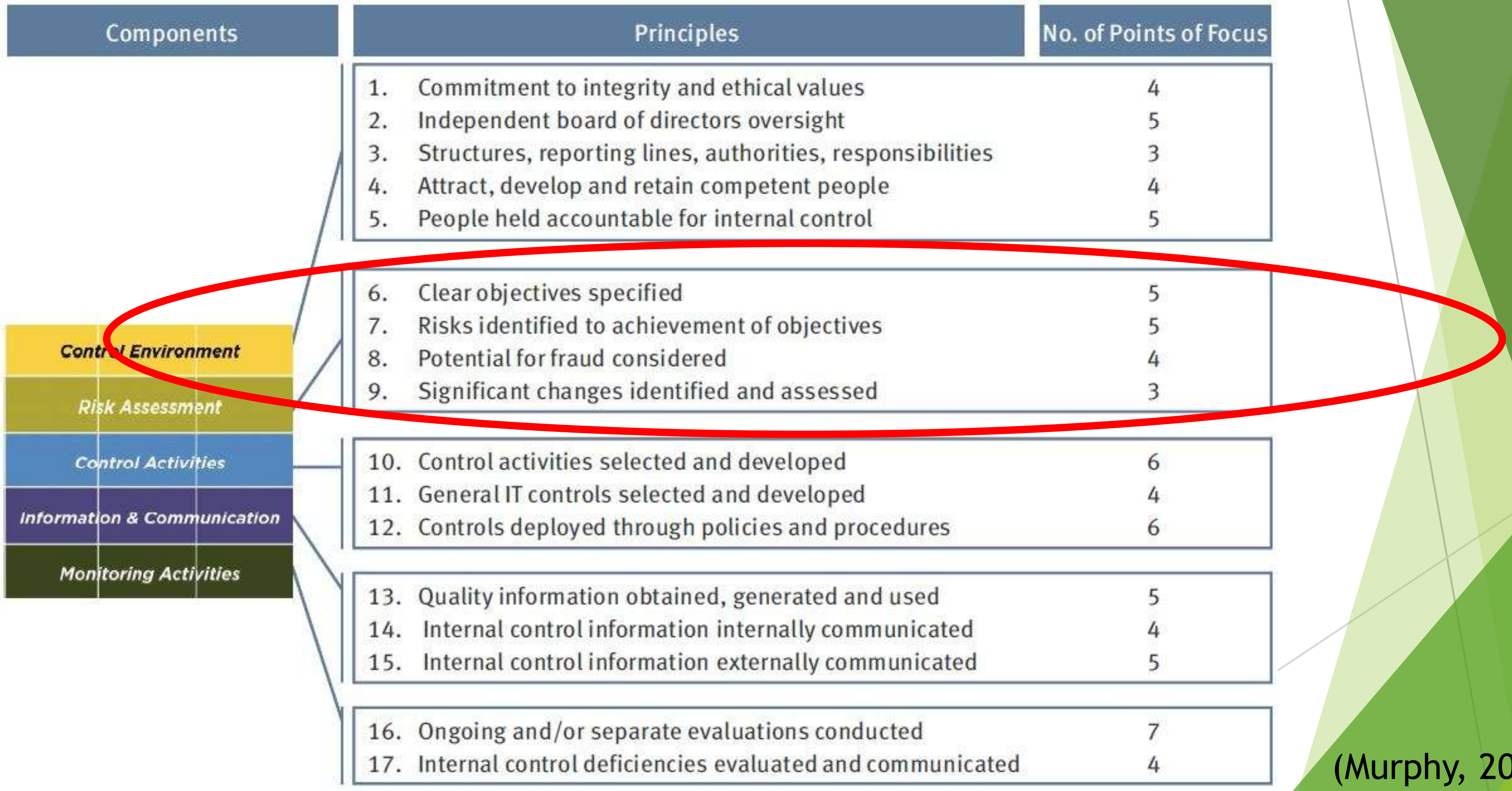
Principles: Control Environment



Components	Principles	No. of Points of Focus
Control Environment	1. Commitment to integrity and ethical values	4
	2. Independent board of directors oversight	5
	3. Structures, reporting lines, authorities, responsibilities	3
	4. Attract, develop and retain competent people	4
	5. People held accountable for internal control	5
Risk Assessment	6. Clear objectives specified	5
	7. Risks identified to achievement of objectives	5
	8. Potential for fraud considered	4
	9. Significant changes identified and assessed	3
Control Activities	10. Control activities selected and developed	6
	11. General IT controls selected and developed	4
	12. Controls deployed through policies and procedures	6
Information & Communication	13. Quality information obtained, generated and used	5
	14. Internal control information internally communicated	4
	15. Internal control information externally communicated	5
Monitoring Activities	16. Ongoing and/or separate evaluations conducted	7
	17. Internal control deficiencies evaluated and communicated	4

(Murphy, 2014)

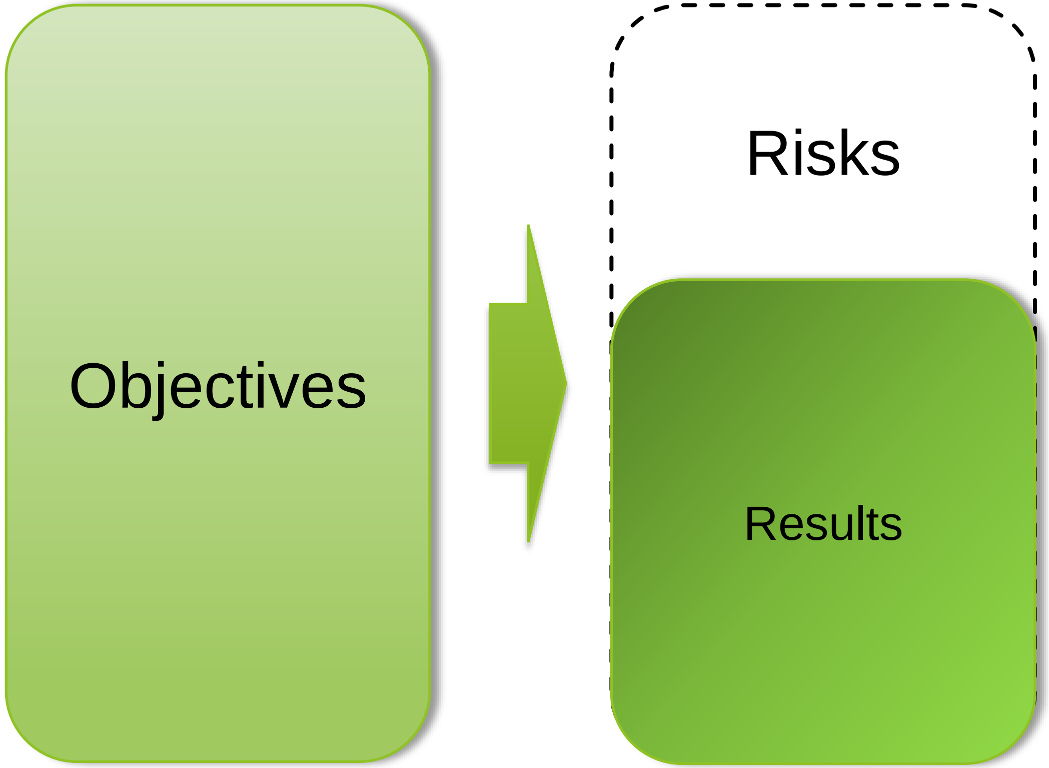
Principles: Risk Assessment



Components	Principles	No. of Points of Focus
Control Environment	1. Commitment to integrity and ethical values	4
	2. Independent board of directors oversight	5
	3. Structures, reporting lines, authorities, responsibilities	3
	4. Attract, develop and retain competent people	4
	5. People held accountable for internal control	5
Risk Assessment	6. Clear objectives specified	5
	7. Risks identified to achievement of objectives	5
	8. Potential for fraud considered	4
	9. Significant changes identified and assessed	3
Control Activities	10. Control activities selected and developed	6
	11. General IT controls selected and developed	4
	12. Controls deployed through policies and procedures	6
Information & Communication	13. Quality information obtained, generated and used	5
	14. Internal control information internally communicated	4
	15. Internal control information externally communicated	5
Monitoring Activities	16. Ongoing and/or separate evaluations conducted	7
	17. Internal control deficiencies evaluated and communicated	4

(Murphy, 2014)

What is risk?


Objectives

Risks

Results

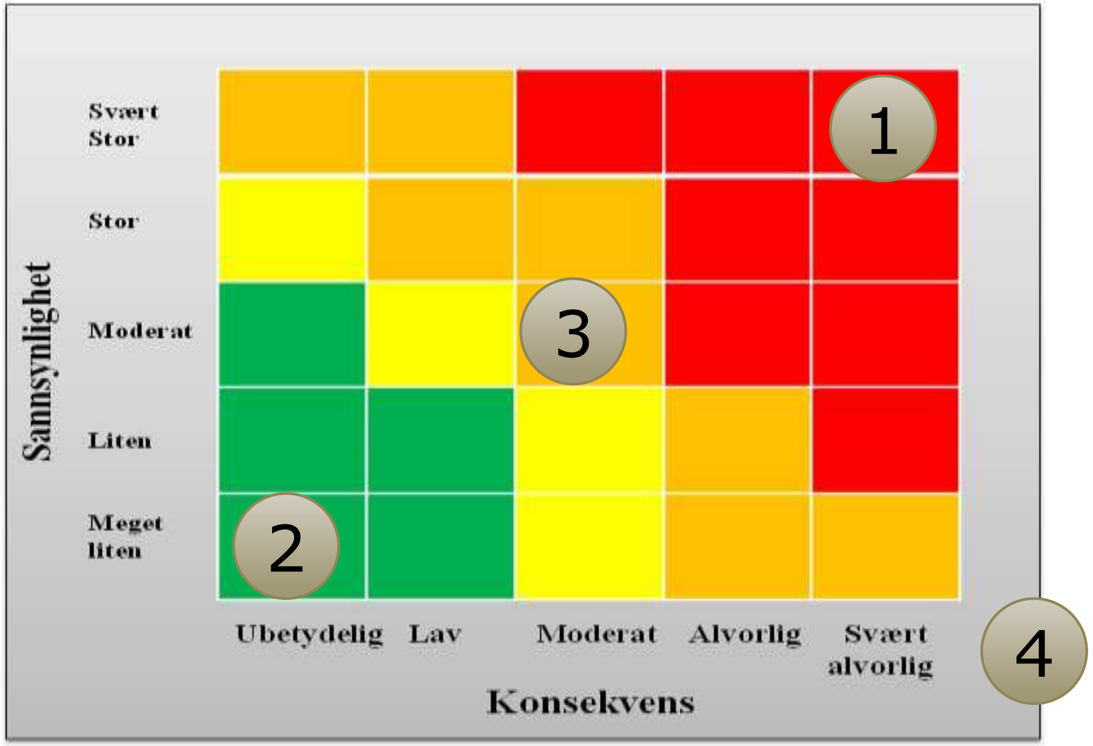
Modified from NMFA (2013)

Evaluating risks

Two dimensions:

- **Probability/Likelihood** that the event will take place
- **Impact** in case of the event

Probability/ Likelihood



	Ubetydelig	Lav	Moderat	Alvorlig	Svært alvorlig
Svært Stor	🟧	🟧	🟥	🟥	🟥 1
Stor	🟨	🟧	🟧	🟥	🟥
Moderat	🟩	🟨	🟧 3	🟥	🟥
Liten	🟩	🟩	🟨	🟧	🟥
Meget liten	🟩 2	🟩	🟨	🟧	🟧

Impact

🟥 Critical risks

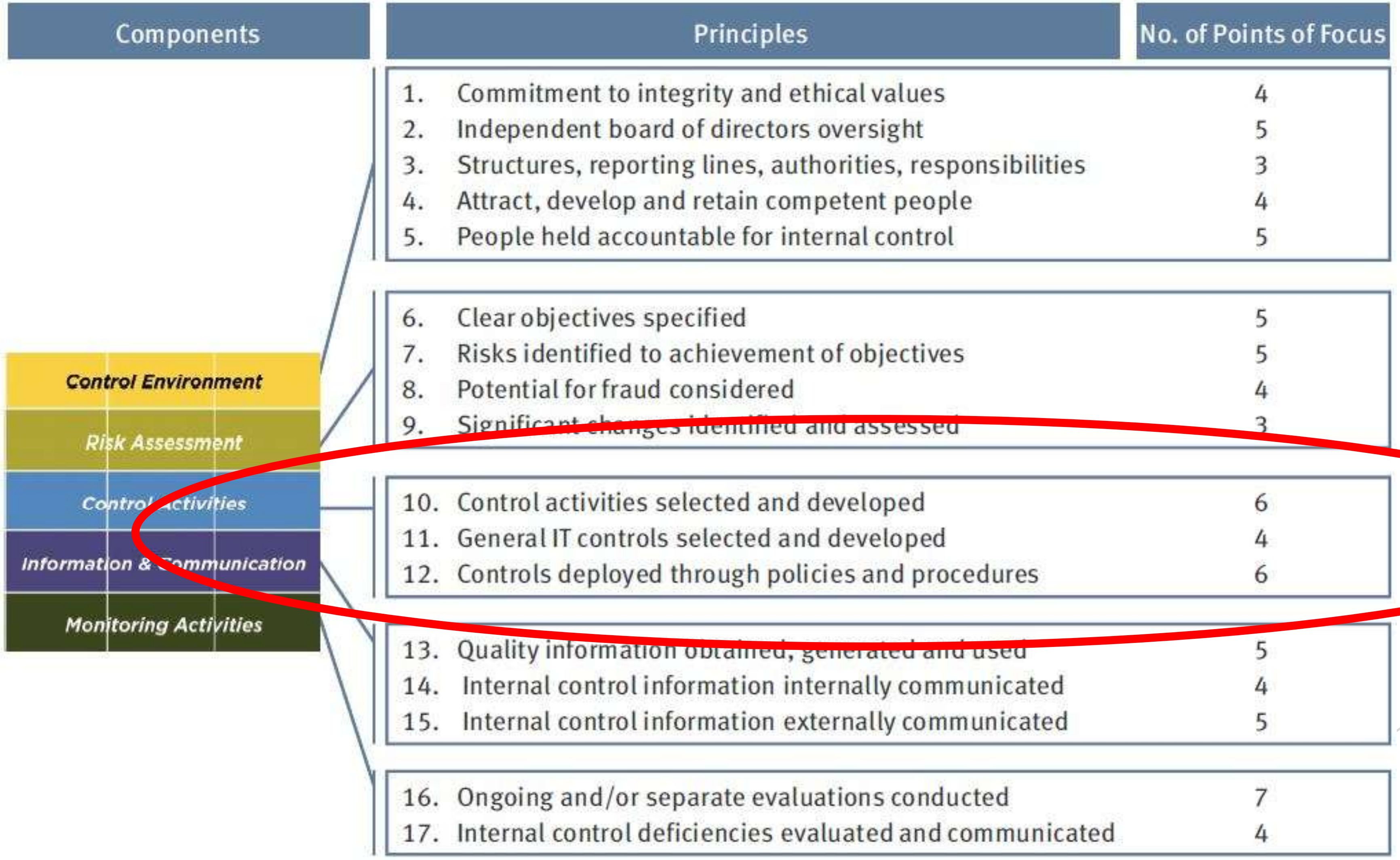
🟧 High risks

🟨 Moderate risks

🟩 Low risks

NMFA (2013)

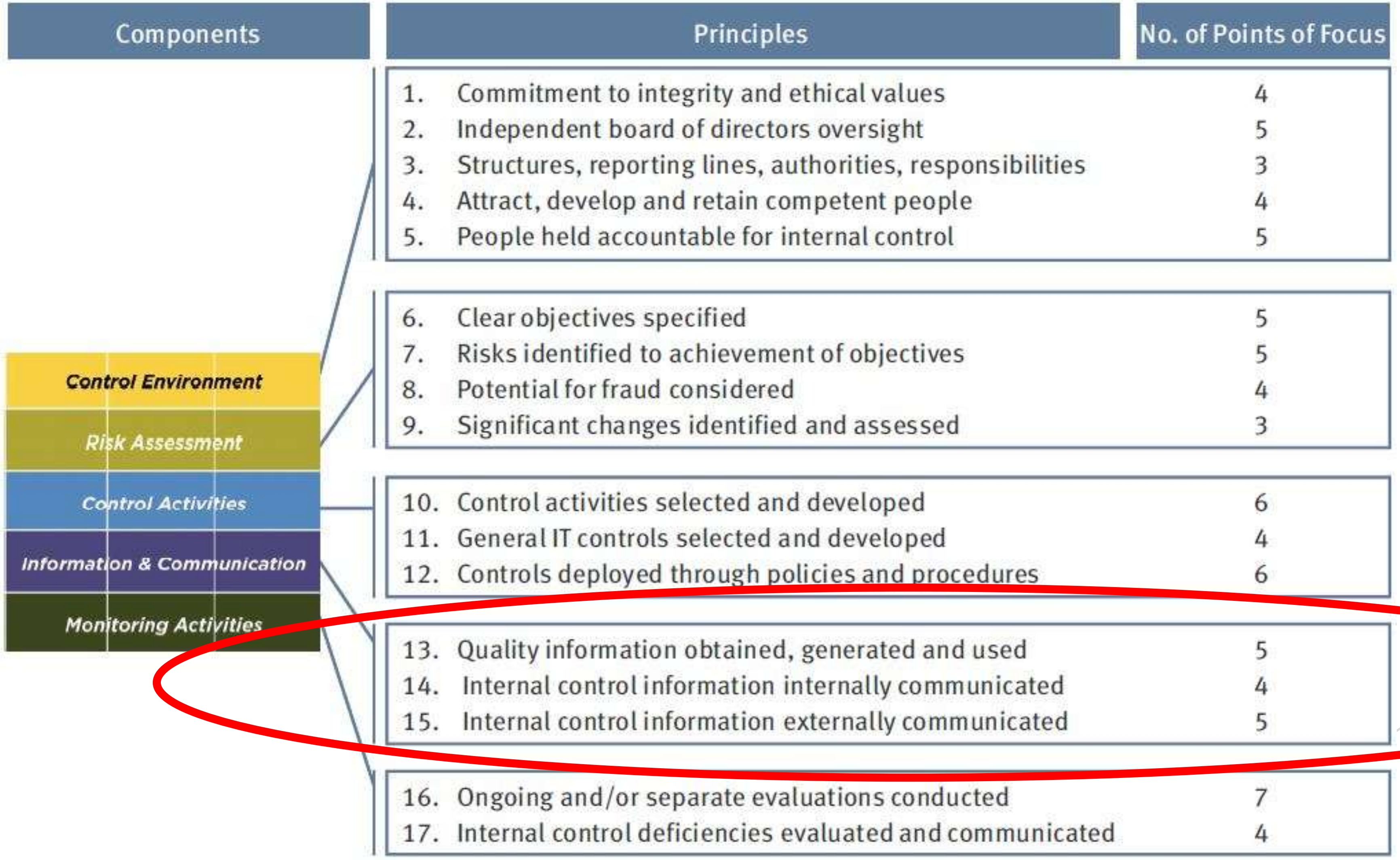
Principles: Control Activities



Components	Principles	No. of Points of Focus
Control Environment	1. Commitment to integrity and ethical values	4
	2. Independent board of directors oversight	5
	3. Structures, reporting lines, authorities, responsibilities	3
	4. Attract, develop and retain competent people	4
	5. People held accountable for internal control	5
Risk Assessment	6. Clear objectives specified	5
	7. Risks identified to achievement of objectives	5
	8. Potential for fraud considered	4
	9. Significant changes identified and assessed	3
Control Activities	10. Control activities selected and developed	6
	11. General IT controls selected and developed	4
	12. Controls deployed through policies and procedures	6
Information & Communication	13. Quality information obtained, generated and used	5
	14. Internal control information internally communicated	4
	15. Internal control information externally communicated	5
Monitoring Activities	16. Ongoing and/or separate evaluations conducted	7
	17. Internal control deficiencies evaluated and communicated	4

(Murphy, 2014)

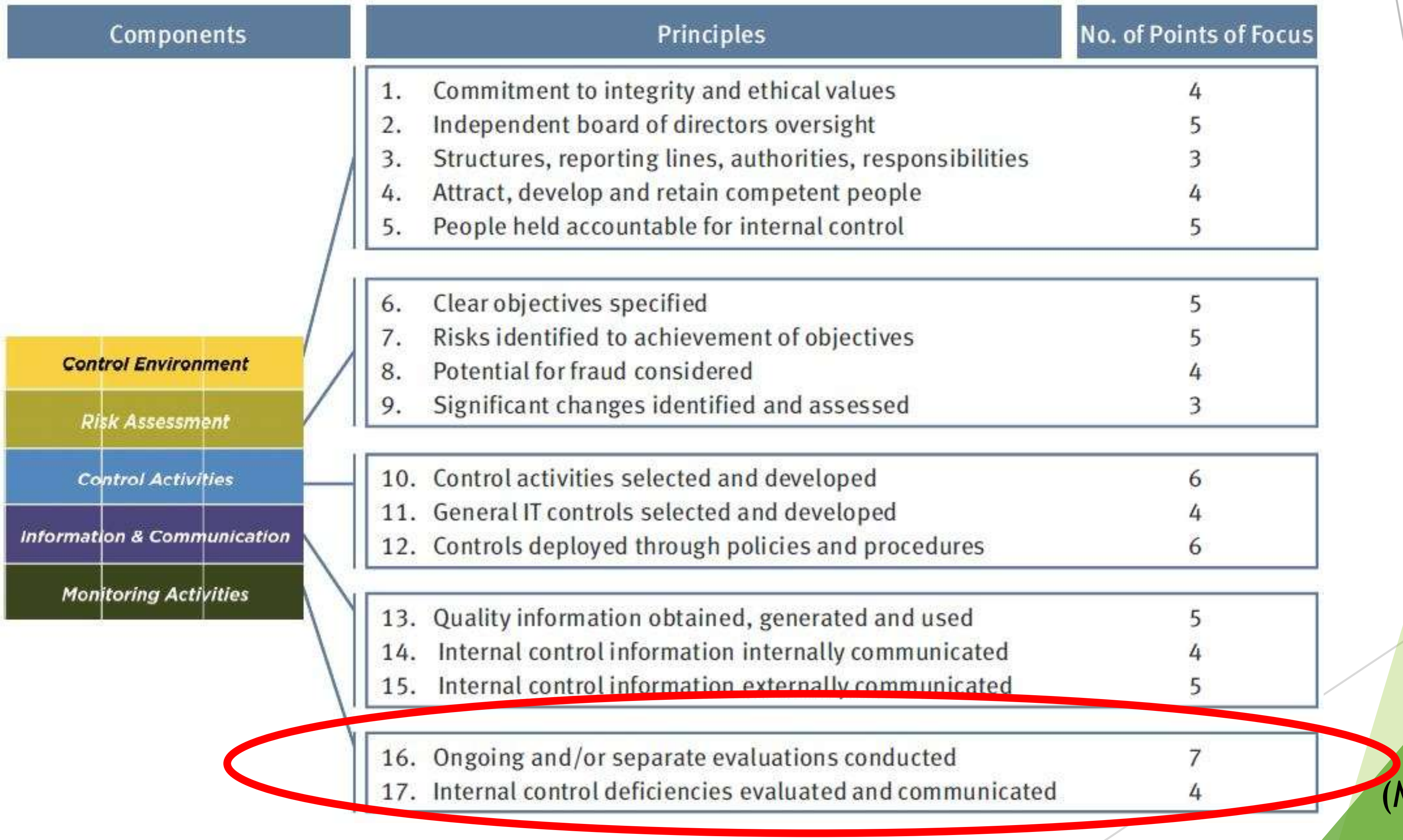
Principles: Information and Communication



Components	Principles	No. of Points of Focus
Control Environment	1. Commitment to integrity and ethical values	4
	2. Independent board of directors oversight	5
	3. Structures, reporting lines, authorities, responsibilities	3
	4. Attract, develop and retain competent people	4
	5. People held accountable for internal control	5
Risk Assessment	6. Clear objectives specified	5
	7. Risks identified to achievement of objectives	5
	8. Potential for fraud considered	4
	9. Significant changes identified and assessed	3
Control Activities	10. Control activities selected and developed	6
	11. General IT controls selected and developed	4
	12. Controls deployed through policies and procedures	6
Information & Communication	13. Quality information obtained, generated and used	5
	14. Internal control information internally communicated	4
	15. Internal control information externally communicated	5
Monitoring Activities	16. Ongoing and/or separate evaluations conducted	7
	17. Internal control deficiencies evaluated and communicated	4

(Murphy, 2014)

Principles: Monitoring Activities



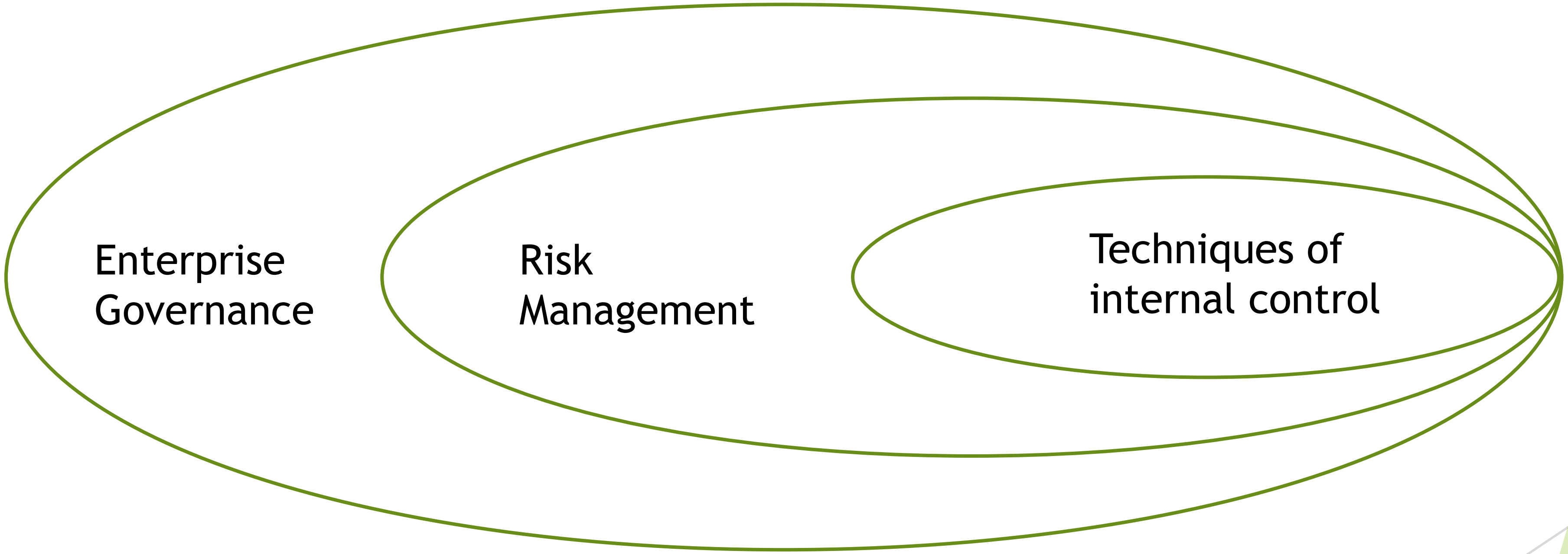
Components	Principles	No. of Points of Focus
Control Environment	1. Commitment to integrity and ethical values	4
	2. Independent board of directors oversight	5
	3. Structures, reporting lines, authorities, responsibilities	3
	4. Attract, develop and retain competent people	4
	5. People held accountable for internal control	5
Risk Assessment	6. Clear objectives specified	5
	7. Risks identified to achievement of objectives	5
	8. Potential for fraud considered	4
	9. Significant changes identified and assessed	3
Control Activities	10. Control activities selected and developed	6
	11. General IT controls selected and developed	4
	12. Controls deployed through policies and procedures	6
Information & Communication	13. Quality information obtained, generated and used	5
	14. Internal control information internally communicated	4
	15. Internal control information externally communicated	5
Monitoring Activities	16. Ongoing and/or separate evaluations conducted	7
	17. Internal control deficiencies evaluated and communicated	4

(Murphy, 2014)

Example: Points of Focus

Control environment			
Principles		Points of Focus	
1	The organization demonstrates commitment to integrity and ethical values	1	Sets the tone at the top
		2	Establishes standards of conduct (SoC)
		3	Evaluates adherence to SoC
		4	Addresses deviations in a timely manner
2	The BoD demonstrates independence from management and exercises oversight of the development and performance of internal control	5	Established oversight responsibilities
		6	Applies relevant expertise
		7	Operates independently
		8	Provides oversight on 5 components of COSO II framework

Summary: Internal control from a governance perspective



Moeller (2014)