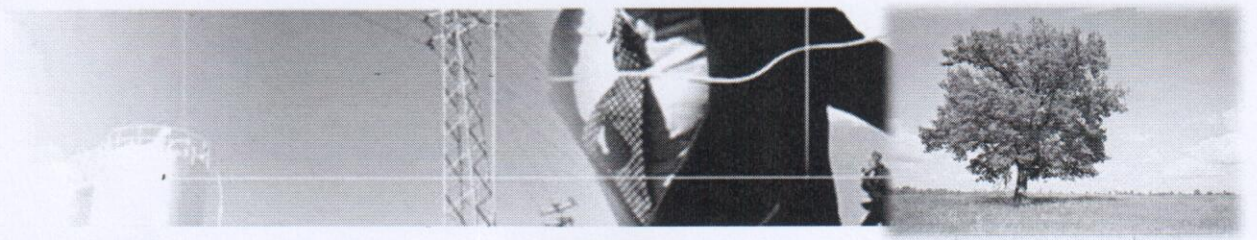
RISK MANAGEMENT SPECIALIST (RMS)
นักบริหารความเสี่ยงมืออาชีพ

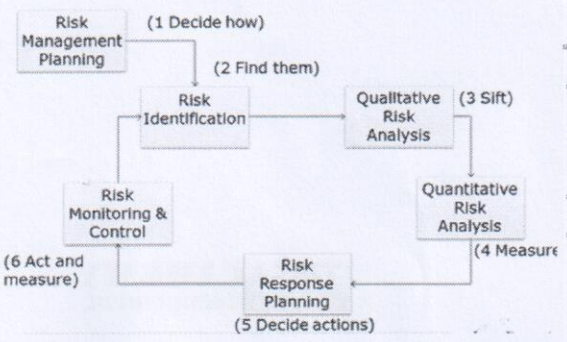
TRISACADEMY of Management

ไวฑูรย์ โภคาชัยพัฒน์
ผู้ช่วยกรรมการผู้จัดการ ทริส คอร์ปอเรชั่น

23 May 2014

GRC: Governance, Risk, and Compliance





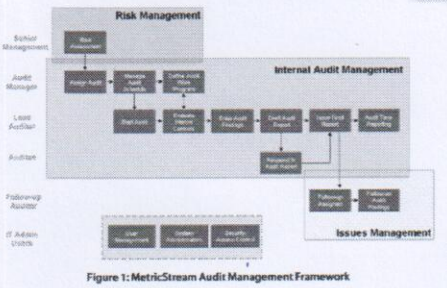
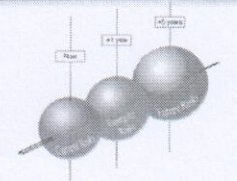


Figure 1: MetricStream Audit Management Framework



TRISACADEMY of Management

หัวข้อการนำเสนอ

1. แนวคิด GRC (Governance, Risk, Compliance)
2. การนำ GRC มาใช้ในทางปฏิบัติ
3. ปัจจัยสำคัญต่อความสำเร็จ

TRISACADEMY of Management

1. แนวคิด GRC (Governance, Risk, Compliance)

TRISACADEMY of Management

Why Public Entities need Governance, Risk, and Compliance

Governance + Risk Management + Compliance = Integrity

equates to

Structures + Threat Mitigation + Proofing = Public Trust

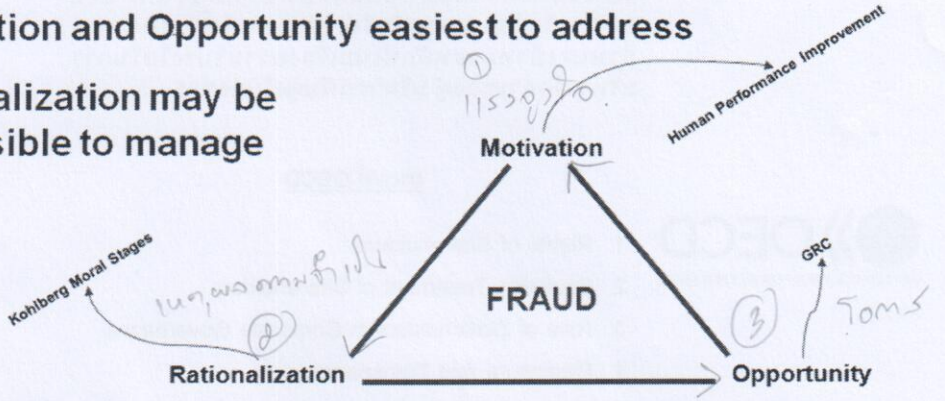
TRIS ACADEMY of Management

Why Public Entities need Governance, Risk, and Compliance

Fraud Triangle

Reducing Fraud in Government

- As much as 7% of annual budget*
  - That is $70m per billion of budget
- Need to break one leg of the triangle
- Motivation and Opportunity easiest to address
- Rationalization may be impossible to manage

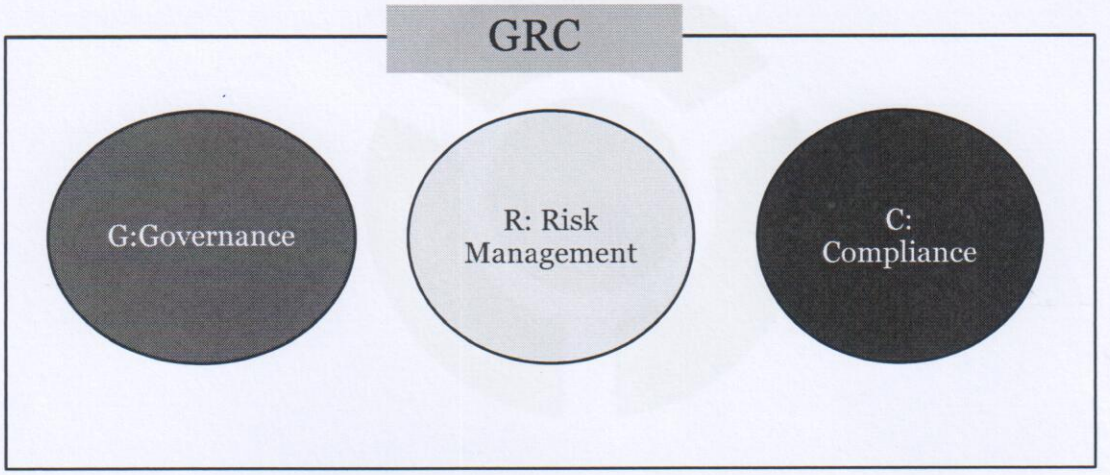


Pednault, S. (2009). *Fraud 101: Techniques and Strategies for Understanding Fraud, 3rd ed.* Hoboken, NJ: John Wiley & Sons, p. xi.

TRIS ACADEMY of Management

What is GRC?

GRC: Governance, Risk (Management), Compliance



TRISACADEMY of Management

ก่อนอื่น ...

รู้จักแต่ละองค์ประกอบของ GRC: Governance, Risk (Management), Compliance

Governance: ธรรมาภิบาล, การกำกับดูแลที่ดี

นโยบาย วัฒนธรรมองค์กร กระบวนการขั้นตอนการปฏิบัติงาน ที่ถูกกำหนดออกมาอย่างชัดเจนในการบริหารจัดการและกำกับดูแลองค์กรโดยคณะกรรมการผ่านผู้บริหารเพื่อการบริหารองค์กรที่โปร่งใส ตรวจสอบได้ รวมถึงความสัมพันธ์และบทบาทของทุกคนในองค์กรไม่ใช่เฉพาะผู้บริหารอย่างเดียว ตลอดจนกำหนดเป้าหมายหลักที่เน้นเรื่องความโปร่งใสในการบริหารจัดการของผู้ บริหารระดับสูงในองค์กร

เกณฑ์ OECD

OECD BETTER POLICIES FOR BETTER LIVES

1. Rights of Shareholders
2. Equitable Treatment of Shareholders
3. Role of Stakeholders in Corporate Governance
4. Disclosure and Transparency
5. Board Responsibilities

TRISACADEMY of Management

GRC: Governance, Risk (Management), Compliance

Governance: ธรรมาภิบาล, การกำกับดูแลที่ดี ของรัฐวิสาหกิจ

3.2 หลักการและแนวทางการกำกับดูแลที่ดีในรัฐวิสาหกิจ ประกอบด้วยหลักการและแนวทางปฏิบัติที่ดีเกี่ยวกับการกำกับดูแลที่ดีในรัฐวิสาหกิจ ซึ่งแบ่งเนื้อหาออกเป็น 6 หมวด ได้แก่

1) หมวดที่ 1 สิทธิของภาครัฐ/ผู้ถือหุ้น

การปฏิบัติต่อผู้ถือหุ้นอย่างเท่าเทียมกันในการประชุม การซักถาม การแสดงความคิดเห็น รวมทั้งการมีสิทธิออกเสียงลงคะแนน

2) หมวดที่ 2 ความเท่าเทียมกันของผู้ถือหุ้น

การได้รับการปฏิบัติที่เท่าเทียมกันในการประชุม การได้รับข้อมูลข่าวสาร การแสดงความคิดเห็น และการมีสิทธิออกเสียงลงคะแนน

3) หมวดที่ 3 ความรับผิดชอบของคณะกรรมการ

หน้าที่และความรับผิดชอบ ภาวะผู้นำและคุณลักษณะของคณะกรรมการ ความเป็นอิสระของคณะกรรมการ การถ่วงดุลของคณะกรรมการ ความมีประสิทธิภาพของคณะกรรมการ และการจัดตั้งคณะอนุกรรมการ การแต่งตั้งและเลือกตั้งกรรมการ คุณลักษณะของกรรมการ บทบาทของกรรมการอิสระ การประเมินผลของคณะกรรมการ การดำเนินการประชุมของคณะกรรมการ การได้รับเอกสารและข้อมูลของคณะกรรมการ และค่าตอบแทนของกรรมการ

4) หมวดที่ 4 บทบาทของผู้มีส่วนได้ส่วนเสีย

การดูแลผู้มีส่วนได้ส่วนเสียของรัฐวิสาหกิจ/องค์กรตามสิทธิที่มีตามกฎหมายที่เกี่ยวข้อง รวมถึงกระบวนการส่งเสริมให้เกิดความร่วมมือระหว่างรัฐวิสาหกิจกับผู้มีส่วนได้ส่วนเสียในการดำเนินการเพื่อให้เกิดความมั่นคงและยั่งยืนของกิจการ

5) หมวดที่ 5 การเปิดเผยข้อมูลสารสนเทศ และความโปร่งใส

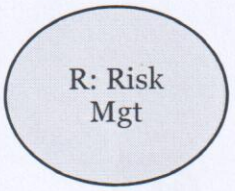
การเปิดเผยข้อมูลสารสนเทศที่สำคัญ ทั้งที่เป็นสารสนเทศทางการเงินและที่ไม่ใช่ทางการเงิน อย่างถูกต้องเชื่อถือได้ ครบถ้วน เพียงพอ สม่ำเสมอ และทันเวลา โดยต้องดำเนินการตามพระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ. 2540 และที่จะมีการแก้ไขเพิ่มเติมในอนาคต

6) หมวดที่ 6 จรรยาบรรณ

แนวทางการปฏิบัติเกี่ยวกับจรรยาบรรณเพื่อให้กรรมการ ฝ่ายจัดการ และพนักงานทุกคนได้ทราบถึงมาตรฐานการปฏิบัติที่รัฐวิสาหกิจเจ้าของกิจการ/ผู้ถือหุ้นคาดหวัง

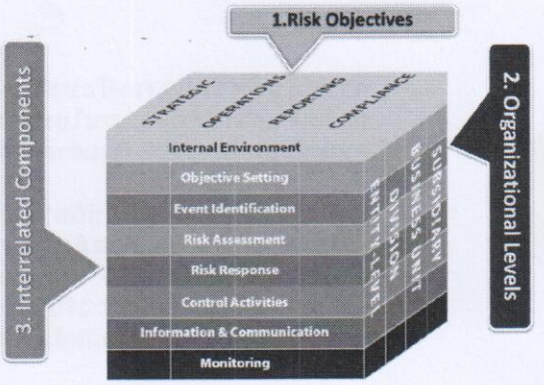
TRISACADEMY of Management

GRC: Governance, Risk (Management), Compliance



Risk Management

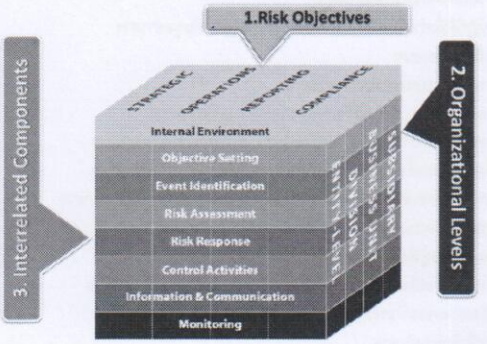
การบริหารจัดการความเสี่ยงที่มีเป้าหมายในการลดผลกระทบจากความเสี่ยงที่อาจ มีโอกาสเกิดขึ้นได้ในองค์กร หากไม่มีการบริหารจัดการความเสี่ยงที่ดีพอ และการสร้างมูลค่าเพิ่มจากการที่มีความมั่นใจอย่างสมเหตุสมผลในการตัดสินใจต่างๆ

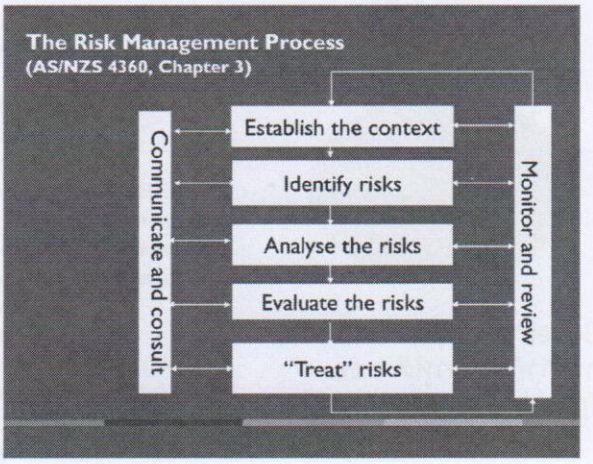


TRISACADEMY of Management

GRC: Governance, Risk (Management), Compliance

แบบจำลอง COSO ERM และ AS/NZS 4360





GRC: Governance, Risk (Management), Compliance

Compliance

- การปฏิบัติตามกฎระเบียบข้อบังคับ และกฎหมาย ตลอดจนการปฏิบัติตามนโยบายด้านสารสนเทศและความปลอดภัยขององค์กรอย่างถูกต้องได้ตามมาตรฐาน
- ยกตัวอย่าง เช่น การปฏิบัติตามประกาศมาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมอิเล็คทรอนิกส์โดยคณะกรรมการธุรกรรมอิเล็คทรอนิกส์ และการจัดทำแผนเพื่อรองรับพระราชบัญญัติ และพระราชกฤษฎีกาด้านความปลอดภัยทางอิเล็กทรอนิกส์
- ประเด็น : ฝ่าย กม., Compliance Unit

ตัวอย่าง กฎ ระเบียบ (จำนวนหนึ่ง) ที่ต้องปฏิบัติตามของ USA

Regulations to be compliant with

Finance	Government	Healthcare Life Sciences	Distribution	Industrial
Basel II	DOD 5015.2	HIPAA	UCC net	Tread Act
Patriot Act	UK-Pro	FDA 21 CFR 11	RFID	Security Standards
Anti-Money Laundering	Gov. Paperwork Elimination Act	FDA Drug Barcode regulation	Bar-code modification	Motor Vehicle Block Exemption Act
Gramm-Leach-Bliley Act			GCI (Global Commerce Init)	
SEC 17-a-4			Chip and Pin	

Sarbanes-Oxley

International Accounting standards

Data Protection Act

Freedom of Information Act

ISO 17799 Information Security Standards

California State Bill – SB 1386

Several Privacy regulations

TRIS ACADEMY of Management

ตัวอย่าง กฎ ระเบียบ (จำนวนหนึ่ง) ที่ต้องปฏิบัติตามของ US Banks

Financial Institutions Are the Heavily Regulated and Can Be a Role Model

- Anti-Money Laundering Laws and Regulations
- Anti-Tying
- Community Reinvestment Act (CRA)
- Federal Reserve Regulation
  - Sections 23A and 23B of the US Federal Reserve Act
  - Covered Borrowers, Regulation U, T
- Federal Deposit Insurance Corporation Improvement Act (FDIC)
- Gramm-Leach-Bliley Act (GLBA)
  - Financial Holding Company (FHC)
    - Banking activities plus expanded activities that include
      - securities underwriting and dealing
      - insurance agency and underwriting activities; and
      - merchant banking activities
  - Bank Holding Company Act
- Public Company Accounting Oversight Board (PCAOB)
- Department of Treasury
  - Office of the Controller of the Currency (OCC)
- Securities and Exchange Commission
  - Consolidated Supervised Entities
- Sanctions
  - Congressional or executive order
- Sarbanes-Oxley Act (SOX)
- US Anti-Boycott Regulations
- US Export Controls
- US Foreign Corrupt Practices Act ("FCPA")
- USA Patriot Act (aka - Know Your Customer)
- Confidentiality, Conflicts of Interest, Personal Investments, Chinese Walls
- Customer Suitability / Appropriateness

PCAOB Public Company Accounting Oversight Board

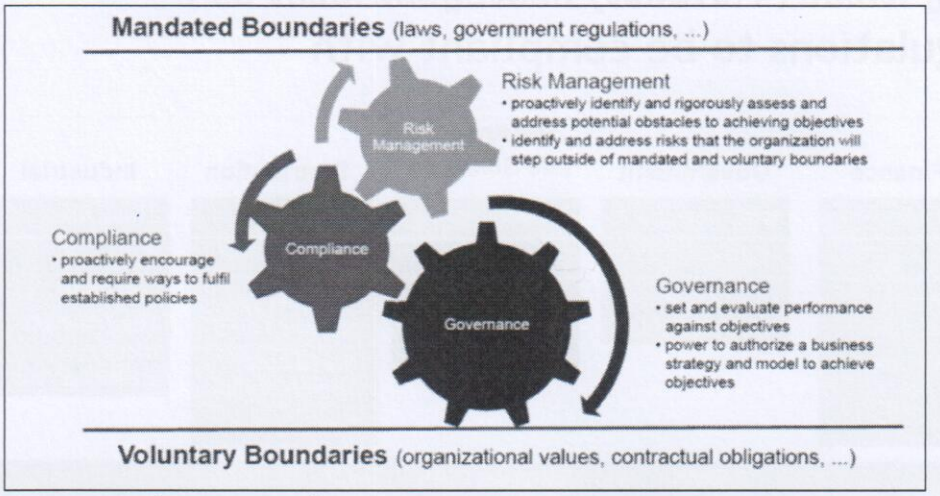
FDIC FEDERAL DEPOSIT INSURANCE CORPORATION

The Federal Reserve Board

Comptroller of the Currency Administrator of National Banks
US Department of the Treasury

TRIS ACADEMY of Management

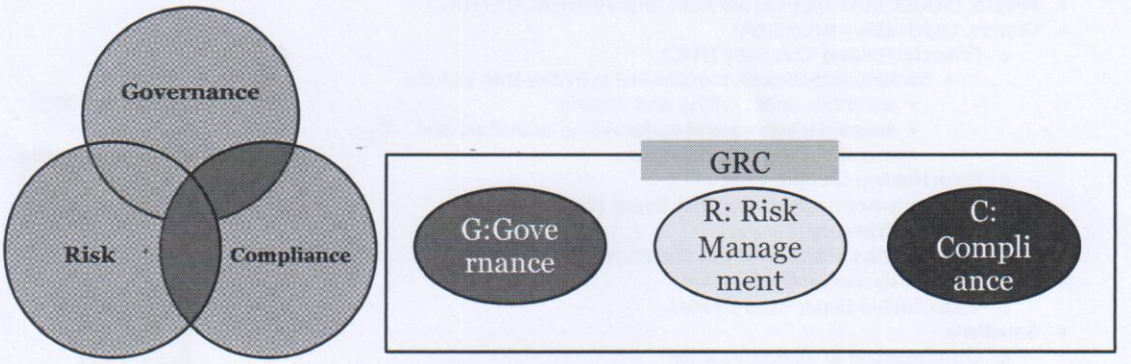
แนวคิด GRC: Governance, Risk (Management), Compliance มาได้อย่างไร?



- Governance เป็นกรอบใหญ่ ที่ทุกหน่วยงานรัฐ และ เอกชน ควรยึดถือปฏิบัติ
- อย่างไรก็ตาม การจะได้มาซึ่ง "Good Governance" ต้องมีการบริหารความเสี่ยง (Risk Management) และการดำเนินการที่มั่นใจว่าได้ปฏิบัติตามกฎระเบียบและข้อกฎหมายต่างๆ (Compliance Management) ควบคู่กันไป
- ดังนั้น จะเห็นว่า "Governance", "Risk" และ "Compliance" มีความสัมพันธ์ และมีความเกี่ยวข้องกัน
- แนวคิด "GRC" นั้น ต้องการที่จะนำองค์ประกอบทั้ง 3 มาปฏิบัติร่วมกันในรูปแบบของการบูรณาการกัน

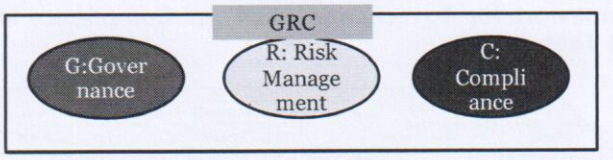
TRISACADEMY of Management

ถ้าเช่นนั้น GRC คืออะไร?



TRISACADEMY of Management

GRC คืออะไร?

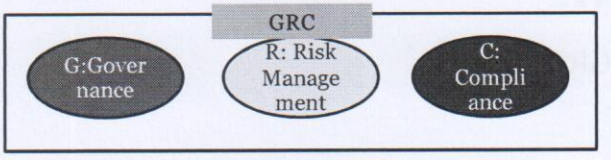


Open Compliance and Ethics Group (OCEG) ได้ระบุความหมายของ GRC ว่าเป็นระบบที่เกี่ยวข้องกับคน (people) กระบวนการ (processes) และเทคโนโลยี (technology) ที่ช่วยขับเคลื่อนองค์กรให้

- มีความเข้าใจและจัดลำดับความสาคัญต่อความคาดหวังของผู้มีส่วนได้เสีย (Stakeholders)
- กำหนดวัตถุประสงค์ทางธุรกิจเพื่อให้สอดคล้องกับมูลค่าและความเสี่ยงที่เกี่ยวข้อง
- บรรลุวัตถุประสงค์ตามเป้าหมายที่กำหนด และสามารถเพิ่มประสิทธิภาพในการเฝ้าระวังความเสี่ยง (Risk Profile) และปกป้องคุณค่าขององค์กร (Value)
- ดำเนินการภายใต้ขอบเขตของกฎหมาย สัญญา ระบบภายใน สังคม และจริยธรรม
- ให้ข้อมูลที่เกี่ยวข้อง เชื่อถือได้ และทันเวลา ต่อผู้มีส่วนได้เสีย
- ส่งเสริมการวัดผลของระบบการดำเนินงานและการมีประสิทธิผล

TRISACADEMY of Management

GRC คืออะไร?



PWC นิยาม GRC ว่า

- GRC หมายถึง การทำให้คณะกรรมการสามารถกำกับดูแลองค์กรและให้คำแนะนำแก่ผู้บริหารเพื่อดำเนินงานให้ปฏิบัติตามกฎระเบียบที่เกี่ยวข้องได้อย่างมั่นใจ

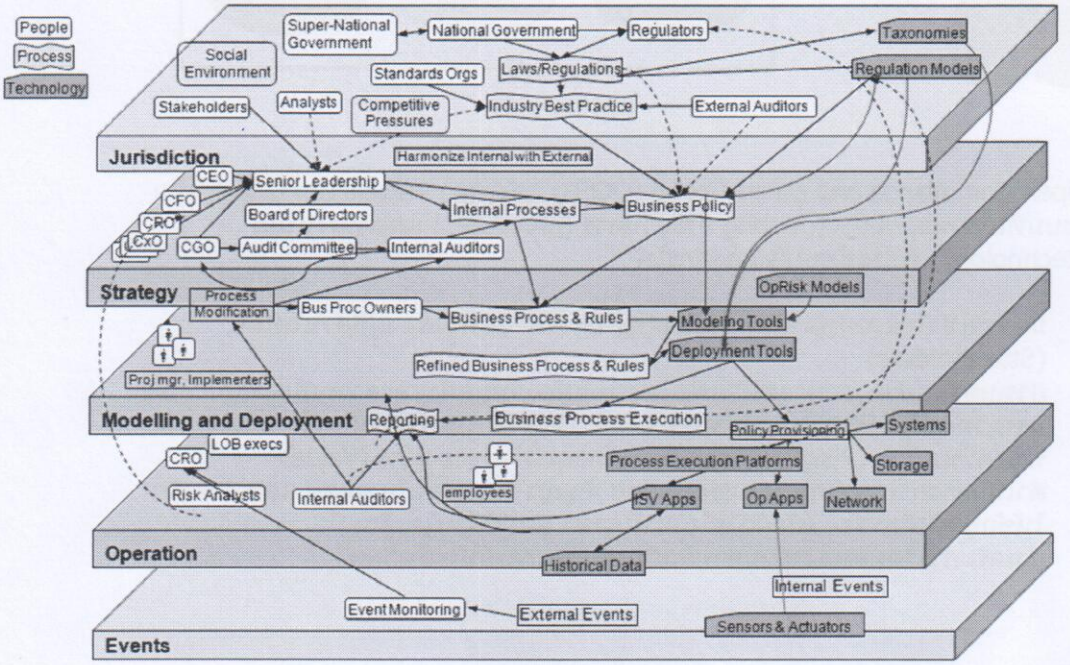
  ทั้งนี้ ผู้บริหารต้องจัดให้มีการบริหารความเสี่ยงที่เป็นระบบ มุ่งเน้นความเสี่ยงที่ตรงประเด็น และสามารถจัดกระบวนการทำงานเพื่อให้มีการปฏิบัติตามระเบียบหรือการควบคุมภายในได้อย่างเหมาะสม ภายใต้ต้นทุนการดำเนินงานที่สมเหตุผล

  รวมถึงการนำเทคโนโลยีมาสนับสนุนการทำงานให้มีประสิทธิภาพ และการสื่อสารข้อมูลอย่างถูกต้องเหมาะสม ทันเวลา ต่อผู้เกี่ยวข้องทุกระดับ

TRISACADEMY of Management

GRC คืออะไร?

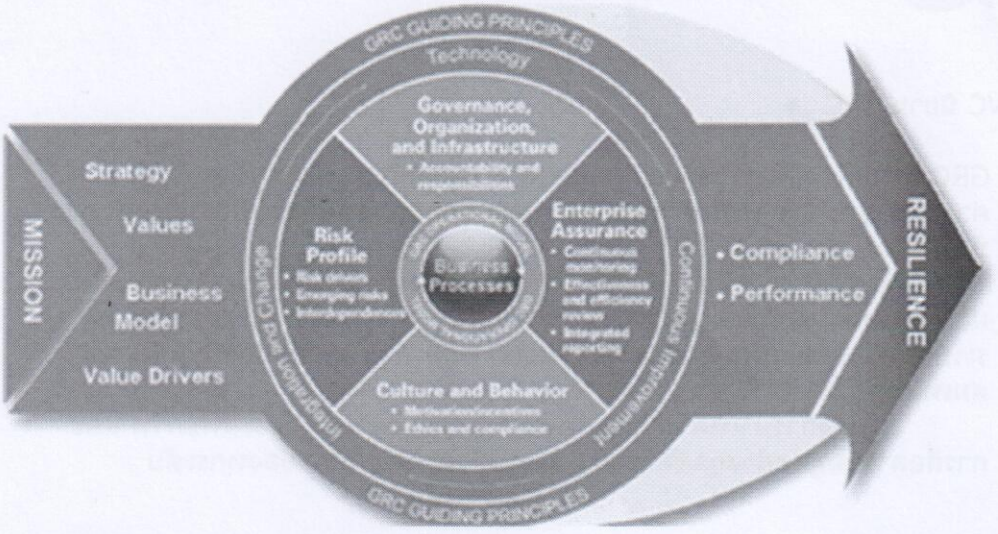
A Unified Framework for Governance, Risk and Compliance Must Support People, Process, and Technology



TRISACADEMY of Management

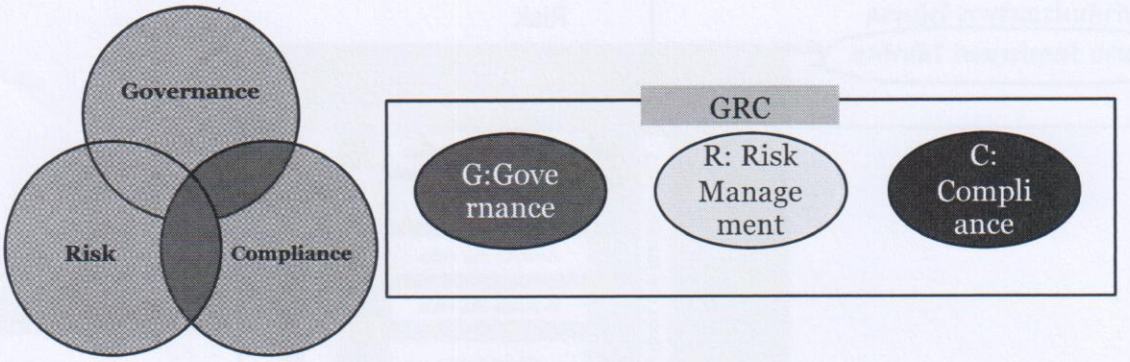
GRC คืออะไร?

KPMG GRC Model



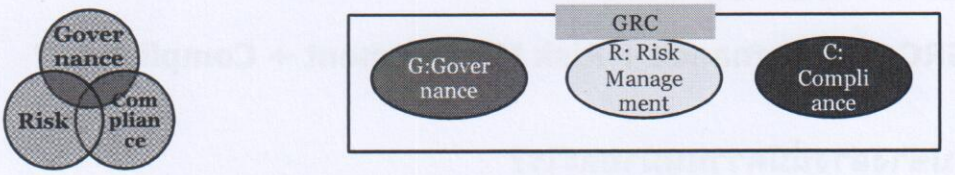
TRISACADEMY of Management

จริงๆ แล้ว GRC คืออะไร?



TRISACADEMY of Management

จริงๆ แล้ว GRC คืออะไร?



- Governance เป็นกรอบใหญ่ ที่ทุกหน่วยงานรัฐ และ เอกชน ควรยึดถือปฏิบัติGRC เป็นการ ยกระดับ ของ Risk Management และ Compliance ขึ้น
- GRC เป็น การบูรณาการ ดังนั้น วงกลมทั้ง 3 วง จึงมีทั้งส่วนที่ ทับซ้อนกัน สัมพันธ์กัน และส่วนที่ แตกต่างกัน เป็นอิสระกัน ตามหลักการที่เรียกว่าInterdependent
- GRC จึงช่วยในการ พัฒนาธรรมภิบาล ของทั่วทั้งองค์กรโดยการยกระดับกระบวนการที่ทับซ้อนกัน และ การเพิ่มการแบ่งปันข้อมูล และการประสานงานระหว่างฝ่ายต่างๆ ขององค์กรที่ทำหน้าที่สัมพันธ์เกี่ยวข้องกัน
- ตัวอย่าง เช่น GRC จะกำหนดให้มีการกระบวนการประเมินความเสี่ยงร่วมกัน ซึ่งโดยปกติมักจะทาแยกระหว่างฝ่ายต่างๆ จึงเป็นการเพิ่มประสิทธิภาพของการทางาน การยกระดับการประเมินความเสี่ยงข้ามฝ่ายนี้จะช่วยลดช่องว่างในกระบวนการและขอบเขตการทางาน และเพิ่มประสิทธิผลโดยการเพิ่มการแบ่งปันข้อมูลและความร่วมมือในการทากิจกรรมต่างๆ

ประเด็น คือ แล้วส่วนที่ ทับซ้อนกัน สัมพันธ์กัน และส่วนที่ แตกต่างกัน เป็นอิสระกัน ตามหลักการที่เรียกว่า Interdependent คืออะไร?

TRISACADEMY of Management

จริงๆ แล้ว GRC คืออะไร?

ประเด็น คือ แล้วส่วนที่ ทับซ้อนกัน สัมพันธ์กัน และส่วนที่ แตกต่างกัน เป็นอิสระกัน ตามหลักการที่เรียกว่า Interdependent

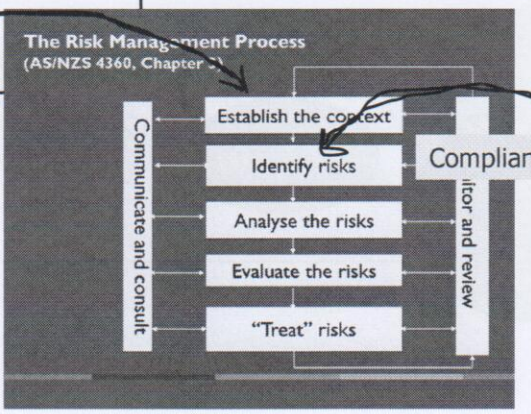
แต่อย่าลืมส่วนที่ไม่ทับซ้อน ที่เป็นอิสระต่างหากกัน ตามหลัก Interdependent

Governance

บทบาทและความรับผิดชอบของคณะกรรมการ

- การกำกับฝ่ายบริหาร ให้บรรลุเป้าหมาย วัตถุประสงค์ วิสัยทัศน์

Risk



Compliance Risk

Compliance

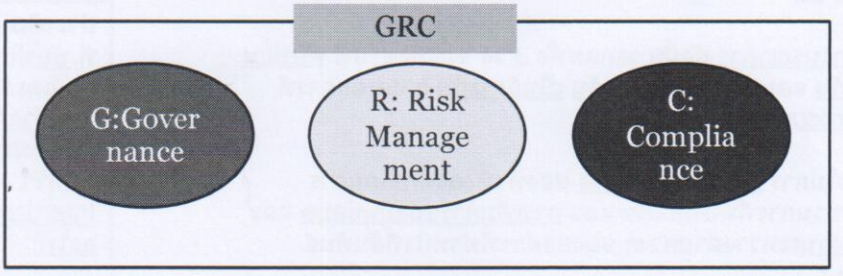
- Preventive
- Corrective

TRISACADEMY of Management

จริงๆ แล้ว GRC คืออะไร?

คำถาม : GRC ≠ Governance + Risk Management + Compliance ?

คำถาม : รูปข้างล่างนี้มีความหมายอะไร?



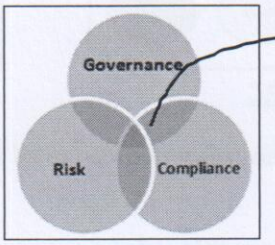
TRISACADEMY of Management

จริงๆ แล้ว GRC คืออะไร?

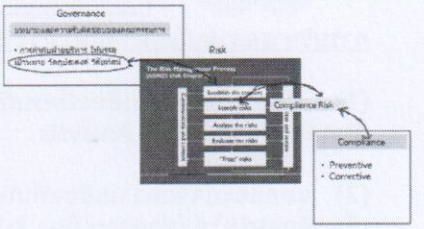
คำตอบ : GRC = Governance + Risk Management + Compliance

แต่ไม่ใช่ = Governance + Risk Management + Compliance
ในลักษณะ 1+1+1 = 3

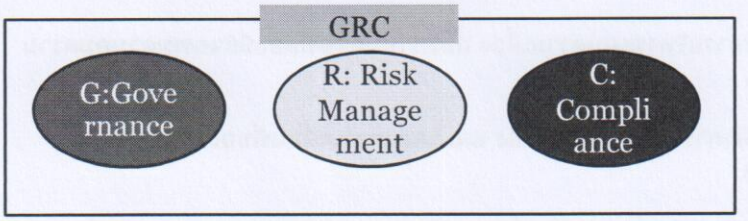
แต่เป็น 1+1+1 = 1 -→ บูรณาการ



ส่วนที่ทับซ้อนของวงทั้ง 3

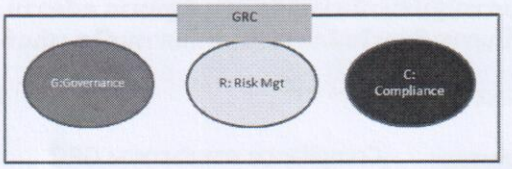


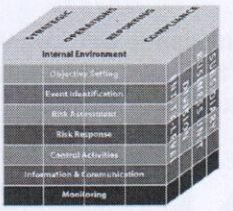
ซึ่งเป็นคำตอบ : รูปข้างล่างนี้มีความหมายอะไร?



TRISACADEMY of Management

คำถาม : GRC เหมือน หรือ ต่าง กับ ERM อย่างไร?

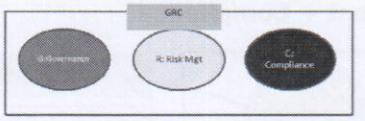




- GRC เป็นกรอบใหญ่ที่สุดที่ยกและแทรกการบริหารความเสี่ยงในเป็นส่วนหนึ่งของการบริหารจัดการทางธุรกิจของกิจการ
- ERM เป็นกรอบแนวทางการบริหารความเสี่ยงที่น่าทุกส่วนในระดับปฏิบัติมาเชื่อมโยงกันให้เป็นภาพในระดับองค์กร

TRISACADEMY of Management

คำถาม : Risk Management (ERM) ตามแนวทาง GRC เหมือน หรือ ต่าง กับ Risk Management (ERM) ทั่วไปอย่างไร?



การบริหารความเสี่ยงตามแนวทาง GRC

(1) การกำหนดปัจจัยเสี่ยงที่ครบถ้วนทุกพันธกิจ แผนกลยุทธ์ ประเด็นที่มาจากการวิเคราะห์จุดอ่อนและภัยคุกคามจาก SWOT Analysis

(2) แยกแยะปัจจัยความเสี่ยงที่เกินเกณฑ์ที่ยอมรับได้ (ค่าความเสี่ยงที่ 4 และ 5) ออกจากปัจจัยความเสี่ยงที่ยอมรับได้ (ค่าความเสี่ยง 1-3)

(3) นำเอาปัจจัยความเสี่ยงที่เกินเกณฑ์ที่ยอมรับได้ มาทำแผนบริหารความเสี่ยงรายธุรกรรม รายพื้นที่ที่ไม่ใช่รายฝ่ายงาน

(4) ตั้งดัชนีชี้วัดความสำเร็จของการบริหารแผนความเสี่ยง และกำหนดจุดที่ต้องมีกิจกรรมควบคุมความเสี่ยงเพิ่มเติม

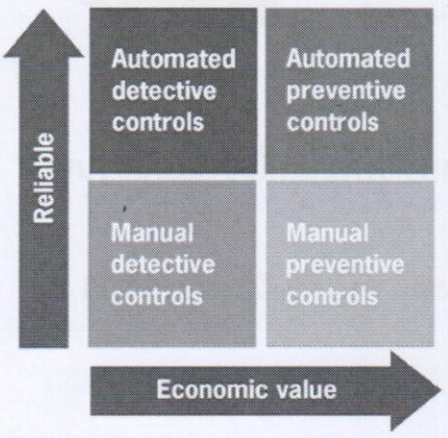
(5) รายงานสถานะความเสี่ยงหลังการทำแผนความเสี่ยง และแสดงการเคลื่อนที่ของความเสี่ยง และนำไปใช้เป็นข้อมูลในการตัดสินใจ

(6) กำหนดให้ผลการปฏิบัติงานด้านบริหารความเสี่ยงในการประเมินผลดำเนินงานรายบุคคล

TRISACADEMY of Management

คำถาม : Compliance ตามแนวทาง GRC เหมือน หรือ ต่าง กับ Compliance ทั่วไปอย่างไร?

Compliance ทั่วไปเน้นการกำกับการปฏิบัติมุ่งที่ความเสี่ยงด้านกฎหมาย คดีความ การร้องเรียนที่เกิดไปแล้ว หรือที่อาจเกิดเป็นหลัก จึงเป็นการบริหารในลักษณะของเน้นการแก้ไข เน้นเชิงป้องกันล่วงหน้าที่คุ้นเคย



Compliance ตามแนวทาง GRC

- เป็นการยกระดับความสามารถในการกำกับการปฏิบัติตามกฎเกณฑ์ในธุรกรรมใหม่ที่กิจการอาจจะไม่มีความคุ้นเคยจนมั่นใจว่า ระดับการกำกับเกินกว่าเกณฑ์ขั้นต่ำที่เป็นความคาดหวังของหน่วยงานและองค์กรกำกับจากภายนอก
- เป็นการลงรายละเอียดถึงระดับของการกำหนดแนวพึงปฏิบัติที่ดีและมีกระบวนการควบคุมการปฏิบัติมิให้มีโอกาสที่จะฝ่าฝืนกฎเกณฑ์
- คำว่า Compliance ใน GRC จึงอาจจะหมายถึง Ensure and Over-minimum Requirement of Compliance

TRISACADEMY of Management

GRC กับ IT

- GRC จึงช่วยในการ พัฒนาธรรมภิบาล ของทั่วทั้งองค์กรโดยการยกระดับกระบวนการที่ทับซ้อนกัน และ การเพิ่มการแบ่งปันข้อมูล และ การประสานงานระหว่างฝ่ายต่างๆ ขององค์กรที่ทำหน้าที่สัมพันธ์ เกี่ยวข้องกัน

- ปัญหาและอุปสรรคของการปฏิบัติตามหลักการ Regulatory นั้น อันดับหนึ่งคือ เรื่องงานเอกสาร (Documentation) และอันดับที่ 2 ถึง 8 นั้นเกี่ยวข้องกับเรื่อง IT Security ที่ยังไม่ได้ปฏิบัติตาม Standard หรือ Best Practice เช่น ISO/IEC 27001, ITIL หรือ ISO/IEC 20000 ตลอดจนมาตรฐาน CobiT 4.1 เป็นต้น

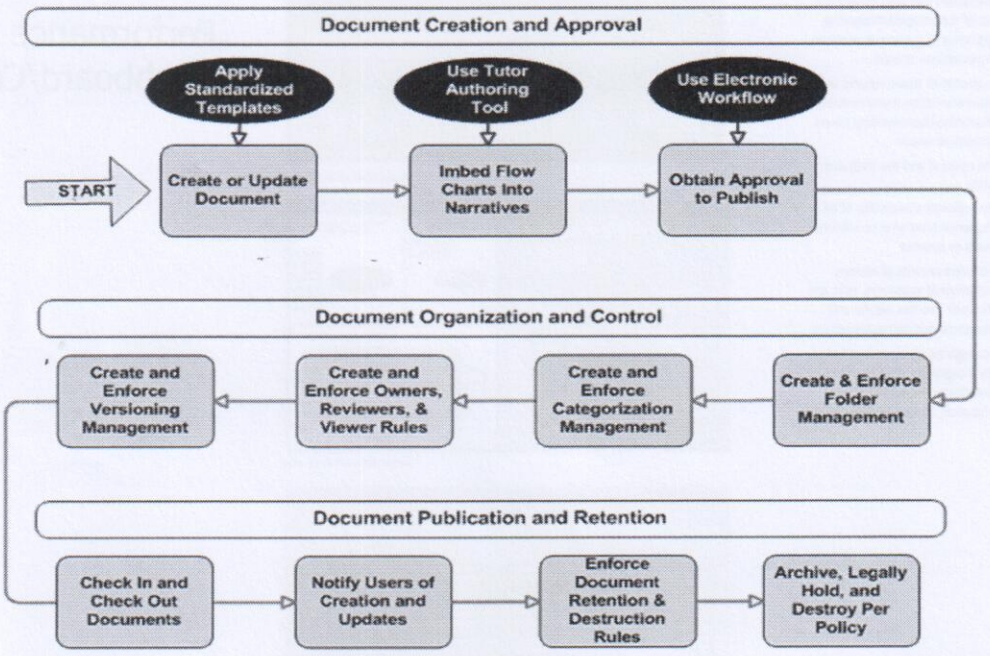
GRC จึงเกี่ยวข้องกับการจัดการสารสนเทศ (MIS) มากกว่าตัวเทคโนโลยี (IT) !

TRISACADEMY of Management

GRC กับ IT

What Does A Document Management Tool Provide?

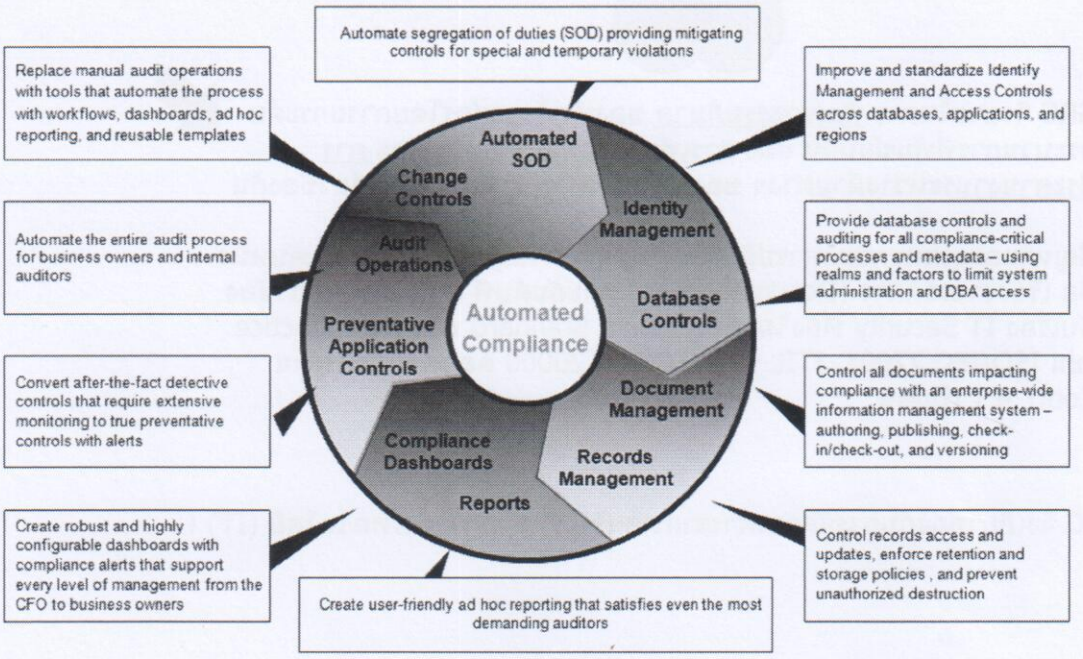
A Complete Document Life Cycle



TRISACADEMY of Management

GRC กับ IT

What is Automated Compliance?

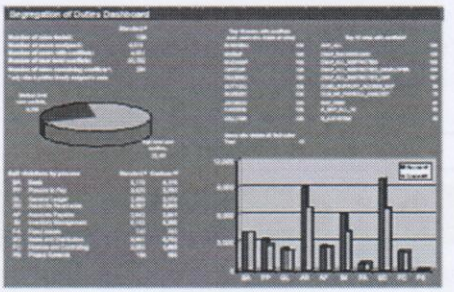


TRISACADEMY of Management

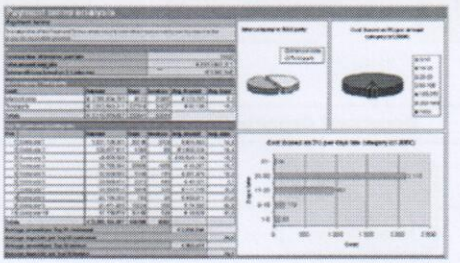
GRC กับ IT

A few key measures can help ensure the effectiveness of reporting/dashboarding. From the beginning of a controls monitoring effort, organizations should:

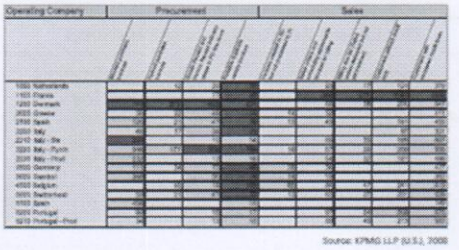
- Identify recipients of these reports as well as their information requirements, and tailor reporting/dashboarding views based on business needs
- Discuss the content and the frequency of the reports
- Identify the separate viewpoints of different compliance programs so reports can be issued as needed
- Identify the requirements of various internal and external reviewers, who are likely to first look into the results and then require more detailed explanations
- Improve acceptance of reporting/dashboarding by integrating it within existing business intelligence reporting tools (such as Hyperion, Business Objects, or Cognos).



Source: KPMG LLP (U.S.), 2008



Source: KPMG LLP (U.S.), 2008



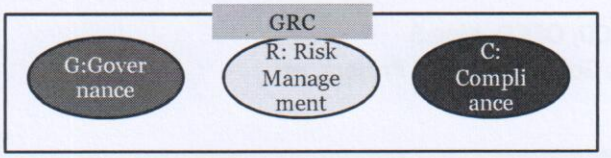
Source: KPMG LLP (U.S.), 2008

Performance Dashboard/Cockpit

TRISACADEMY of Management

สุดท้าย ...

GRC มีจุดแข็ง จุดเด่น อะไร?



"จุดแข็ง" หรือ "จุดขาย" ของ GRC คือ "GRC" นั้น นอกจากจะทำให้องค์กรแสดงถึงความเป็น "Good Governance" ที่เป็นกรอบใหญ่ แล้ว ยังทำให้องค์กรเกิดความสามารถในการแข่งขัน (Competitive Advantage) ที่เป็นรูปธรรมอีกด้วย

Good Governance ธรรมาภิบาล/การกำกับดูแลที่ดี = เป็น คน "เก่ง" และ คน "ดี"

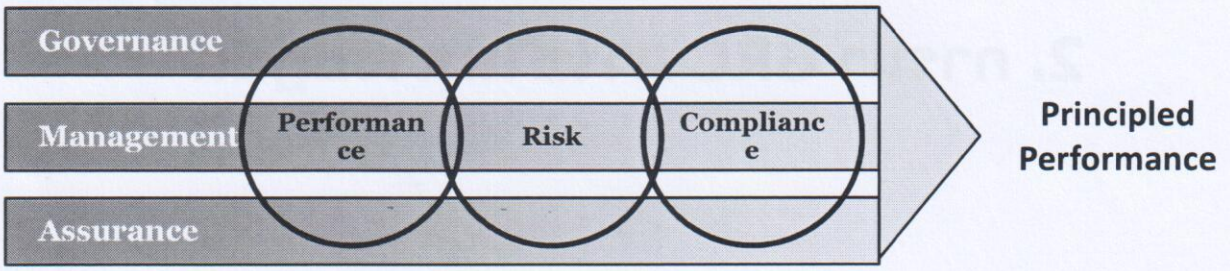
แต่เข้าใจยาก และหลายปัจจัยเป็น "นามธรรม"

ขณะที่ "Risk Management" และ "Compliance" ชัดเจนกว่า เป็น "รูปธรรม" มากกว่า และส่งผลต่อ ผลการดำเนินงาน "Performance" ได้ชัดเจนกว่า และรวดเร็วกว่า

TRISACADEMY of Management

GRC มีจุดแข็ง จุดเด่น อะไร?

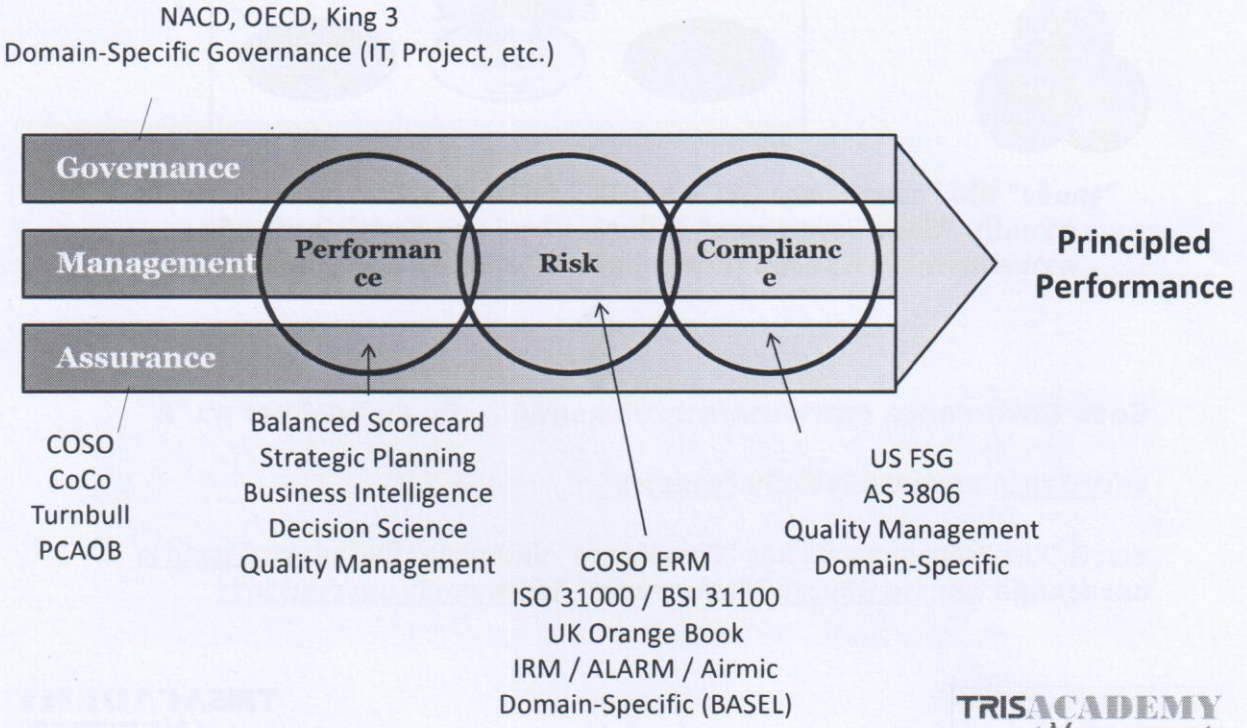
OCEG



The rigorous governance, assurance and management of performance, risk and compliance helps an organization reliably achieve objectives while addressing uncertainty and acting with integrity.

TRISACADEMY of Management

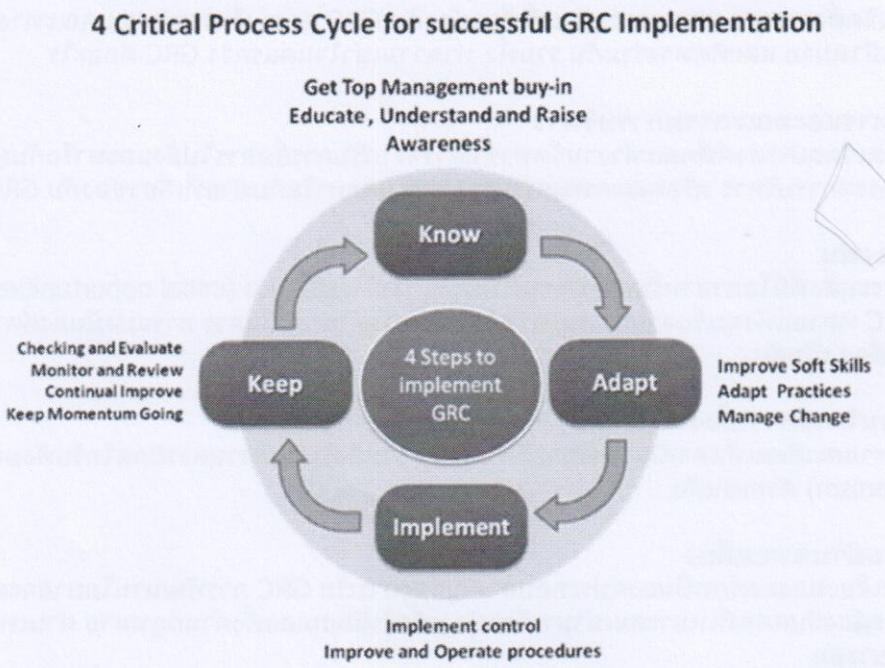
GRC มีจุดแข็ง จุดเด่น อะไร?



2. การนำ GRC มาใช้ในทางปฏิบัติ

การนำ GRC มาใช้ในทางปฏิบัติ

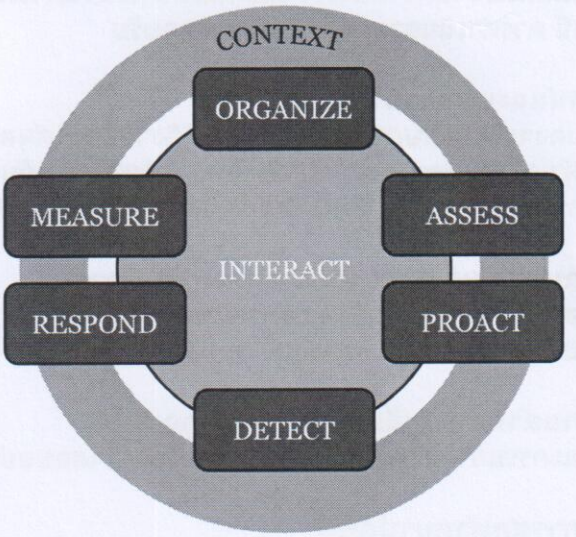
ตัวอย่างที่ 1 : ACIS' 4 ขั้นตอนหลัก ในการนำGRC มาใช้



การนำ GRC มาใช้ในทางปฏิบัติ

ตัวอย่างที่ 2: OCEG 8 ขั้นตอนหลัก ในการนำGRC มาใช้

8 INTEGRATED COMPONENTS



การนำ GRC มาใช้ในทางปฏิบัติ

ตัวอย่างที่ 3 : ศาสตราจารย์ มหาวิทยาลัยเดอพอล USA ได้ศึกษาและเสนอแนวทางที่มี 10 กระบวนการในการนำ GRC มาใช้

1. การร่วมมือของฝ่าย GRC ต่างๆ
ผู้บริหารควรเริ่มต้นจัดตั้งคณะทางานและระบุฝ่ายที่เกี่ยวข้องกับ GRC ต่างๆ ที่ควรเข้าร่วม คณะทางานจะต้องสร้างความเข้าใจ เป้าหมาย และทิศทางร่วมกัน รวมทั้ง ทำความเข้าใจแต่แรกว่า GRC คืออะไร

2. หารือกับผู้บริหารและคณะกรรมการบริหาร
ทัศนวิสัยแรกเริ่มและวัตถุประสงค์ที่คณะทำงานจัดทาขึ้นควรจะได้รับการสื่อสารไปยังและหารือกับผู้บริหารระดับสูงและคณะกรรมการบริหาร หรือคณะกรรมการตรวจสอบ และหารือกับฝ่ายที่เกี่ยวข้องกับ GRC อื่นๆ ด้วย

3. ระบุโอกาสเบื้องต้น
คณะทำงานควรจะระบุสิ่งที่มีโอกาสำหรับการนำมาปรับปรุงแก้ไขในเบื้องต้น (initial opportunities) ที่เกี่ยวข้องกับ GRC หลายแห่งจะเริ่มจากการทบทวนกระบวนการด้านการสื่อสาร การแบ่งปันองค์ความรู้ หรือการประเมินความเสี่ยง เป็นต้น

4. พัฒนาแผนงานโครงการเบื้องต้น
พัฒนาแผนงานในรายละเอียดเพื่อดาเนินโครงการในเบื้องต้น รวมถึงในแผนงานควรมีกลไกรับฟังผลตอบรับ (feedback mechanism) ด้วยเช่นกัน

5. ยกร่างนโยบายด้านความเสี่ยง
นโยบายด้านความเสี่ยงขององค์กรเป็นองค์ประกอบสาคัญของการเริ่ม GRC การพัฒนานโยบายจะต้องทาด้วยความรอบคอบ และต้องมีบุคคลที่เหมาะสมเข้ามาเกี่ยวข้องเพื่อให้มีมุมมองทั้งด้านกฎหมาย ด้านเทคนิค และบรรษัทภิบาลที่เหมาะสม

การนำ GRC มาใช้ในทางปฏิบัติ

ตัวอย่างที่ 3 : ศาสตราจารย์ มหาวิทยาลัยเดอพอล USA ได้ศึกษาและเสนอแนวทางที่มี 10 กระบวนการในการนำ GRC มาใช้ (ต่อ)

6. ดำเนินการตามแผนงานโครงการเบื้องต้น
ต้องมีการนิยามจุดวัดและปัจจัยความสำเร็จ และพัฒนากระบวนการเพื่อนำไปสู่การดำเนินการดังกล่าว ในขั้นตอนนี้ ควรดำเนินตามกลไกรับฟังผลตอบรับ

7. ทบทวนวิสัยทัศน์และแผนงานโครงการ
ในชั้นนี้ คณะทำงานคงจะมีประสบการณ์จากการปฏิบัติงานและได้ผลลัพธ์ที่เพียงพอจากโครงการเบื้องต้นแล้ว จากนี้ คณะทำงานจะต้องจัดการประชุมร่วมกันเพื่อประเมินวิสัยทัศน์ เป้าหมาย และวิธีการดำเนินการด้าน GRC อีกครั้ง โดยอาศัยประสบการณ์ที่ผ่านมา

8. สรุปนโยบายด้านความเสี่ยงของคณะกรรมการบริหาร
สรุปสุดท้ายนโยบายด้านความเสี่ยงของคณะกรรมการบริหาร รวมถึง วิสัยทัศน์ด้าน GRC และเป้าหมาย โดยอาศัยผลลัพธ์จากการประเมินผลรอบใหม่ของคณะทำงาน

9. เห็นชอบนโยบายด้านความเสี่ยงและโครงสร้าง GRC
การเห็นชอบจากคณะกรรมการบริหารและคณะกรรมการตรวจสอบอย่างเป็นทางการ

10. นำแผนโครงการสุดท้ายมาปฏิบัติ
เมื่อแผนสุดท้ายเสร็จสิ้น รวมทั้ง นโยบายและโครงสร้างด้านความเสี่ยงได้รับการเห็นชอบ องค์กรก็ควรจะเริ่มต้นนำแผนนั้นมาปฏิบัติให้บรรลุวิสัยทัศน์ที่ตั้งไว้