The Stock Exchange of Thailand

CGForum #3/2016

ทุจริตในองค์กร ภัยมืดที่ป้องกันและควบคุมได้

การบริหารความเสี่ยงจากการทุจริต

วันที่ 24 สิงหาคม 2559
ณ หอประชุมศาสตราจารย์สังเวียน อินทรวิชัย
ตลาดหลักทรัพย์แห่งประเทศไทย (แห่งใหม่ – ข้างสถานทูตจีน)

โดย เมธา สุวรรณสาร / CGEIT; CRISC; CRMA; CIA; CPA
กรรมการอิสระและกรรมการตรวจสอบ บริษัท ศรีอยุธยา แคปปิตอล จำกัด (มหาชน)
อุปนายกสมาคม Information Systems Audit and Control Association – Bangkok Chapter

www.itgthailand.com
e-mail : suvanasarn@gmail.com

Metha Suvanasarn Profile

CGEIT; CRISC; CRMA ; CIA; CPA

ปัจจุบัน... (พ.ค. 2559)

- อนุกรรมการตรวจสอบของ มูลนิธิขาเทียมในสมเด็จพระศรีนครินทรา บรมราชชนนี
- ประธานกรรมการตรวจสอบคณะเศรษฐศาสตร์ มหาวิทยาลัยเชียงใหม่
- กรรมการอิสระและกรรมการตรวจสอบ ประธานกรรมการสรรหาและกำหนดผลตอบแทน บริษัท ศรีอยุธยาประกันภัย จำกัด (มหาชน)
- กรรมการอิสระและกรรมการตรวจสอบ ประธานกรรมการสรรหาและกำหนดผลตอบแทน บริษัท ศรีอยุธยา เจอเนอรัล ประกันภัย จำกัด
- อุปนายกสมาคม ISACA (Information Systems Audit and Control Association) Bangkok Chapter
- อุปนายกสมาคม ความมั่นคงปลอดภัยระบบสารสนเทศ (TISA – Thailand Information Security Association)
- กรรมการสรรหาและ กำหนดผลตอบแทนของ ธพว.
- ผู้บรรยาย ทางด้าน GEIT; Corporate Governance, IT Governance, การบริหารความเสี่ยง, การควบคุมและการตรวจสอบภายในตามฐานความเสี่ยง การตรวจสอบด้านคอมพิวเตอร์ / IT Audit, IT Audit for Non-IT Auditor และ การกำกับ-การควบคุม และการตรวจสอบการทุจริตฯลฯ ให้กับหลายหน่วยงาน
- ผู้เขียนบทความต่าง ๆ ที่เกี่ยวข้องกับ การประยุกต์ใช้ การนำไปปฏิบัติ ในเรื่อง GEIT, Corporate Governance, IT Governance, GRC ,CSA , การบริหารความเสี่ยง, การควบคุมและการตรวจสอบภายในตามฐานความเสี่ยง, การตรวจสอบด้านคอมพิวเตอร์/ สารสนเทศ, IT Audit, การตรวจสอบแบบบูรณาการ / Integrated Audit by Integrated Auditors และอื่นๆ เช่น การขียน เรื่อง Digital Economy , การสร้างความเชื่อและ การเติบโตอย่างยั่งยืน ในปัจจุบัน โดยเผยแพร่ส่วนใหญ่ที่สมาคมผู้ตรวจสอบภายในแห่งประเทศไทย (สตท) และ ในเว็บไซต์เพื่อสังคมแห่งการเรียนรู้ที่ www.itgthailand.com และ www.itgthailand.wordpress.com

Metha Suvanasarn Profile

การทำงานในอดีต

- ผู้อำนวยการอาวุโส ฝ่ายเทคโนโลยีสารสนเทศ และการสื่อสาร ธปท และ ผู้อำนวยการอาวุโส สำนักงาน ธปท ภาคตะวันออกเฉียงเหนือ ฯลฯ
- ผู้เชี่ยวชาญด้าน IT Examination ของ ธปท.
- กรรมการบริหารความเสี่ยงหอการค้าไทย
- ที่ปรึกษาการทำวิทยานิพนธ์ปริญญาเอก เรื่อง Integrated GRC ให้กับอาจารย์มหาวิทยาลัยเชียงใหม่ (ปี พ.ศ. 2556 – 2557)
- ที่ปรึกษาสมาคมผู้ตรวจสอบภายในแห่งประเทศไทย (สตท.) (ปี พ.ศ. 2555-2556)
- กรรมการวิชาการมาตรฐานการรักษาความมั่นคงในการประกอบธุรกรรมทาง อิเล็กทรอนิกส์ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (NECTEC – National Electronics and Computer Technology Center) (ปี พ.ศ. 2554 – 2555)
- อนุกรรมการประเมินผลการดำเนินงานรัฐวิสาหกิจ (ปี พ.ศ. 2547- 2555)
- อนุกรรมการปรับปรุงระบบประเมินผลการดำเนินงานรัฐวิสาหกิจ (ปี พ.ศ. 2553 – 2554)
- อุปนายกสมาคมผู้ตรวจสอบภายในแห่งประเทศไทย (ปี พ.ศ. 2553 – 2554)
- คณะอนุกรรมการประเมินบริหารความเสี่ยงรัฐวิสาหกิจ (ปี พ.ศ. 2547 – 2555)
- ประธานกรรมการสรรหาและกำหนดผลตอบแทน, กรรมการอิสระและกรรมการตรวจสอบ ธนาคารไทยเครดิต (ปี พ.ศ. 2555)
- กรรมการตรวจสอบ บลจ. ธนชาติ (ปี พ.ศ. 2550 – 2551)
- ประธานกรรมการตรวจสอบและที่ปรึกษา สำนักงานส่งเสริมอุตสาหกรรมซอร์ฟแวร์แห่งชาติ (SIPA) (ปี พ.ศ. 2546 – 2549)
- กรรมการอิสระ กรรมการตรวจสอบ และกรรมการบริหารความเสี่ยง การไฟฟ้านครหลวง – กฟน. (ปี พ.ศ. 2543 – 2546)
- ประธานกรรมการตรวจสอบ ธนาคารเพื่อการเกษตรและสหกรณ์การเกษตร – ธกส. (ปี พ.ศ. 2543 – 2544)
- เป็นหัวหน้าคณะผู้แทนของไทย (Thailand Representative) ในการประชุมที่องค์การสหประชาชาติที่ New York ประเทศสหรัฐอเมริกา ในปี 2532 เรื่อง Draft Model Rules on Electronic Funds Transfer ที่ UN จัดให้มีขึ้นเป็นครั้งแรก
- ประธานกรรมการ บริษัทเครดิตฟองซิเอร์สากลสยาม จำกัด
- ประธานคณะทำงานพิจารณากำหนดรายการและความหมายของรายการในงบดุลและบัญชีกำไร ขาดทุนของบริษัทมหาชนที่ประกอบธุรกิจเงินทุน ธุรกิจหลักทรัพย์ ธุรกิจเงินทุนและหลักทรัพย์ และธุรกิจเครดิตฟองซิเอร์
- ประธานคณะทำงานด้านเศรษฐกิจและการเงินจังหวัดขอนแก่นในการเชื่อมความสัมพันธ์กับเมืองหนานหนิง ประเทศจีน ปี พ.ศ. 2537
- หัวหน้าคณะทำงานศึกษาปัญหาการค้าชายแดนไทย-ลาว ปี พ.ศ. 2537
- รองประธานคณะอนุกรรมการพิจารณาผลตอบแทนและความเสี่ยงของบริษัทเงินทุนและสถาบันการเงิน

Metha Suvanasarn Profile

การทำงานในอดีต และการปรับปรุงระบบงาน (ต่อ)

- กรรมการที่ปรึกษาของสมาคมผู้ตรวจสอบงานคอมพิวเตอร์ ภาคพื้นกรุงเทพฯ (EDPPA – Bangkok Chapter) ปัจจุบัน เปลี่ยนชื่อเป็น ISACA
- อนุกรรมการสอบบัญชีกิจการที่ใช้คอมพิวเตอร์ กบ.ช.
- อนุกรรมการมารยาทผู้สอบบัญชีรับอนุญาต กบ.ช.
- ที่ปรึกษาของสมาคมผู้ตรวจสอบงานคอมพิวเตอร์ภาคพื้นกรุงเทพฯ (Information Systems Audit and Control Association (ISACA) – Bangkok Chapter)
- รองประธานกรรมการสหกรณ์ออกทรัพย์พนักงานธนาคารแห่งประเทศไทย
- ที่ปรึกษาด้านการเงินและการบัญชีสหกรณ์อมทรัพย์พนักงานธนาคารแห่งประเทศไทย
- กรรมการพัฒนาจังหวัดขอนแก่น (กพจ.)
- กรรมการพัฒนาเทศบาลนครขอนแก่น
- ที่ปรึกษากิตติมศักดิ์โครงการศึกษาและจัดทำแผนลงทุนจังหวัดขอนแก่น กาฬสินธุ์ มหาสารคาม และหนองบัวลำภู
- ที่ปรึกษาคณะกรรมการศึกษารูปแบบการบริการวิชาการของมหาวิทยาลัยขอนแก่น
- คณะทำงานศึกษาศักยภาพและแนวทางการพัฒนาเพื่อกระจายความเจริญสู่ภูมิภาค จังหวัดขอนแก่น
- กรรมการผู้ทรงคุณวุฒิประจำศูนย์บริการวิชาการ มหาวิทยาลัยขอนแก่น
- กรรมการชุดต่าง ๆ ในธนาคารแห่งประเทศไทย
  - กรรมการคณะทำงานแผนสำรวจฉุกเฉินเพื่อรองรับปัญหาปี ค.ศ. 2000
  - กรรมการคณะทำงานแก้ไขปัญหาปี ค.ศ. 2000 งานด้านเทคโนโลยีสารสนเทศ
  - กรรมการคณะทำงานแก้ไขปัญหาปี ค.ศ. 2000 ด้าน Non-IT
  - กรรมการคณะทำงานกำกับตรวจสอบการแก้ไขปัญหาปี ค.ศ. 2000 ของ ธปท.
  - กรรมการคอมพิวเตอร์
  - กรรมการคณะทำงานปรับปรุงข้อมูล ฐานข้อมูล และระบบข้อมูลของธนาคารแห่งประเทศไทย
  - กรรมการบริหารและประสานงานสาขาภาค
  - กรรมการพัฒนาสถาบันการเงิน
  - กรรมการเกี่ยวกับเอกสารและระบบของเอกสารของธนาคารแห่งประเทศไทยที่สถาบันการเงินต้องปฏิบัติ
  - กรรมการระบบการชำระเงิน
  - กรรมการ โครงการพัฒนาระบบห้องค้าเงินฝ่ายการธนาคาร กรรมการการสื่อสารภายในธนาคาร

หัวข้อการเสวนา

- การเปลี่ยนแปลงสภาพแวดล้อมที่มีผลกระทบต่อ บทบาทและความรับผิดชอบของคณะกรรมการและผู้บริหาร ที่มีผลต่อการบริหารความเสี่ยง และการทุจริต
- ปัจจัยเอื้อและหลักการบริหารยุคใหม่ ที่มีผลต่อการบริหารความเสี่ยงและการทุจริต
- GEIT – Governance of Enterprise IT และการบริหารความเสี่ยงยุคใหม่กับองค์กร
- การทุจริตกับการควบคุมภายในและการตรวจสอบแบบบูรณาการ
- การตรวจสอบ การร้องเรียน และการควบคุมการทุจริต
- Monitoring for Behavior Audit and Integrated Management / Controls
- การปฏิบัติหน้าที่ด้วยความไว้วางใจ / Fiduciary Duty ของคณะกรรมการและผู้บริหาร
- การบริหารความเสี่ยงกับการทุจริต ตามแนวทางของ COSO 2013
- สรุป ถาม-ตอบ

ความหมายของการทุจริต

การทุจริต

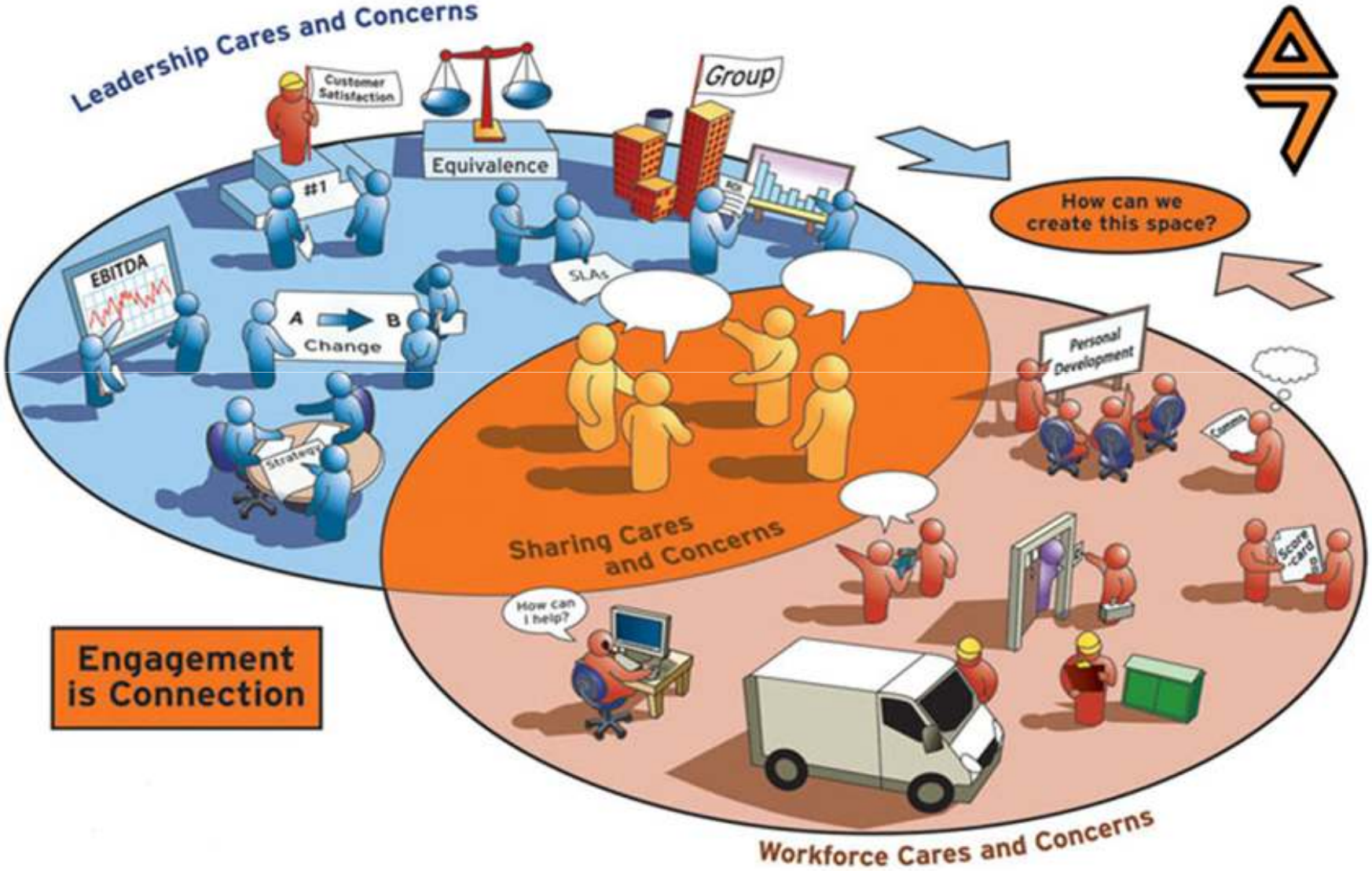
คือ การกระทำใด ๆ ไม่ว่าจะใช้วิธีที่ไม่ใช้คอมพิวเตอร์ หรือ วิธี Manual หรือใช้เทคโนโลยีสารสนเทศ หรือผสมผสานกันไป ซึ่งมีกฎหมายหรือ ระเบียบ แนวการปฏิบัติที่ระบุว่า เป็น

- การฉ้อฉล
- การหลอกลวง
- การปกปิด
- การละเมิดอำนาจหน้าที่ตามความรับผิดชอบหรือจรรยาบรรณในการปฏิบัติงานที่ดี
- การกระทำที่เกิดขึ้นโดยปราศจากการข่มขู่บังคับหรือมีเหตุบีบคั้นจากผู้อื่น
- การกระทำของบุคคล กลุ่มบุคคล หรือองค์การ เพื่อให้ได้มาซึ่งทรัพย์สินเงินทอง หรือข้อมูลหรือบริการพิเศษ เช่น การเพิกเฉย ละเลย การจ่ายเงินหรือให้บริการ เป็นต้น
- การกระทำเพื่อก่อให้เกิดผลประโยชน์ส่วนตัวหรือผู้อื่น หรือเอื้อผลประโยชน์ต่อธุรกิจอื่น ซึ่งเป็นความขัดแย้งในเรื่องผลประโยชน์ ไม่ว่าจะทางตรงหรือทางอ้อม

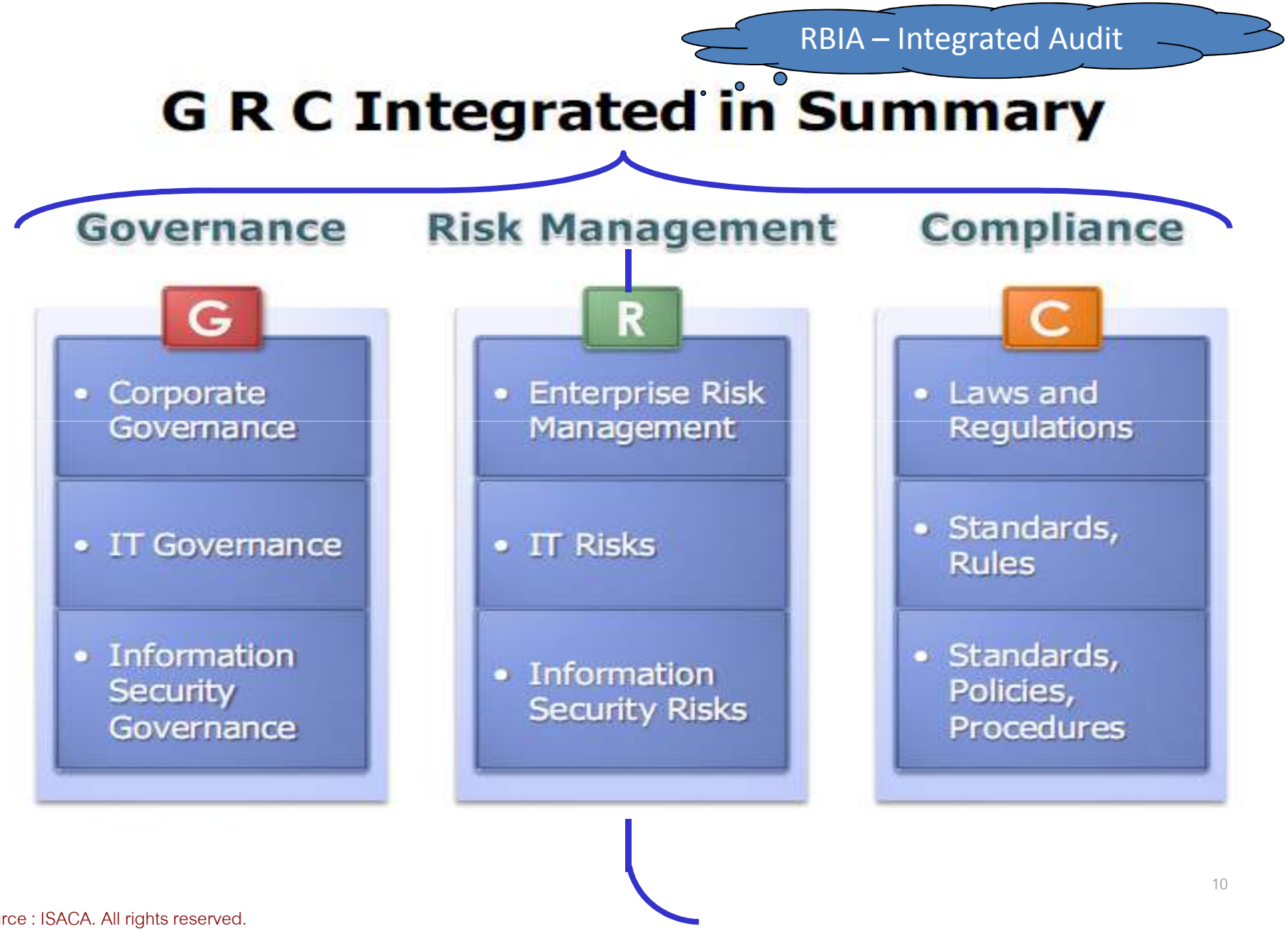
Attitude & Key Success Factors

การโยงใยและความสัมพันธ์ของ
การกำกับดูแลกิจการที่ดีกับการบริหารความเสี่ยงขององค์กร

ความสัมพันธ์ของธุรกิจกับ เทคโนโลยีสารสนเทศ กับ ความเสี่ยง

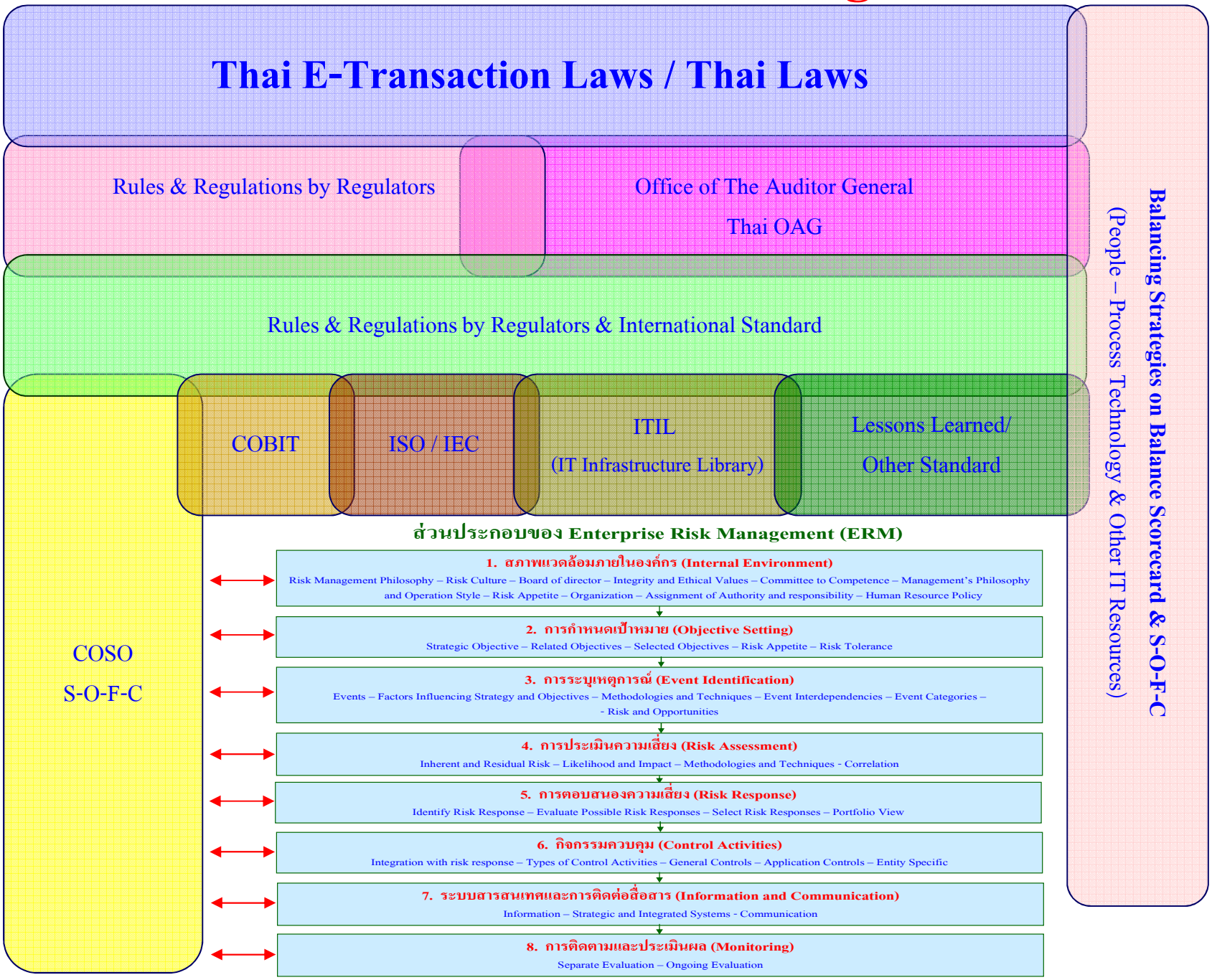


GRC IN COBIT5 & SINGLE UMBRELLA MANAGEMENT & AUDIT



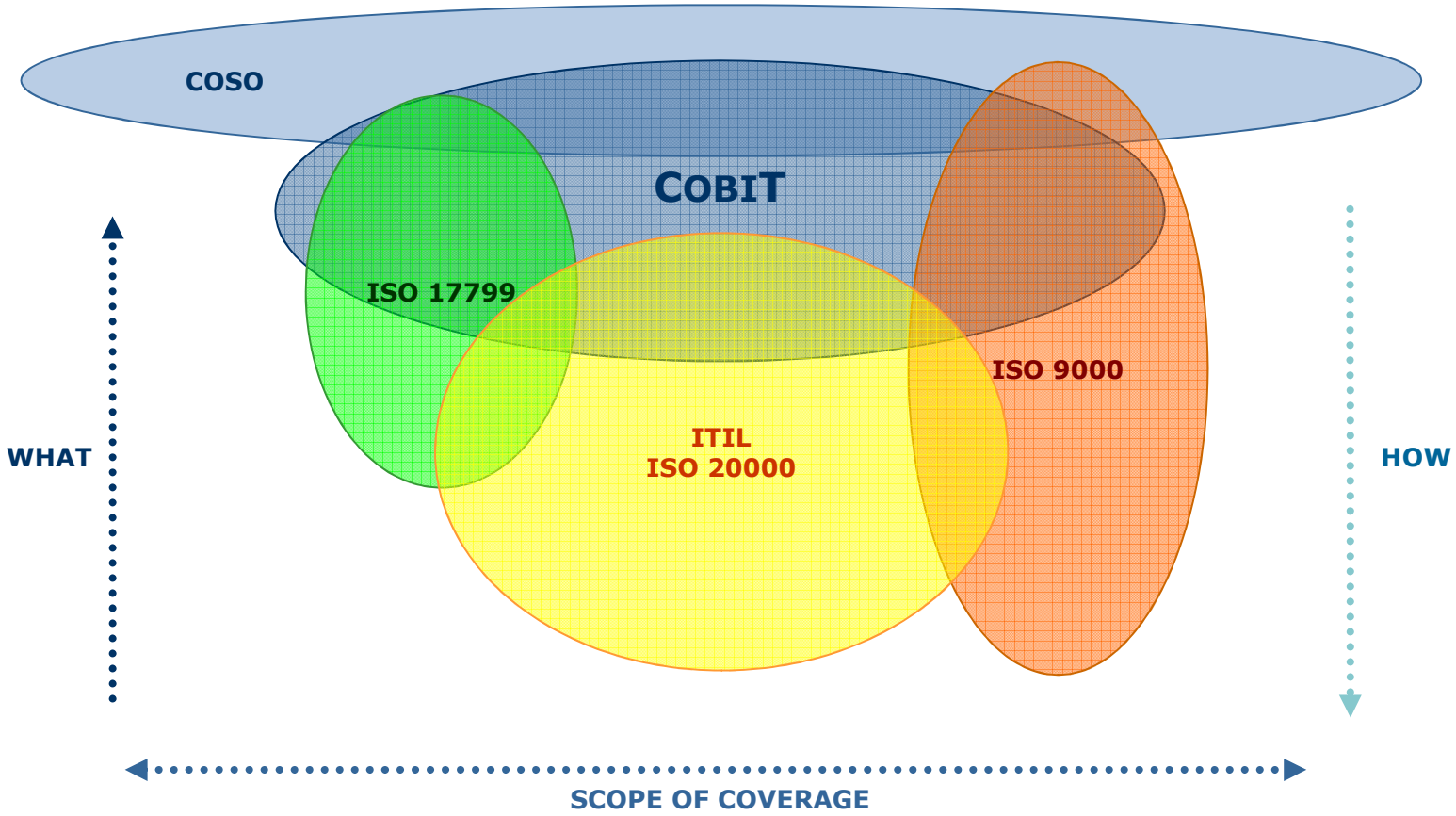
10

IT Governance & GRC + Risk Convergence Framework



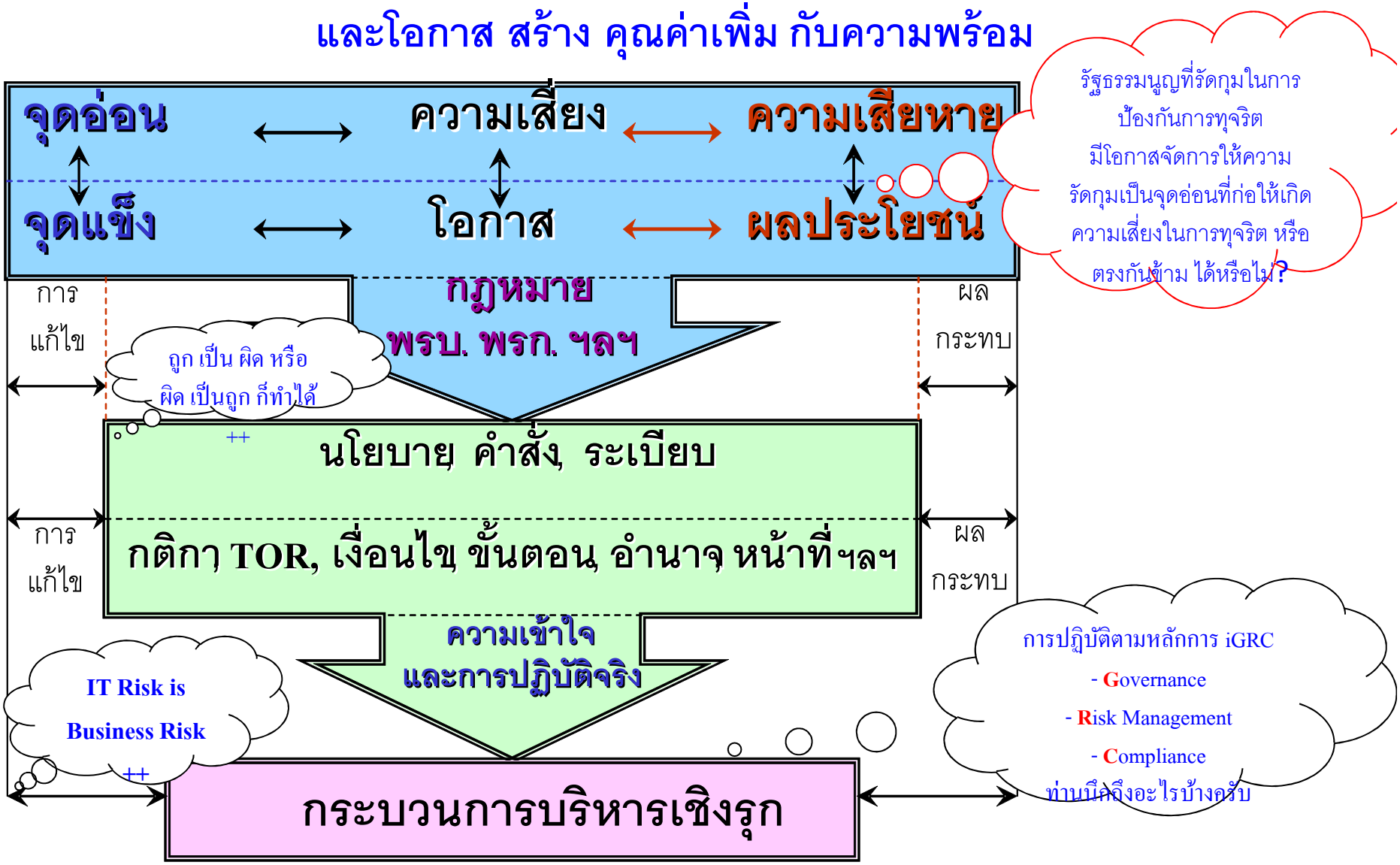
COBIT – Control Objectives for Information & Related Technology and Other IT Risk / Management

Organisations will consider and use a variety of IT models, standards and best practices. These must be understood in order to consider how they can be used together, with COBIT acting as the consolidator ('umbrella').



Source: ITGI

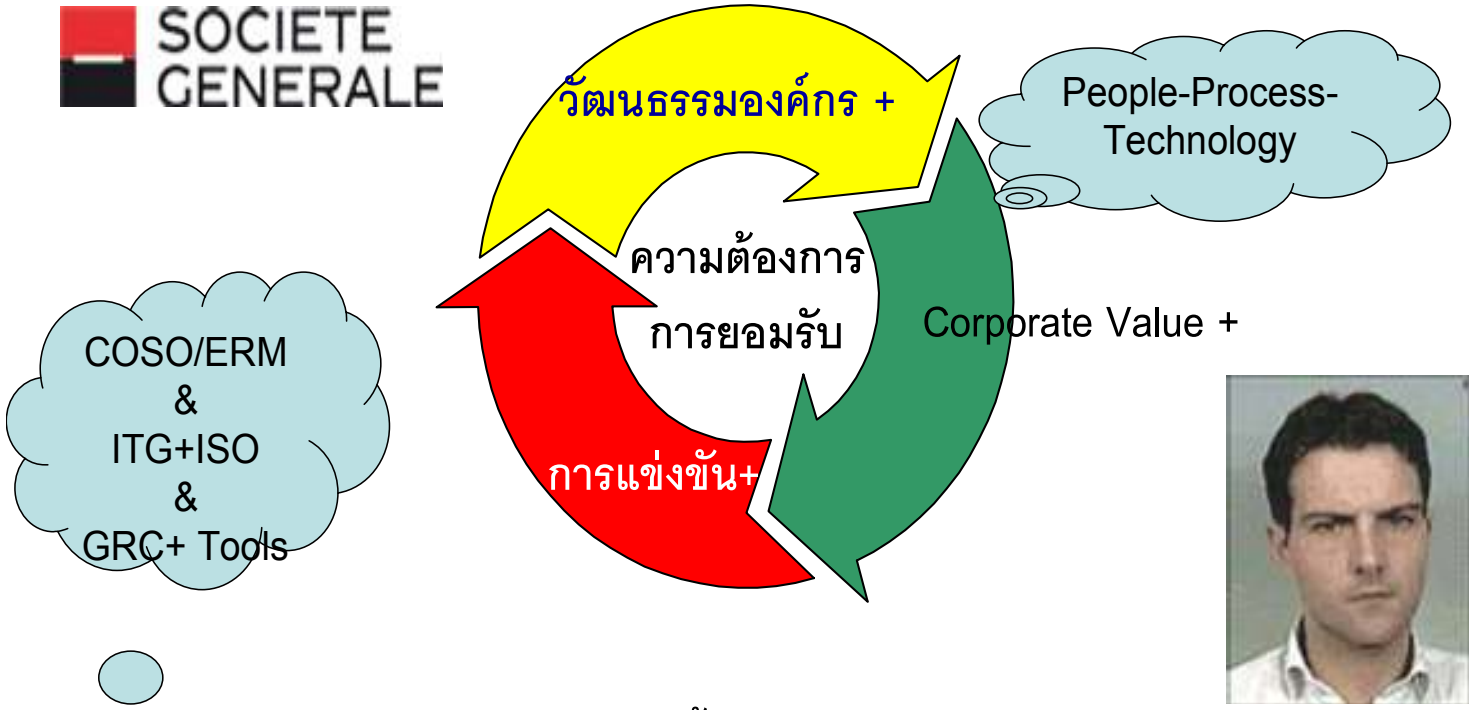
X-Ray ความรู้เท่าทันในการบริหารความเสี่ยงกับข้อมูลการปฏิบัติที่ไม่เหมาะสม / การประพฤติมิชอบ การทุจริตตามระเบียบ ความเสียหาย กับ Whistleblowing และโอกาส สร้าง คุณค่าเพิ่ม กับความพร้อม



GRC : Value Creation & Lesson Learned

บทเรียน จากการ ทุจริต 340,000.00 ล้านบาท ทางด้าน IT Risk

ของธนาคาร โซซิเอเต้ เจเนอราล [Soc Gen]/ ฝรั่งเศส/ Jan.08



❖ความรู้ ความเข้าใจในกระบวนการ / ขั้นตอน ระบบงาน การตรวจสอบและ การควบคุมภายใน + ของนาย Kerviel ผู้บริหาร และ คณะกรรมการต่างๆ

ร่วมกันทบทวน กำหนด นโยบาย กลยุทธ กระบวนการทำงาน++ จากบทเรียนนี้

ความรับผิดชอบของ Board ต่อ Governance และความรับผิดชอบของผู้บริหารในเรื่อง Management

E - D- M → Evaluate - Direct - Monitors

- มั่นใจในการกำหนดกรอบการดำเนินงานการกำกับดูแล และการบำรุงรักษา
- มั่นใจในการส่งมอบผลประโยชน์
- มั่นใจในความเสี่ยงที่เหมาะสม
- มั่นใจในการใช้ทรัพยากรให้ได้ประโยชน์สูงสุด
- มั่นใจในความโปร่งใสต่อผู้มีส่วนได้เสีย

จัดวางแนว จัดทำแผน และจัดระบบ / APO

- บริหารจัดการกรอบการดำเนินงานการบริหารงานด้านไอที
- บริหารจัดการกลยุทธ์
- บริหารจัดการสถาปัตยกรรมองค์กร
- บริหารจัดการนวัตกรรม
- บริหารจัดการกลุ่มของชุดโครงการ
- บริหารจัดการงบประมาณและต้นทุน
- บริหารจัดการทรัพยากรบุคคล
- บริหารจัดการความสัมพันธ์
- บริหารจัดการข้อตกลงการให้บริการ
- บริหารจัดการผู้ขายหรือผู้ให้บริการ
- บริหารจัดการคุณภาพ
- บริหารจัดการความเสี่ยง
- บริหารจัดการความมั่นคงปลอดภัย

จัดสร้าง จัดหา และนำไปใช้ / BAI

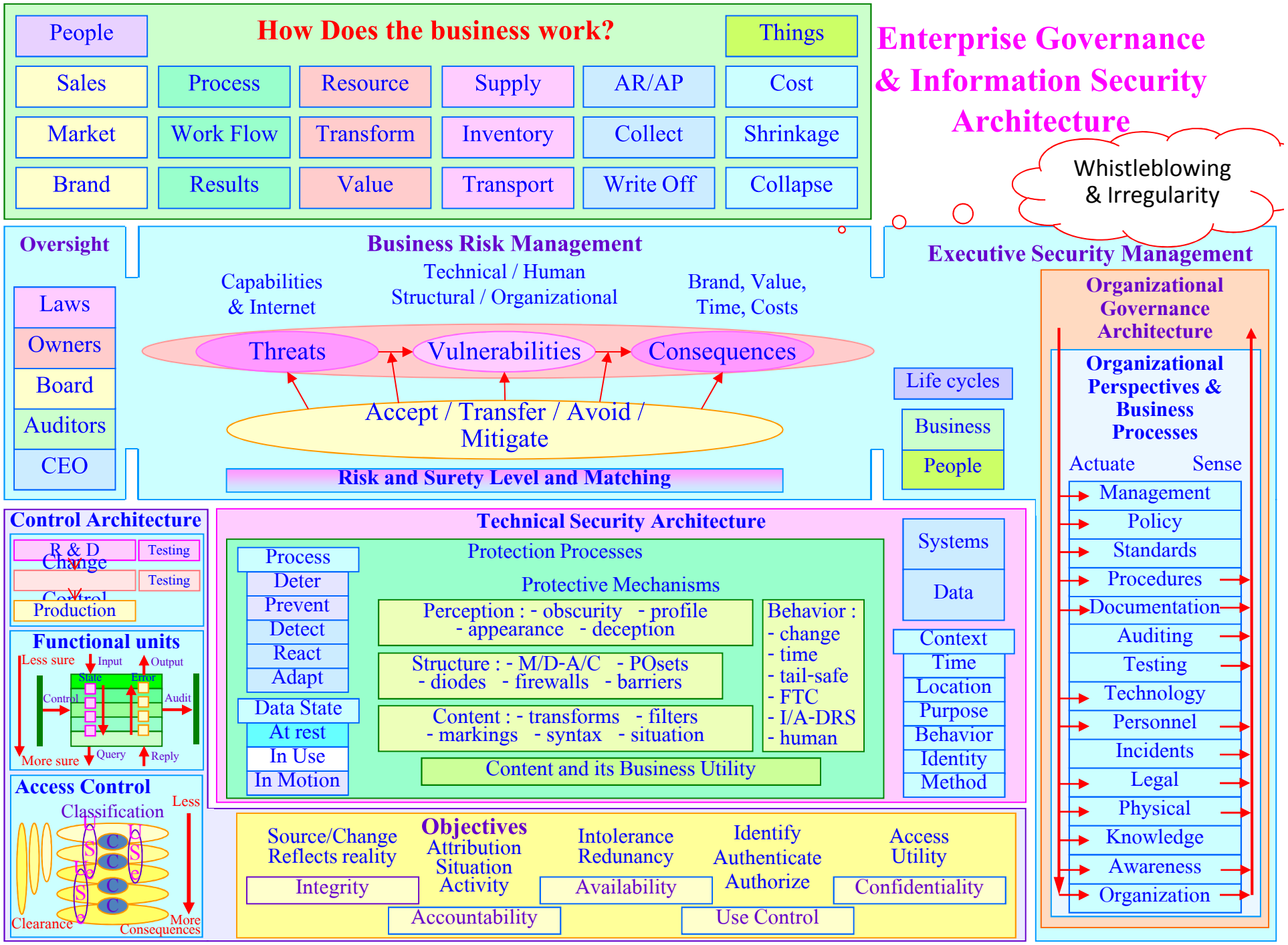
- บริหารจัดการโครงการและชุดโครงการ
- บริหารจัดการข้อกำหนดความต้องการ
- บริหารจัดการระบุและจัดสร้างกระบวนการแก้ปัญหาแบบเบ็ดเสร็จ
- บริหารจัดการความพร้อมใช้งานและจัดความสามารถ
- บริหารจัดการเพื่อให้การเปลี่ยนแปลงองค์กรสัมฤทธิ์ผล
- บริหารจัดการการเปลี่ยนแปลง
- บริหารจัดการการยอมรับการเปลี่ยนแปลงและการปรับเปลี่ยน
- บริหารจัดการความรู้
- บริหารจัดการสินทรัพย์
- บริหารจัดการองค์ประกอบของระบบ

ส่งมอบ ให้บริการ และสนับสนุน / DSS

- บริหารจัดการการปฏิบัติการ
- บริหารจัดการคำร้องขอบริการและเหตุการณ์ที่เกิดขึ้น
- บริการจัดการมีปัญหา
- บริหารจัดการความต่อเนื่อง
- บริหารจัดการบริการผ่านความมั่นคงปลอดภัย
- บริหารจัดการการควบคุมกระบวนการทางธุรกิจ

เฝ้าติดตาม วัดผล และประเมิน / MEA

- เฝ้าติดตาม วัดผล และประเมินประสิทธิภาพและความสอดคล้องในการดำเนินงาน
- เฝ้าติดตาม วัดผล และประเมินระบบการควบคุมภายใน
- เฝ้าติดตาม วัดผล และประเมินการปฏิบัติตามข้อกำหนดจากหน่วยงานภายนอก

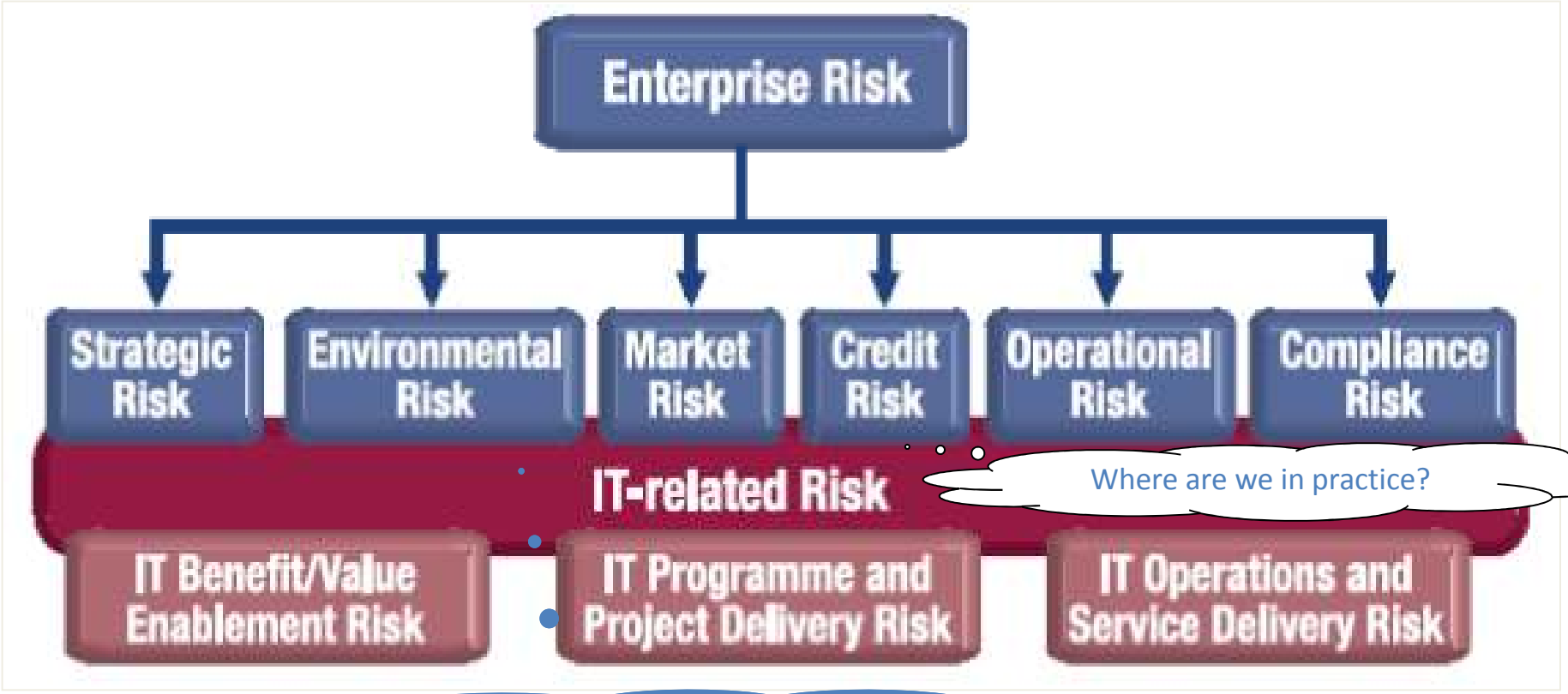


Source : IT Security Governance Guidebook / FRED COHEN

GRC in COBIT5 & Risk IT – it Impacts on Business

DEFINING A RISK UNIVERSE AND SCOPING RISK MANAGEMENT

IT Risk in the Risk Hierarchy and Risk Universe – COBIT5 / GEIT



IT Risk and COSO-ERM

Source : ISACA

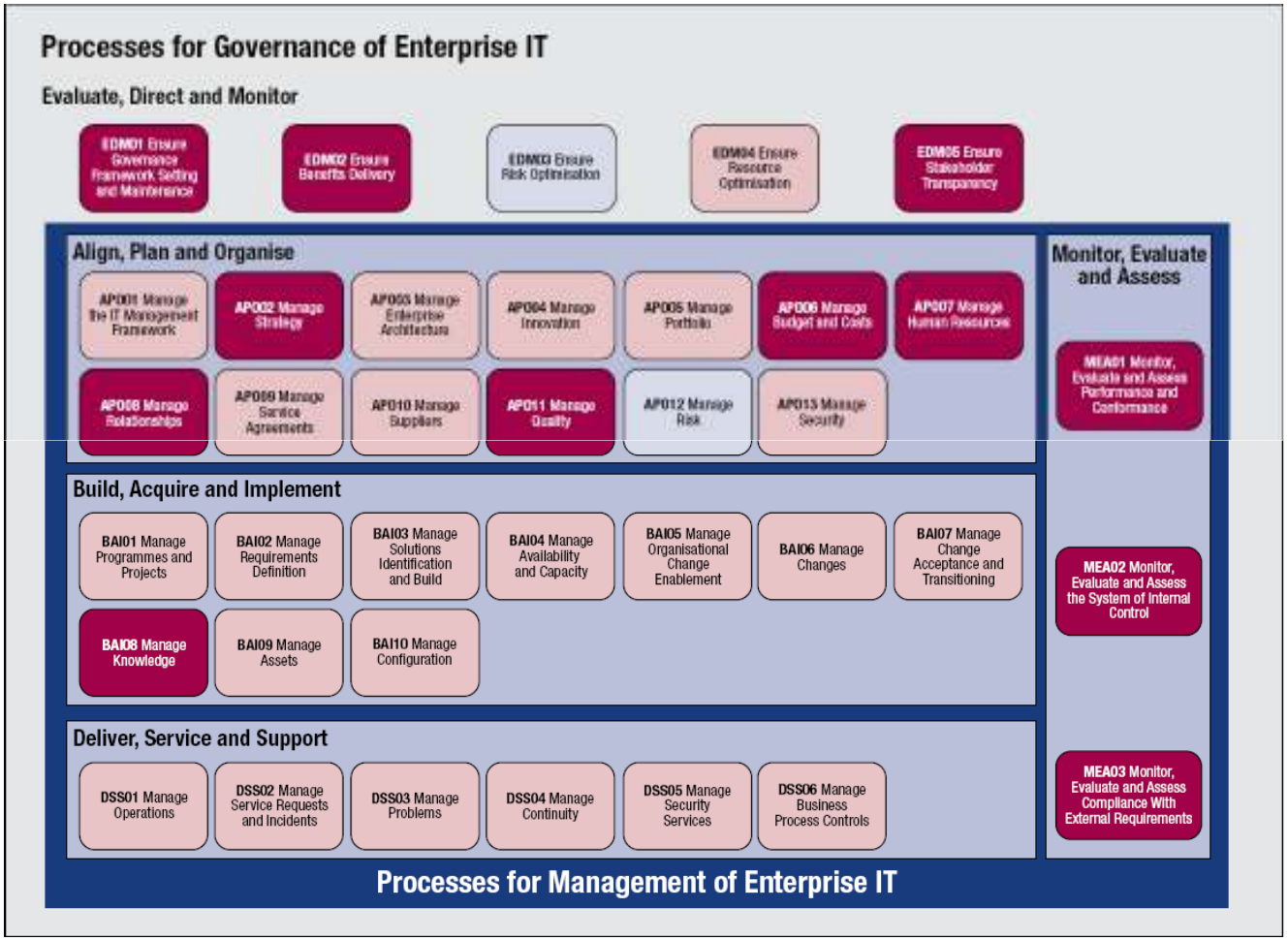
GEIT & Risk Function Perspective

COBIT 5 for Risk identifies all COBIT 5 processes that are required to support the risk function:

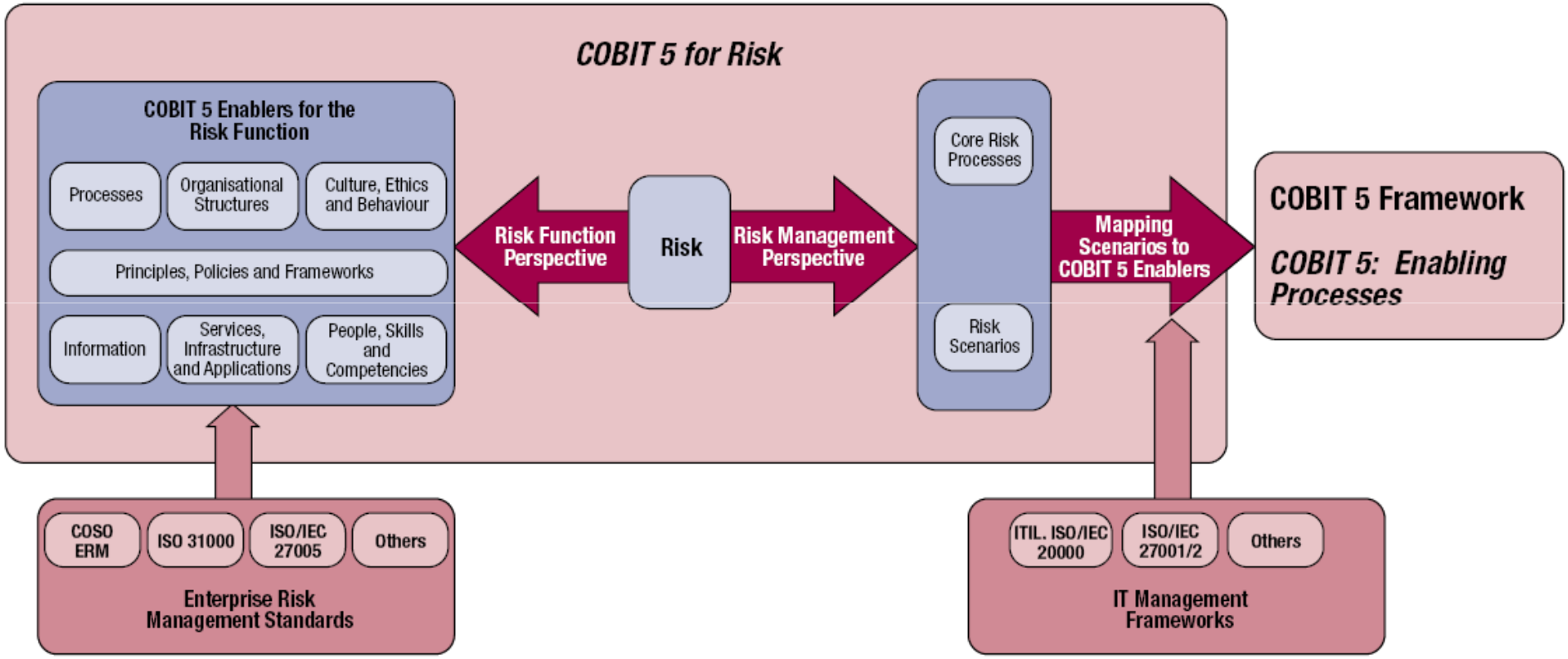
- Key supporting processes– dark pink
- Other supporting processes – light pink

Core risk processes, shown in light blue are also highlighted—these processes support the risk management perspective:

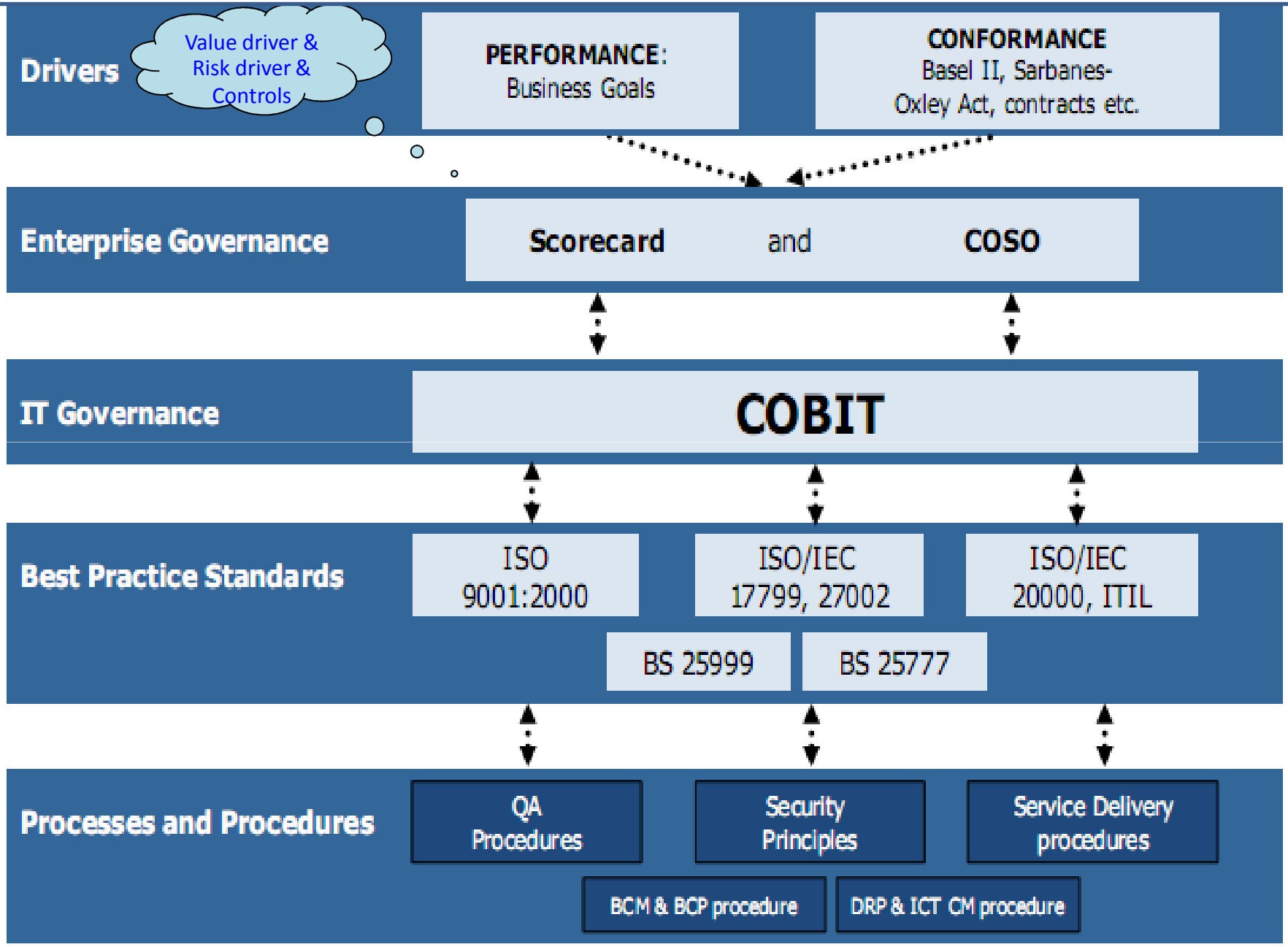
- EDM03 Ensure risk optimisation.
- APO12 Manage risk.



GEIT & Risk Perspectives

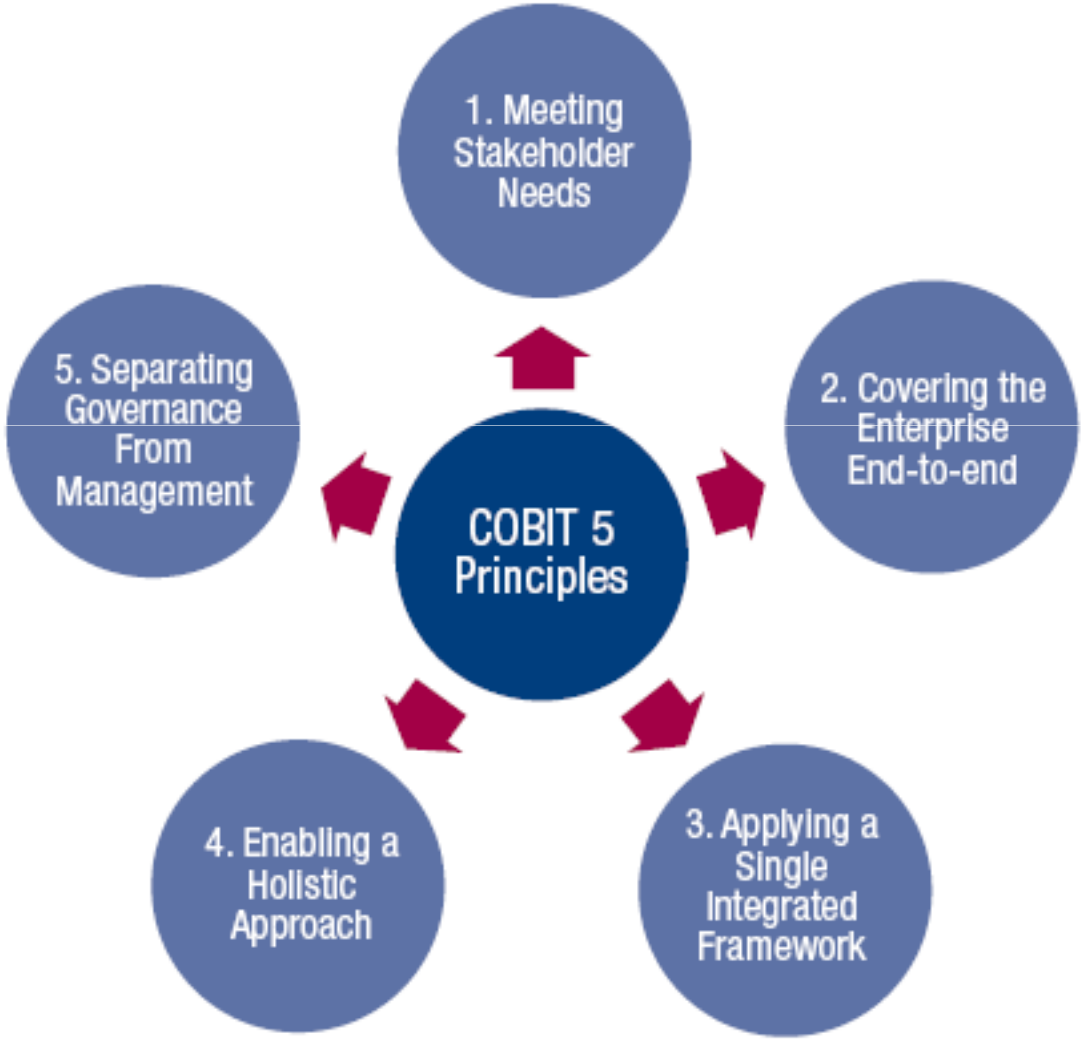


Business & IT Alignment for Better Governance and Integrated Mgmt.



Source: ITGI

COBIT 5 / GEIT – Governance of Enterprise IT Principles

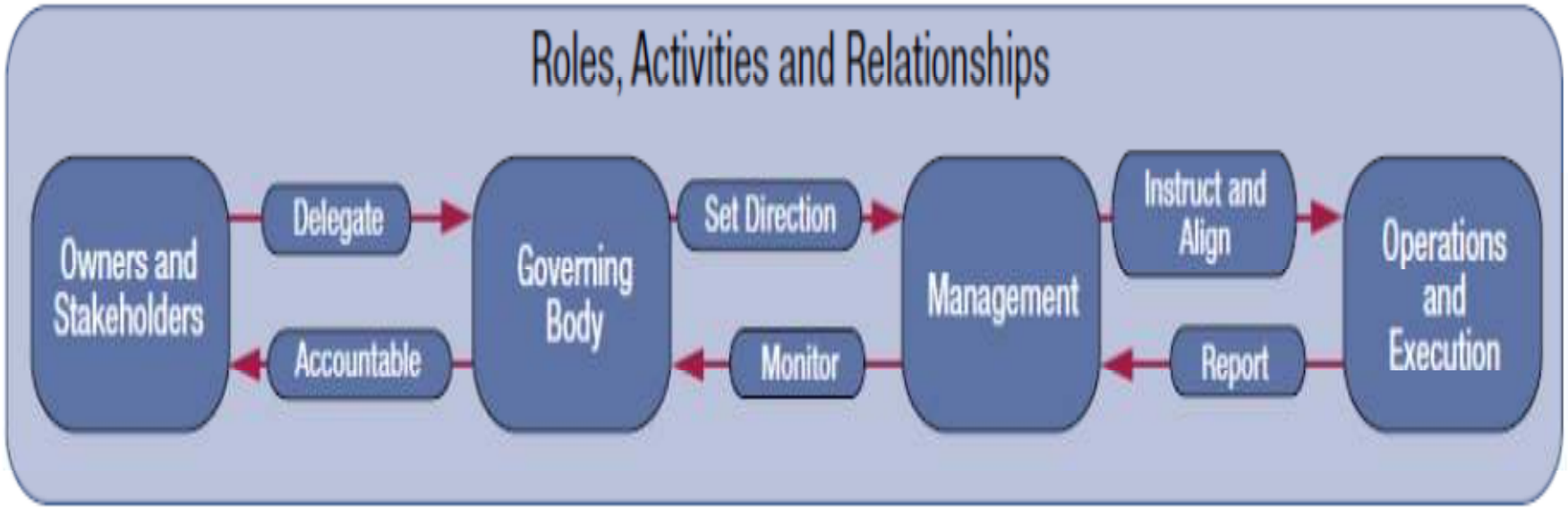


ความสำคัญของ COBIT 5 / GEIT – Governance Enterprise IT

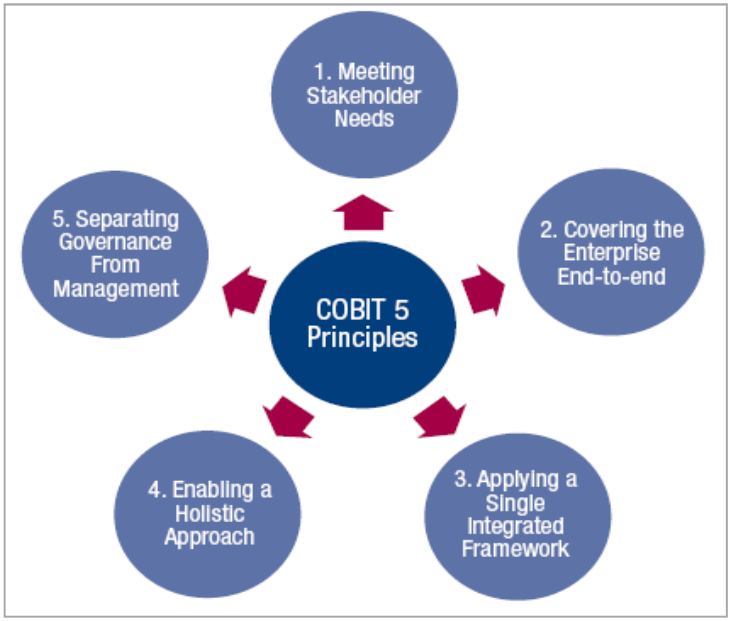
COBIT 5 คืออะไร ทำไมองค์กรต้องใช้ COBIT 5

A Business Framework for the Governance and Management of Enterprise IT

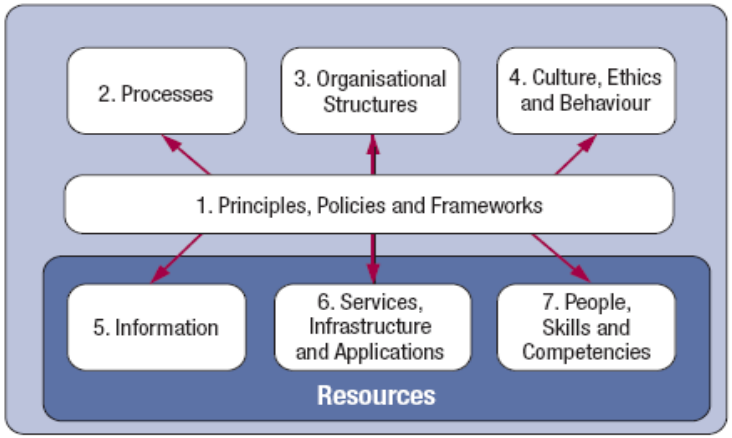
Key Roles, Activities and Relationships



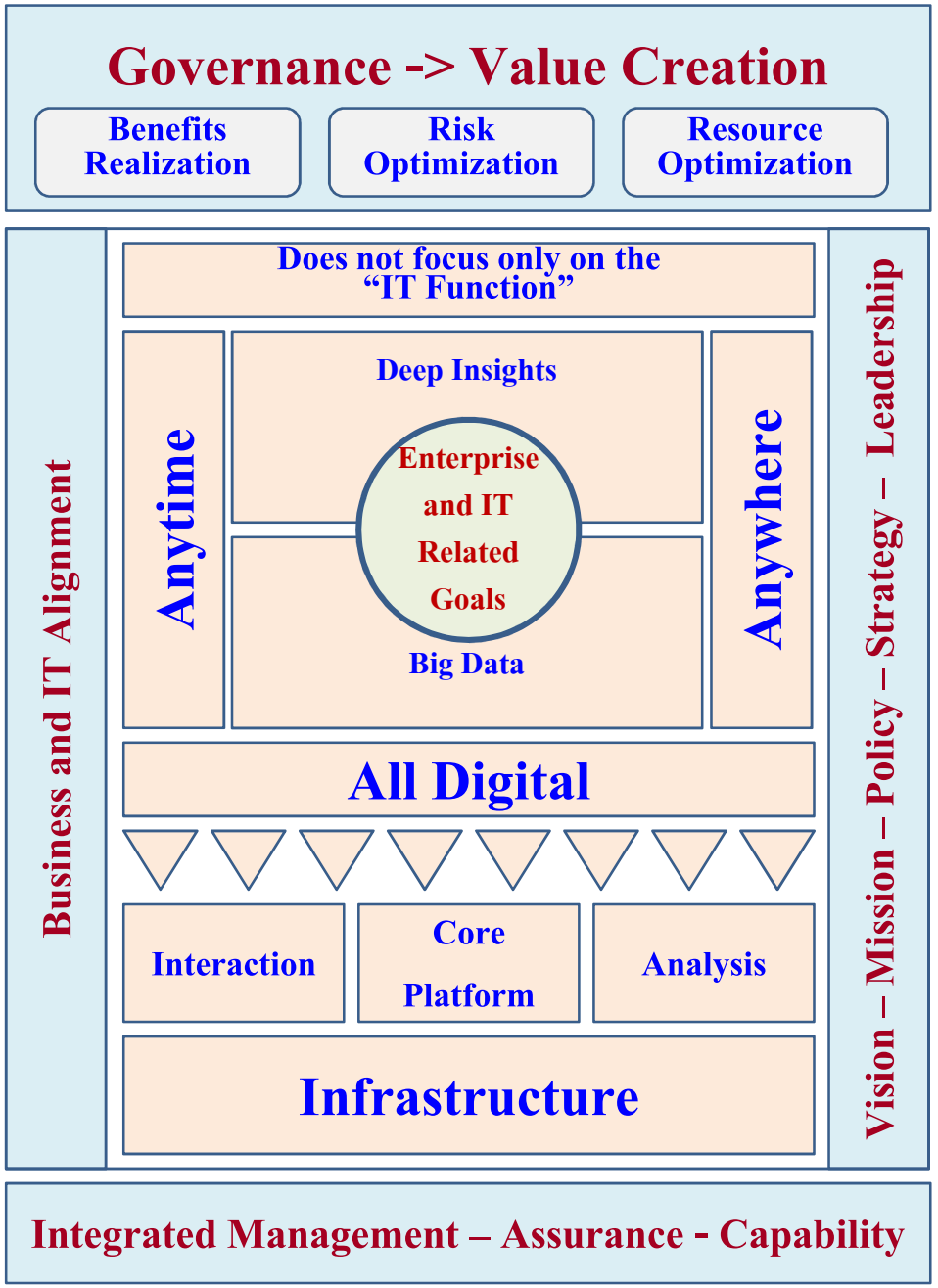
Business and Technology Architecture -> IT Risk to-be Concerned



Effective **governance** and **management** framework based on a holistic set of **seven enablers** that optimises **information** and **technology** investment and use for the benefit of **stakeholders**.

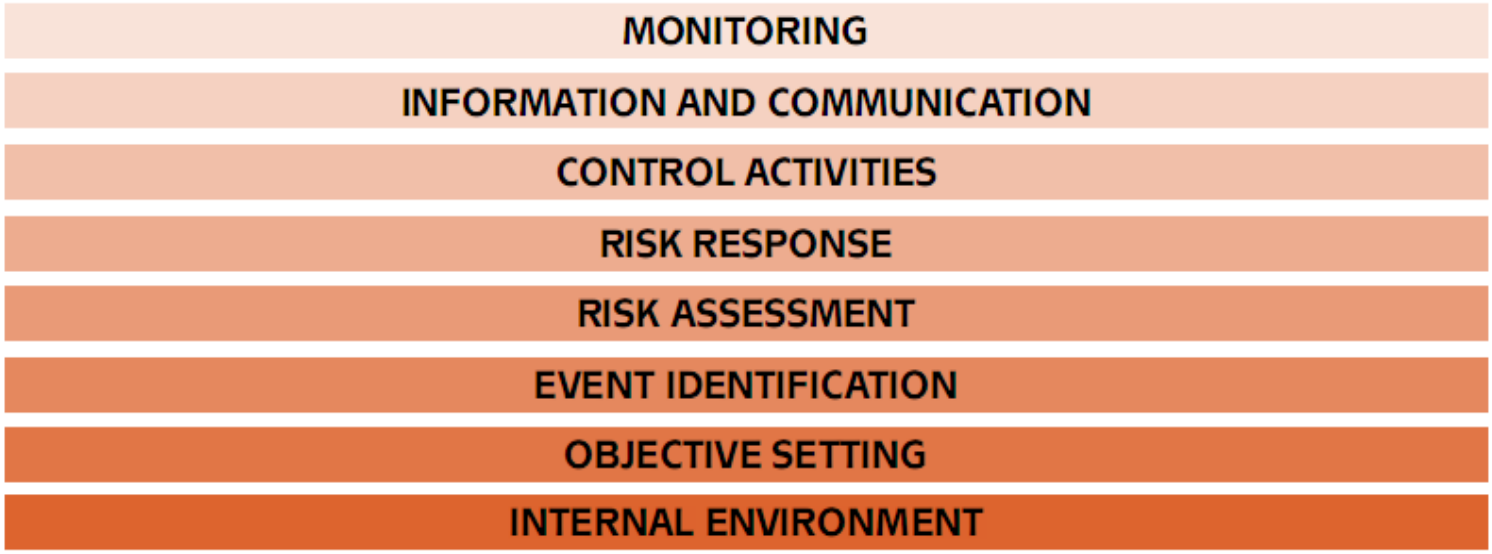


Source : ISACA. All rights reserved.



Source : www.itgthailand.com

COSO ERM Model for Risk Management and Change Management - Stakeholders



Monitoring

- Monthly performance metrics and change analysis provided to the CIO.
- Audits of change management process conducted by internal auditing.
- Annual control self-assessment (CSA) conducted by business units and the IT department.
- Periodic reports from the change management board provided to senior management.

Information and Communication

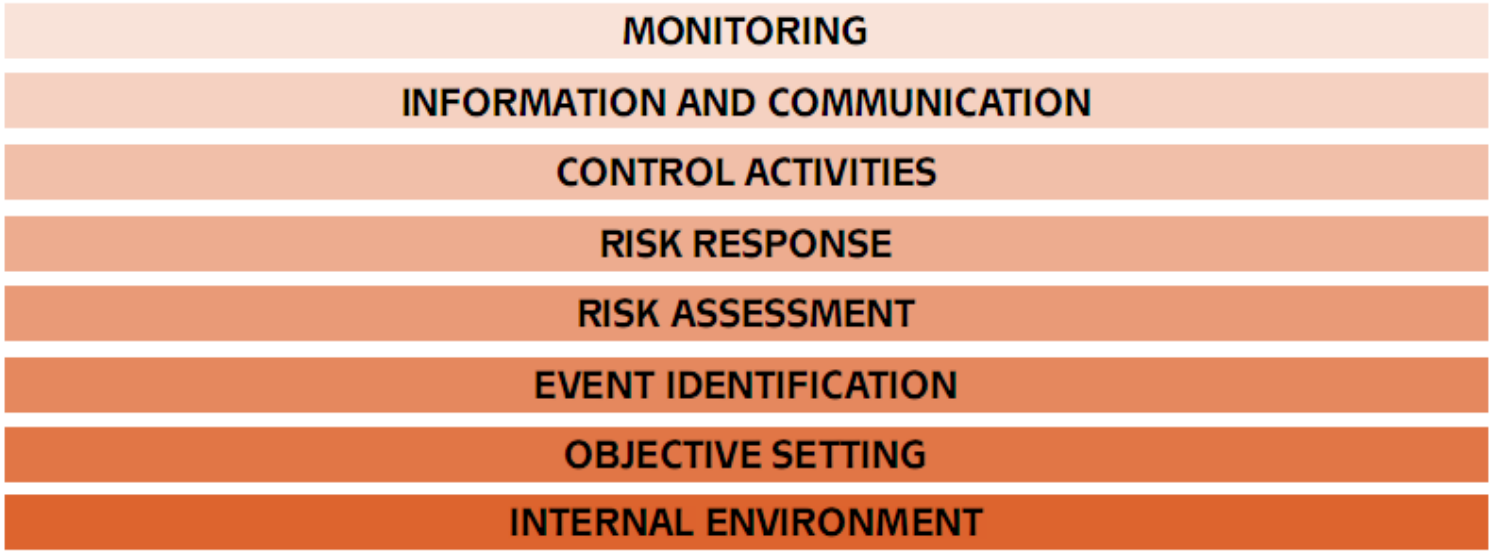
- Periodic messages from senior management that change control is important.
- Service desk issues communicated for resolution and trend analysis.
- Changes in policy communicated to all affected personnel.
- Regular communication of upcoming changes.

Control Activities

- Common process in place and documented.
- Effective change control committee structure.
- Change control log used.
- Segregation of duties between developers and technical staff maintained.
- Automated controls to enforce process of promoting changes into production.
- Automated process to return production environment to pre-change state.
- Approved configurations documented.
- Clear delegation of authority documented.
- Approvals for changes documented.
- Automated system and data backups and ability to restore from approved environment.

Source : GTAG

COSO ERM Model for Risk Management and Change Management - Stakeholders



Risk Assessment

- Firm's strategic and process-level risk assessments consider risks associated with out-of-process (unintended or unauthorized) changes.
- Risks due to change well understood by IT personnel.
- Thorough risk assessment of all proposed changes performed.
- Business continuity planning in place.
- Internal audit assessment performed.
- Business insurance needs assessment performed.
- Risk factors assessed to determine classification of the change and level of testing and approval.

Objective Setting and Event Identification

- Management establishes business objectives and strategies.
- Management establishes objectives for change management; identifies what events could prevent successful achievement of business objectives and adherence to change process.

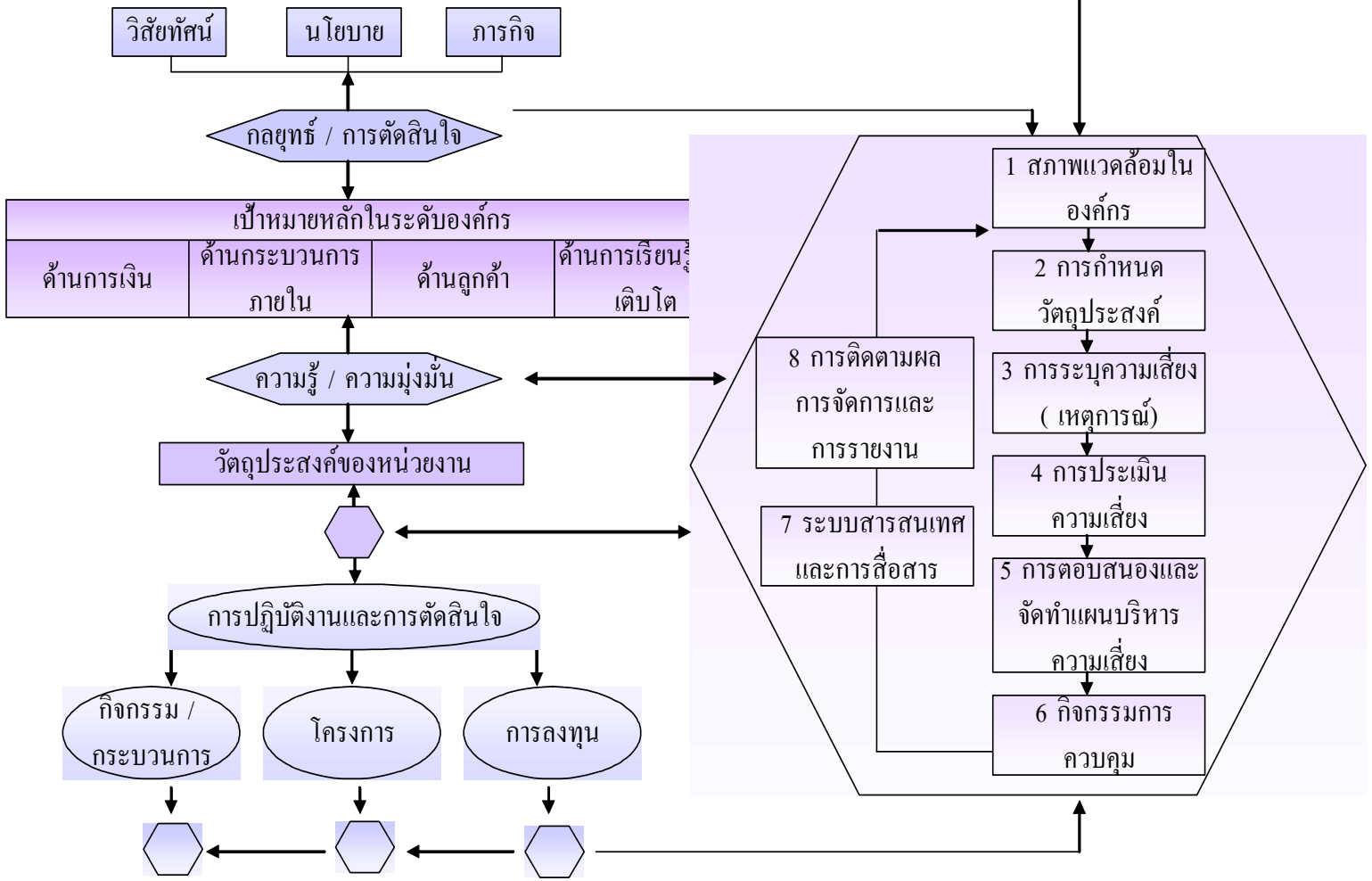
Internal Environment

- Senior management demonstrates that change management is important.
- Presence of an effective culture of change management.
- No tolerance for out-of-process changes; waiver process in place.
- Documentation exists (policies, procedures, process for managing changes in applications, databases, operating systems, and all other IT assets).
- Process training for all affected personnel provided.
- Defined roles and responsibilities enforced.
- Service level aggreements (SLAs) and contracts with vendors in place that define process and performance standards.
- Company-level standards and guidelines for the change process in place.

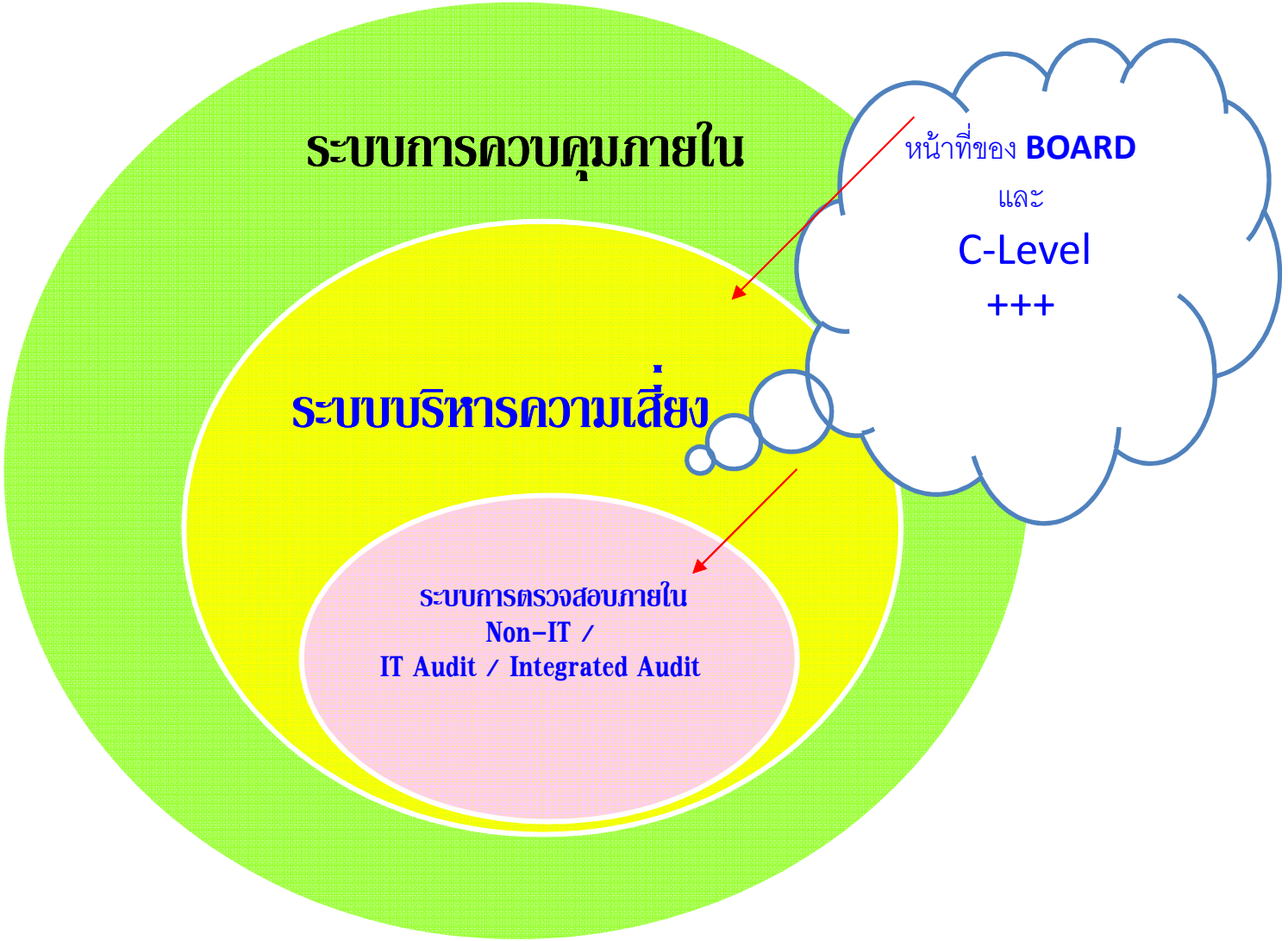
Source : GTAG

แนวทางการบริหารความเสี่ยงแบบบูรณาการขององค์กร

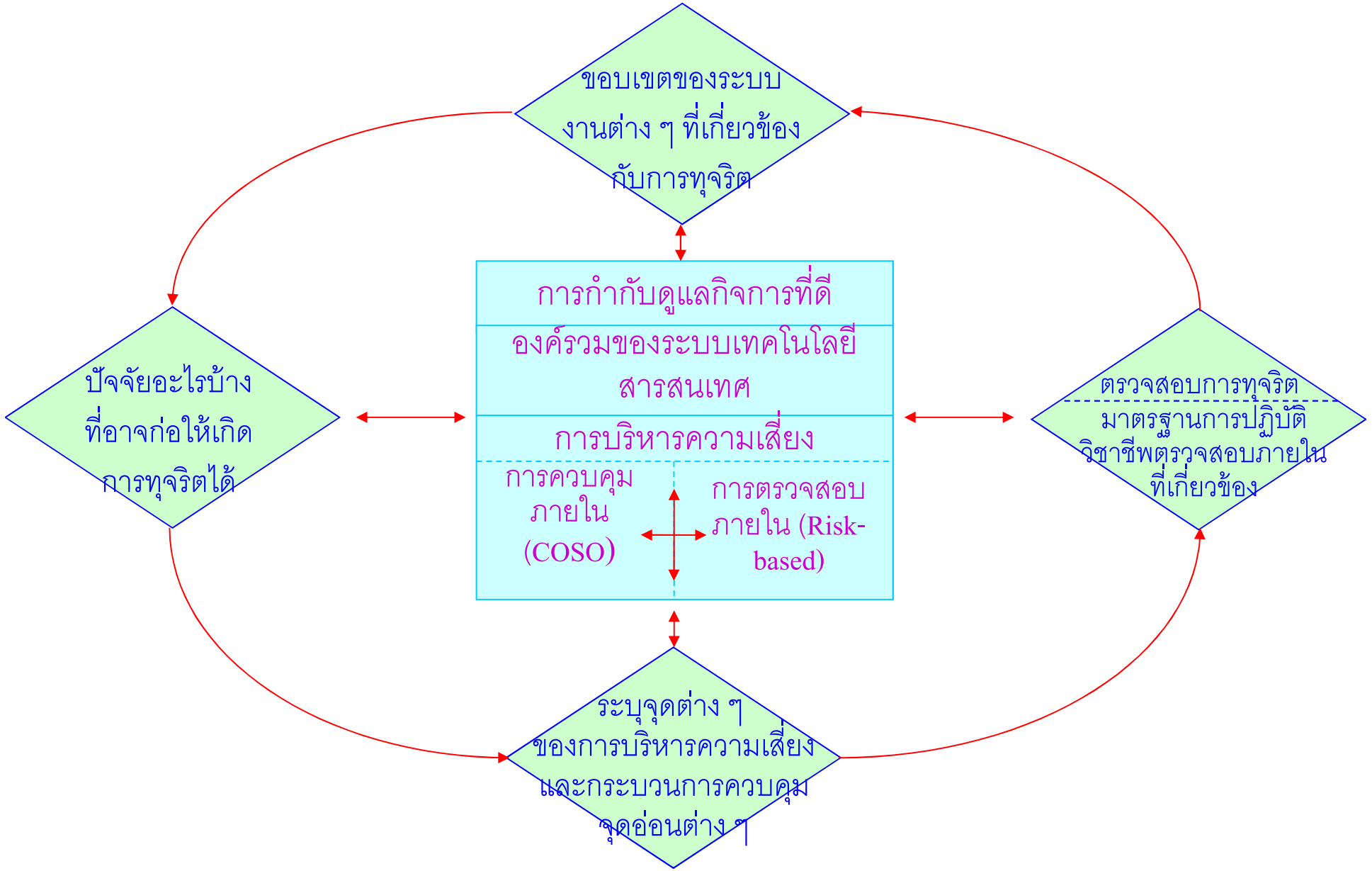
การนำการบริหารความเสี่ยงไปปฏิบัติ



ความสัมพันธ์ของการควบคุมภายใน การบริหารความเสี่ยง และการตรวจสอบภายใน



องค์ประกอบของการบริหารความเสี่ยงและการควบคุม/ตรวจสอบการทุจริตโดยคำนึงถึงกิจกรรมที่ก่อให้เกิดความเสี่ยง ซึ่งจะนำไปสู่ความเสียหายจากแนวโน้มการทุจริตได้



ที่มา : การดำเนินงานและการตรวจสอบสถาบันการเงินด้านคอมพิวเตอร์ เล่มที่ 3 คอมพิวเตอร์กับการทุจริต / หน้า 349 โดยเมธา สุวรรณสาร

การทุจริตกับการตรวจสอบภายใน

การทุจริตกับการตรวจสอบภายใน

- ผู้ตรวจสอบภายในมีความรับผิดชอบในการช่วยป้องกันการทุจริตโดย*การสอบทานและประเมินความเพียงพอและประสิทธิผลของการควบคุมภายใน* ดังต่อไปนี้

1. ด้านสภาพแวดล้อมการควบคุม
2. การประเมินความเสี่ยงจากการทุจริต
3. การสอบทานประสิทธิผลของการควบคุมที่กำหนดขึ้นเพื่อป้องกันการทุจริต
4. การเปลี่ยนแปลง กฎ ระเบียบ หรือระบบในการปฏิบัติงานที่อาจมีผลกระทบต่อการควบคุมภายใน
5. การประเมินประสิทธิผลของระบบการสื่อสารและสารสนเทศ
6. ประเมินกิจกรรมการติดตามผล

Organization Structure and Auditors
Old Paradigm

Business Auditor Focus

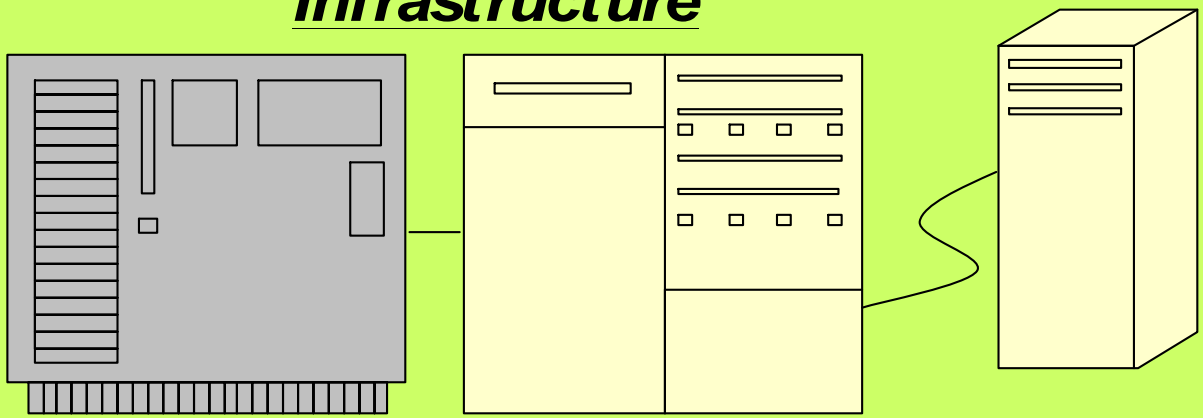
Business Process

Approaching to Integrated Audit

Infrastructure

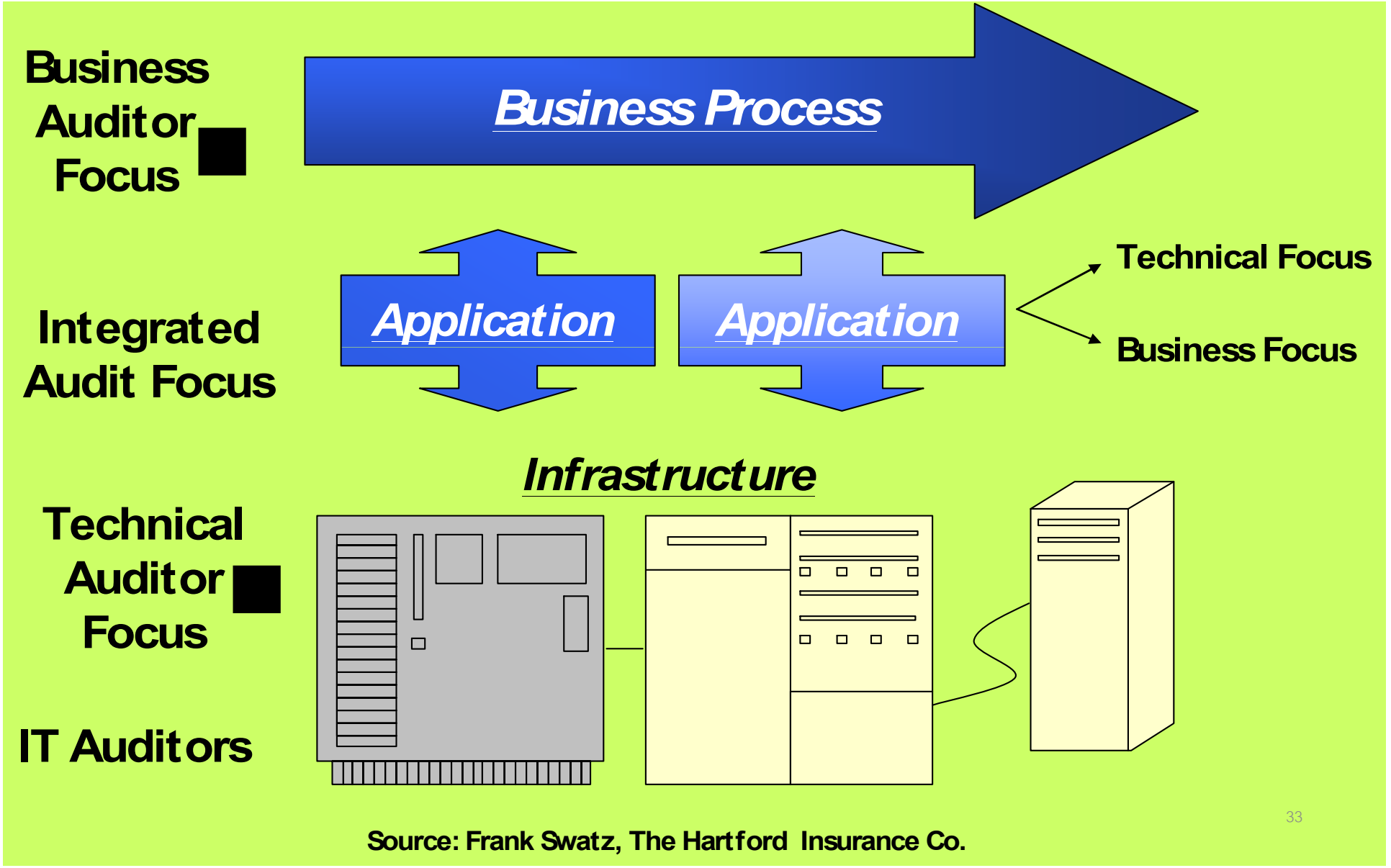
Technical Auditor Focus

IT Auditors



Source: Frank Swatz, The Hartford Insurance Co.

Approach to Integrated Auditing & Fraud Audit

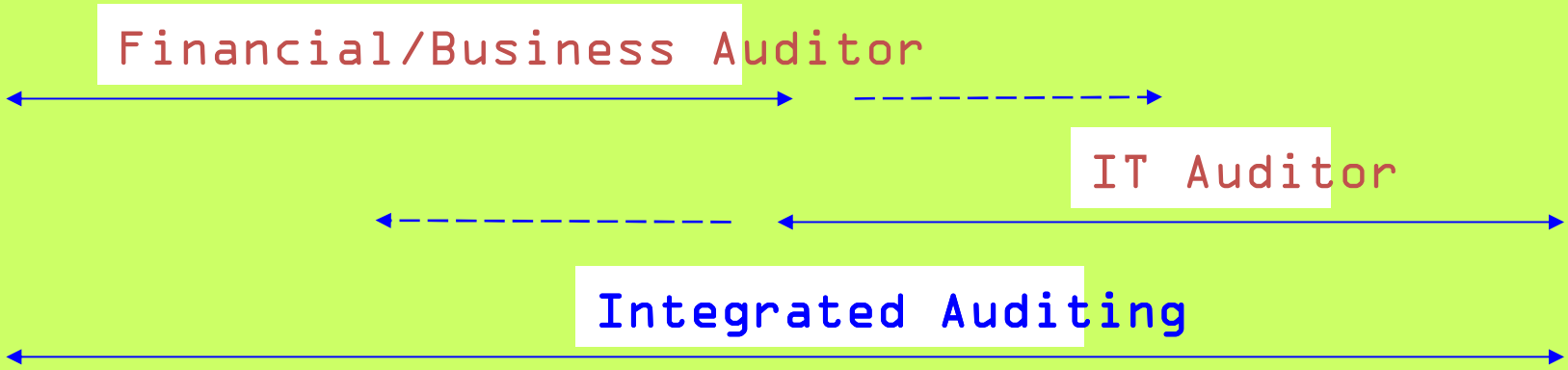


Source: Frank Swatz, The Hartford Insurance Co.

Integrated Auditing and Understanding

Financial / Operational / Applications / General

IT / Technical IT

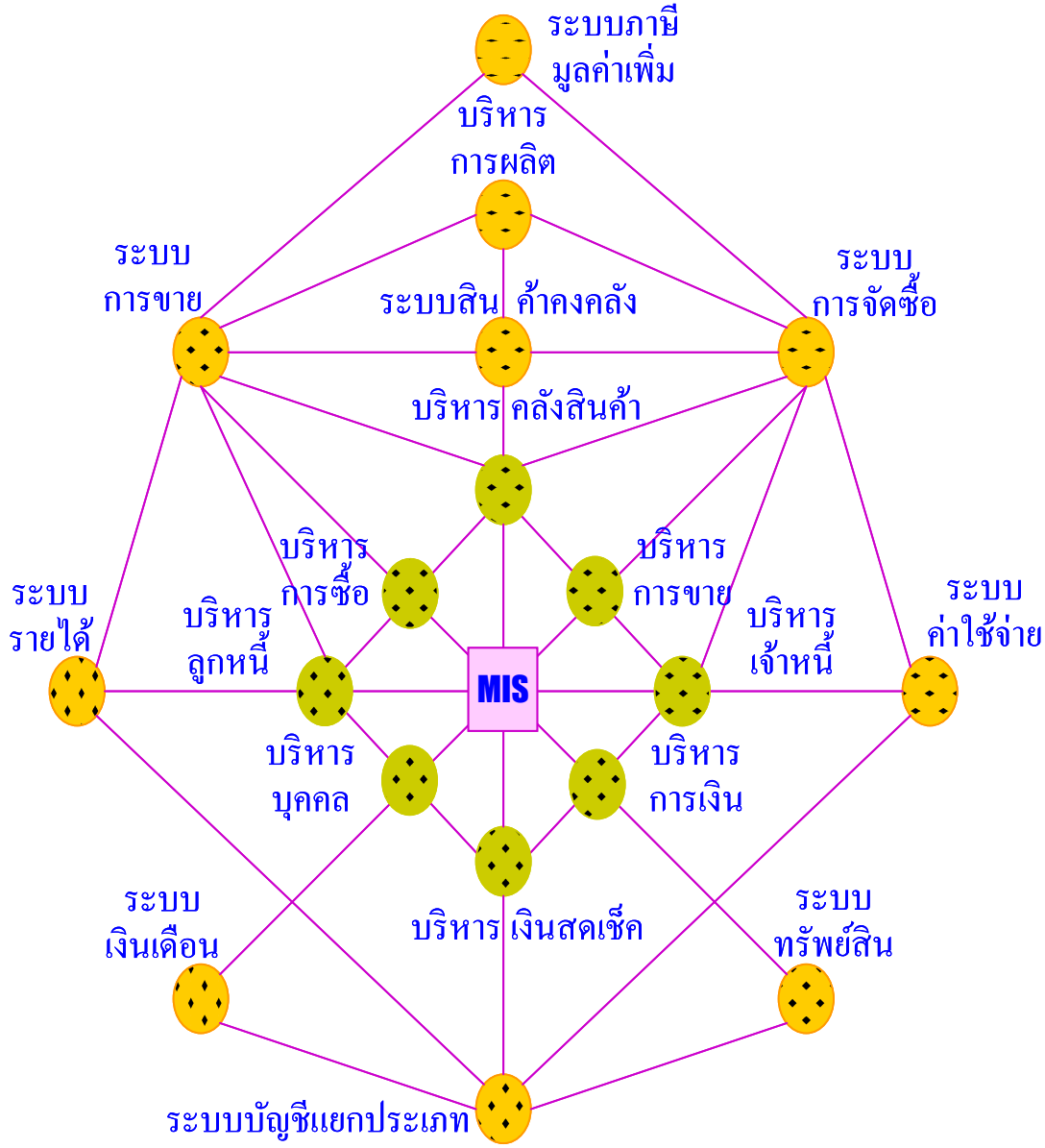


Merging of IT, Finance and Operations Auditors

- IT Auditors need to know the business.
- Financial/Operations Auditors need to know the systems.

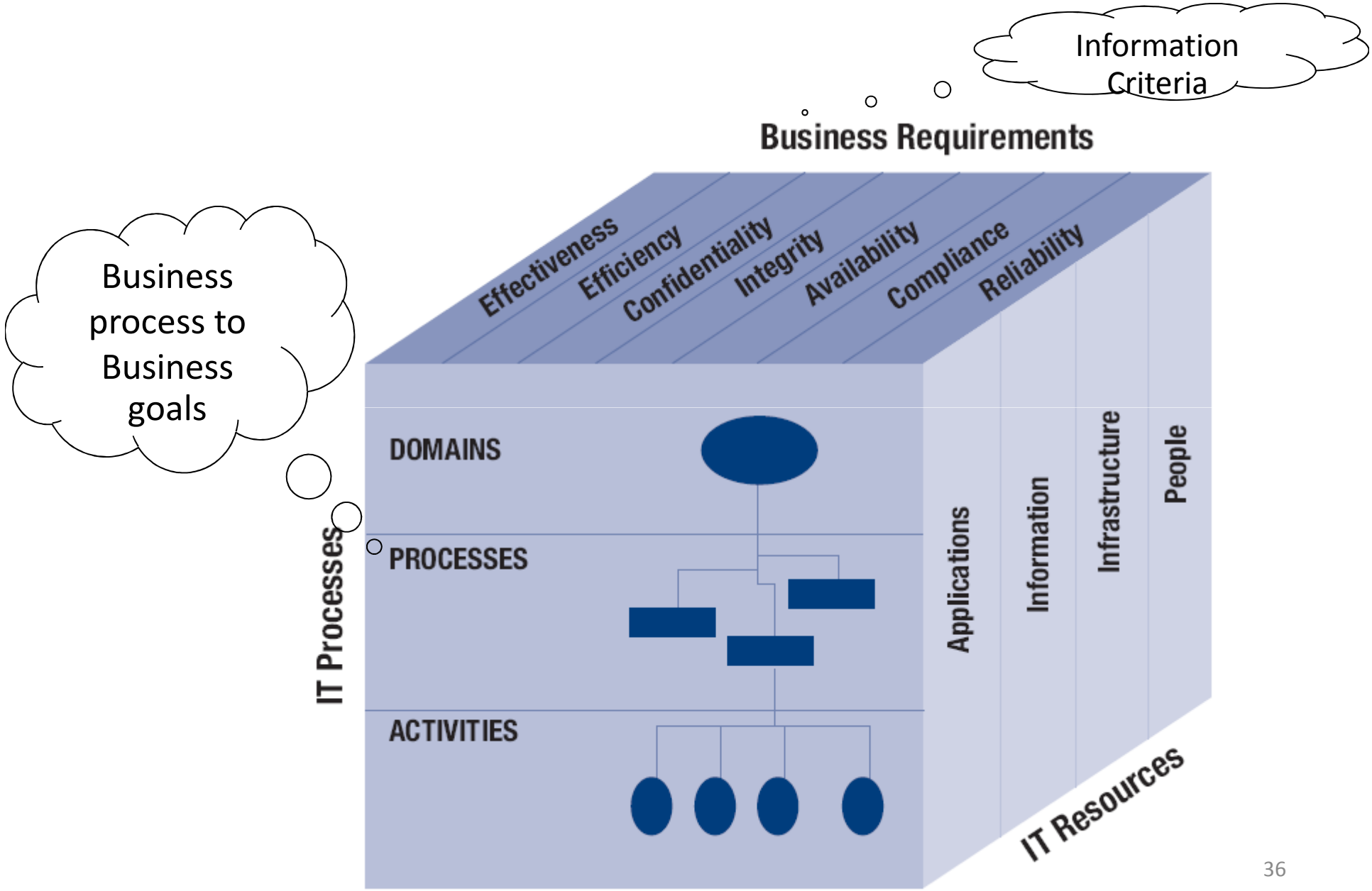
ERP Perspective and Integrated Management / Audit by Regulators and Operators

ตัวอย่าง ระบบงาน ERP เบื้องต้นกับความเข้าใจของผู้บริหารและผู้ตรวจสอบการทุจริค แบบบูรณาการ โดยใช้หลักการ COBIT บางมิติ



ที่มา : www.itgthailand

CG / IT Governance – ITG / CobiT "Control Practices"



การตรวจสอบ การร้องเรียน และการควบคุมการทุจริต

Whistleblowing and Fraud Audit

Detection

Fraud indicators

- Receipt of tip-offs
- Refusal to take vacation or sick leave
- Significant personal debt and credit problems
- Behavioral changes - These may be an indication of drugs, alcohol, gambling, or just fear of losing the job
- High employee turnover, especially in those areas which are more vulnerable to fraud
- Lack of segregation of duties in a vulnerable area
- Employee lifestyle changes: expensive cars, jewelry, homes, clothes
- Management decisions are dominated by an individual or small group.
- Managers display significant disrespect for regulatory bodies
- Policies and procedures are not documented or enforced.

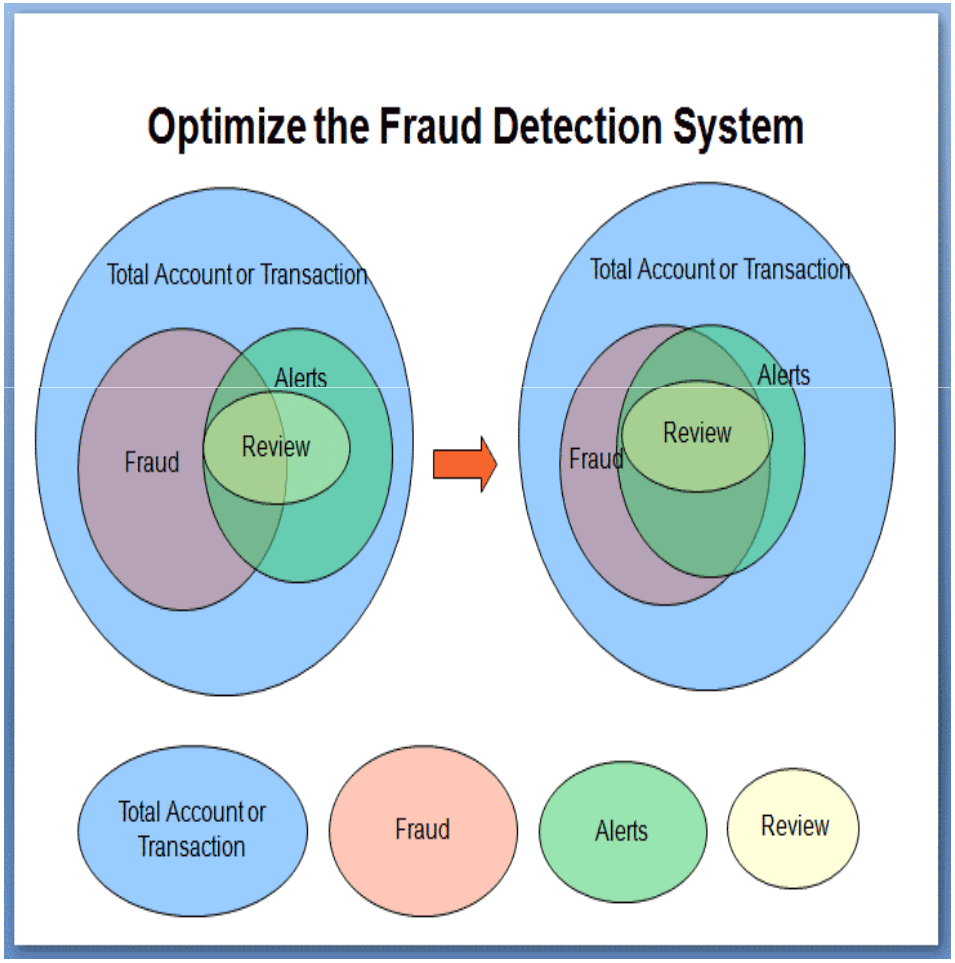
http://www.slideshare.net/donsquire/presentation-on-fraud-prevention-detection-control

Fraud Prevention, Detection & Control.

Figure 1: the four pillars of managing fraud risk

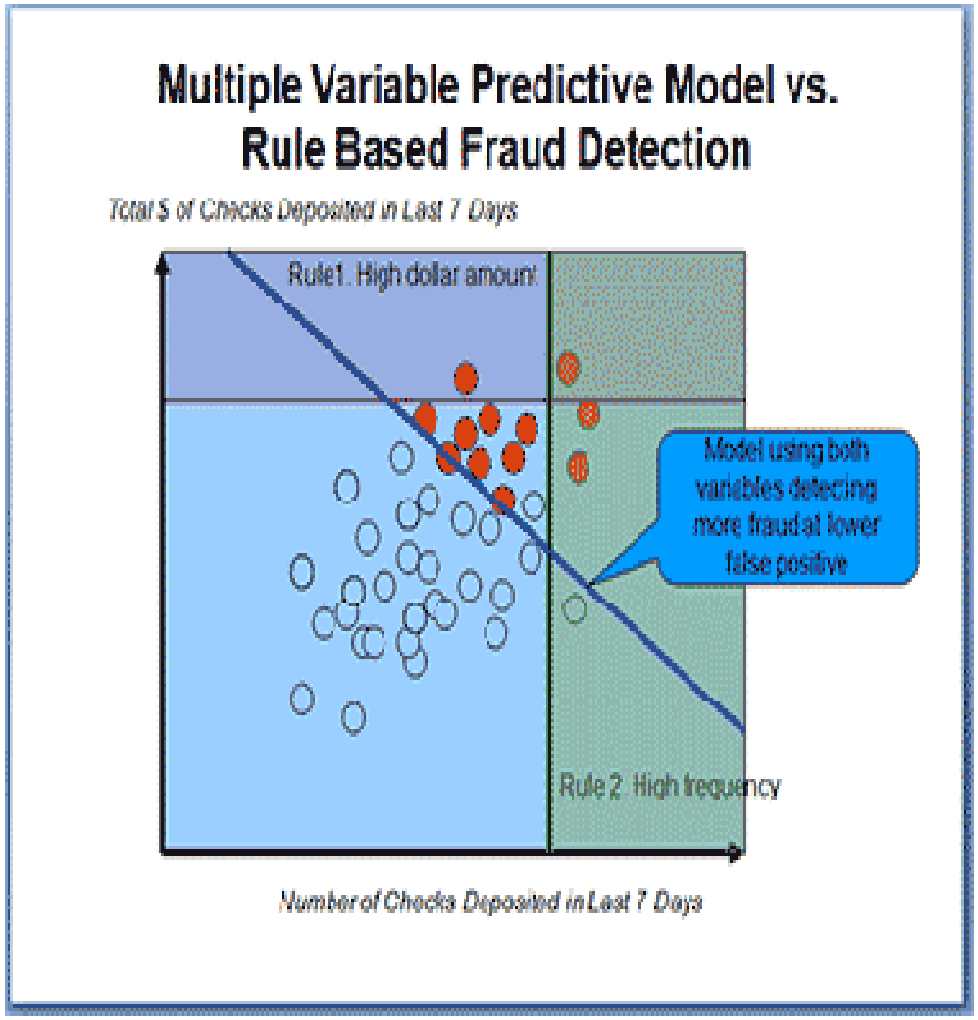
http://www.acl.com/2016/06/fight-fire-with-fire-a-technology-driven-response-to-fraud/

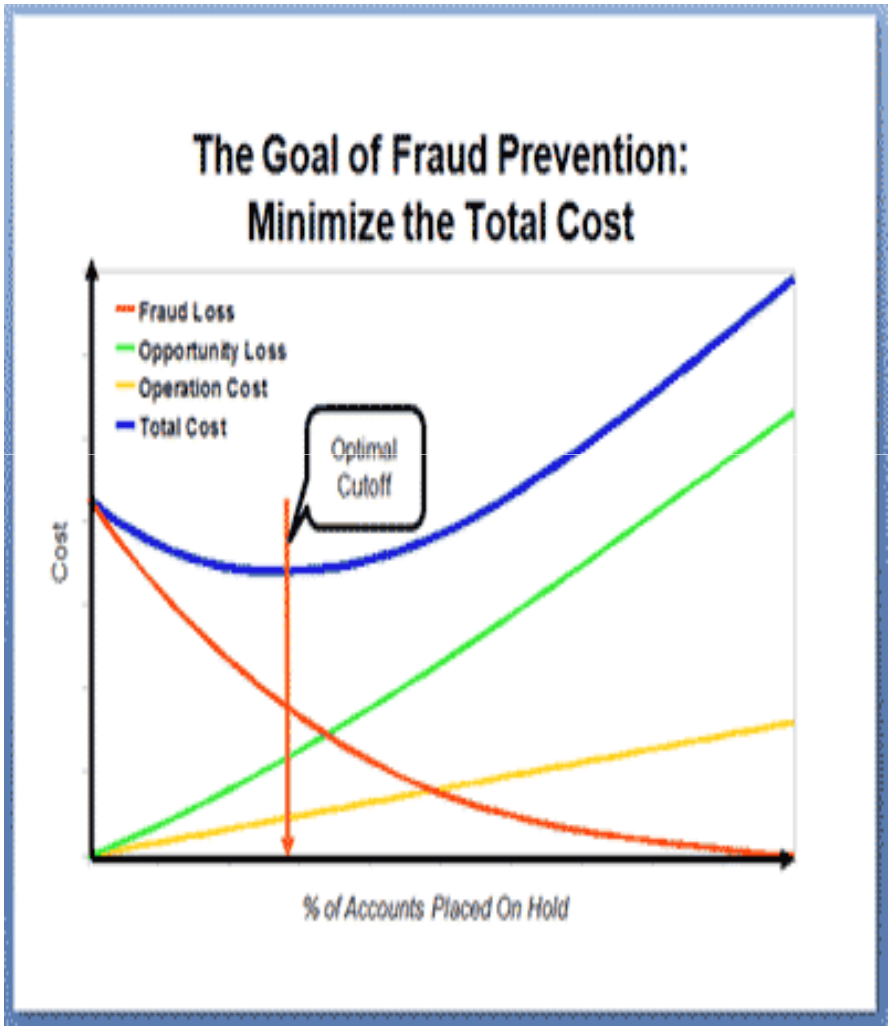
Fraud prevention and detection



http://businessdataminers.com/products/products.htm

Fraud prevention and detection

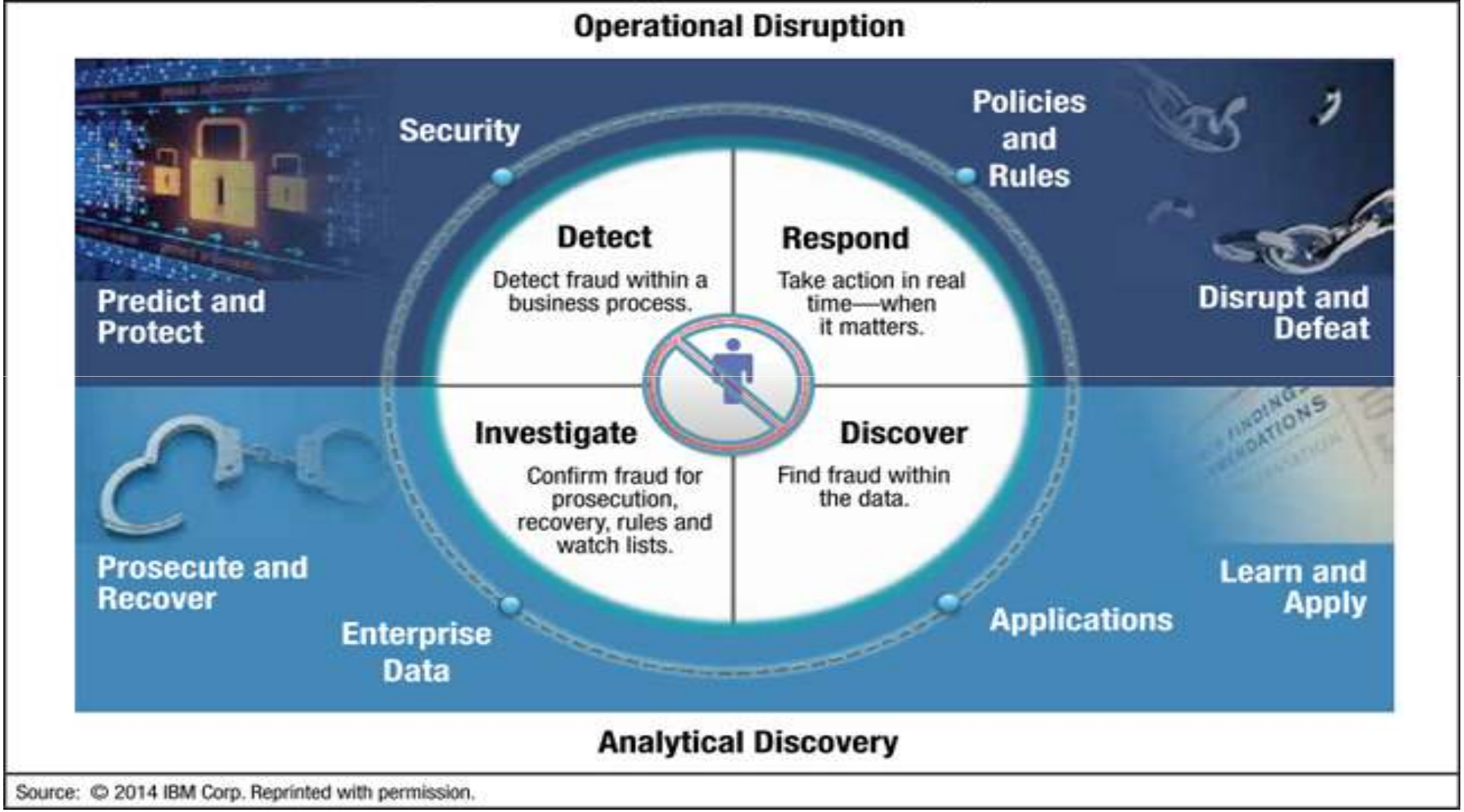




http://businessdataminers.com/products/products.htm

Fraud prevention and detection and Analytical Discovery

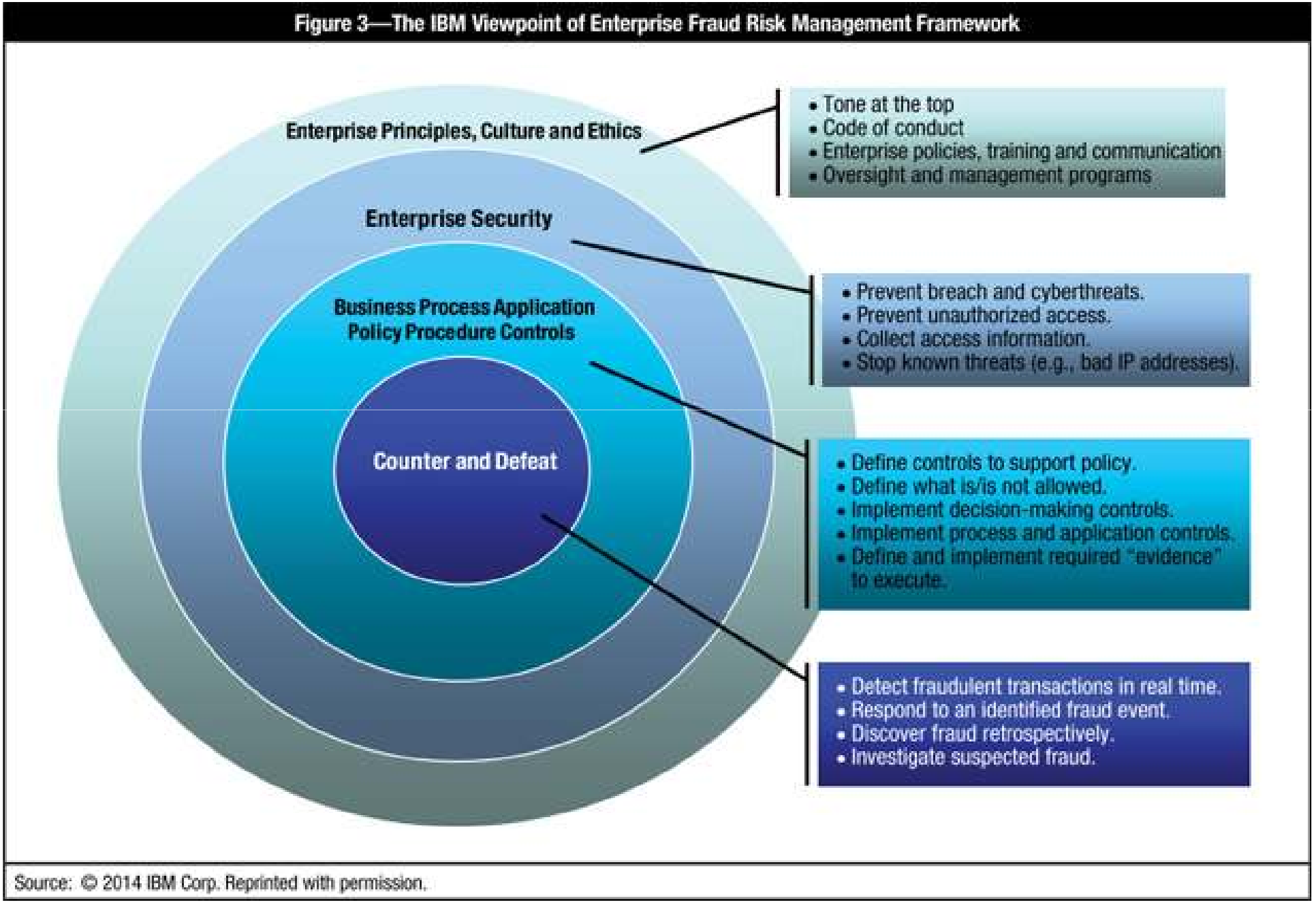
Figure 4—The IBM Viewpoint of Critical Counterfraud Capabilities



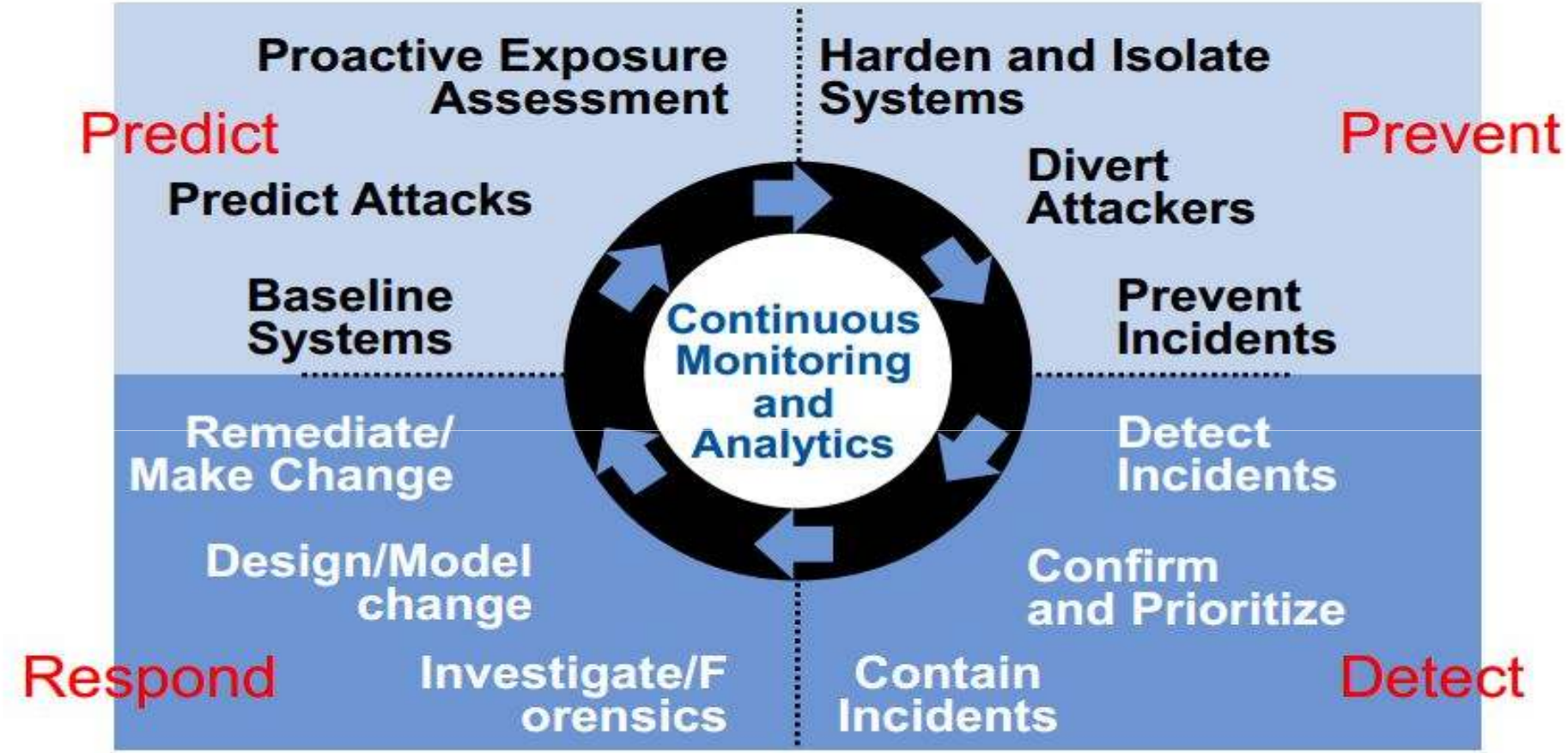
Source: © 2014 IBM Corp. Reprinted with permission.

http://www.isaca.org/Journal/archives/2014/Volume-5/Pages/Manage-What-You-Know-and-What-You-Do-Not-Know-A-Road-Map-to-Managing-Enterprise-Fraud-Risk.aspx

Enterprise Principles, Enablers- Cultures and Ethics- Counter and Defeat



The Adaptive Security Architecture



Gartner

enterprises buy too much threat prevention and not enough detection and response technology.

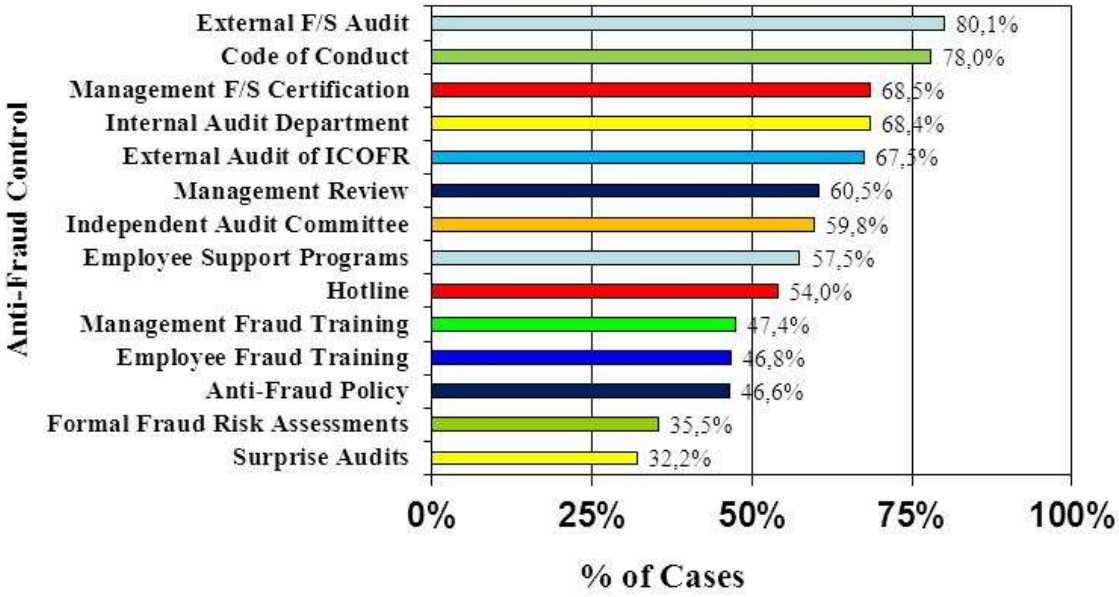
http://searchsecurity.techtarget.com/news/2240223269/On-prevention-vs-detection-Gartner-says-to-rebalance-purchasing

Enterprise Principles, Enablers- Cultures and Ethics- Counter and Defeat

http://www.slideshare.net/donsquire/presentation-on-fraud-prevention-detection-control

Enterprise Principles, Enablers- Cultures and Ethics- Counter and Defeat

Frequency of Anti-Fraud Controls



CBIZ

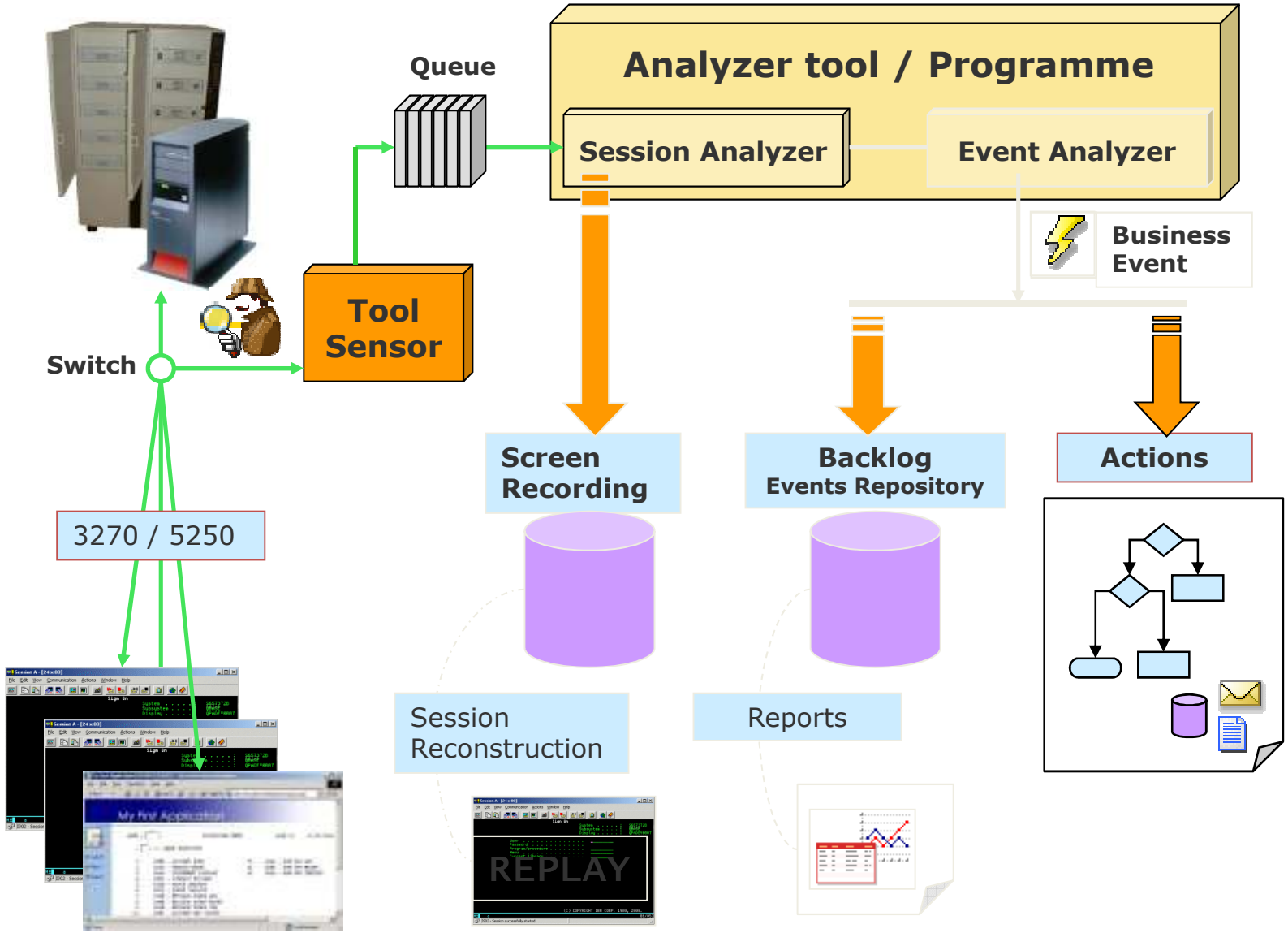
http://slideplayer.com/slide/2372757/

Monitoring for Behavior Audit

and

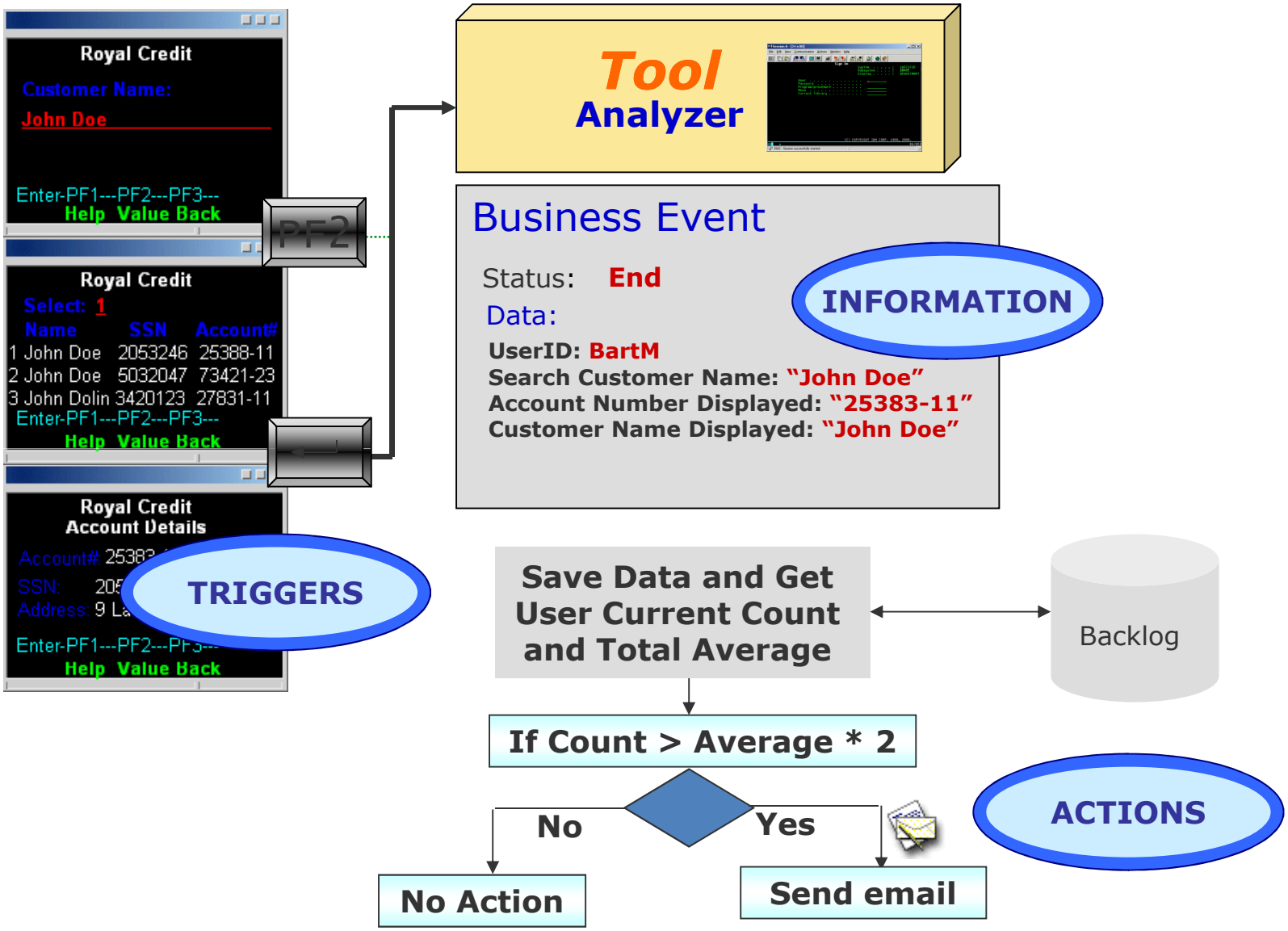
Integrated Management / Controls

Monitoring Solution for Mgmt./ Control and Behavior Audit



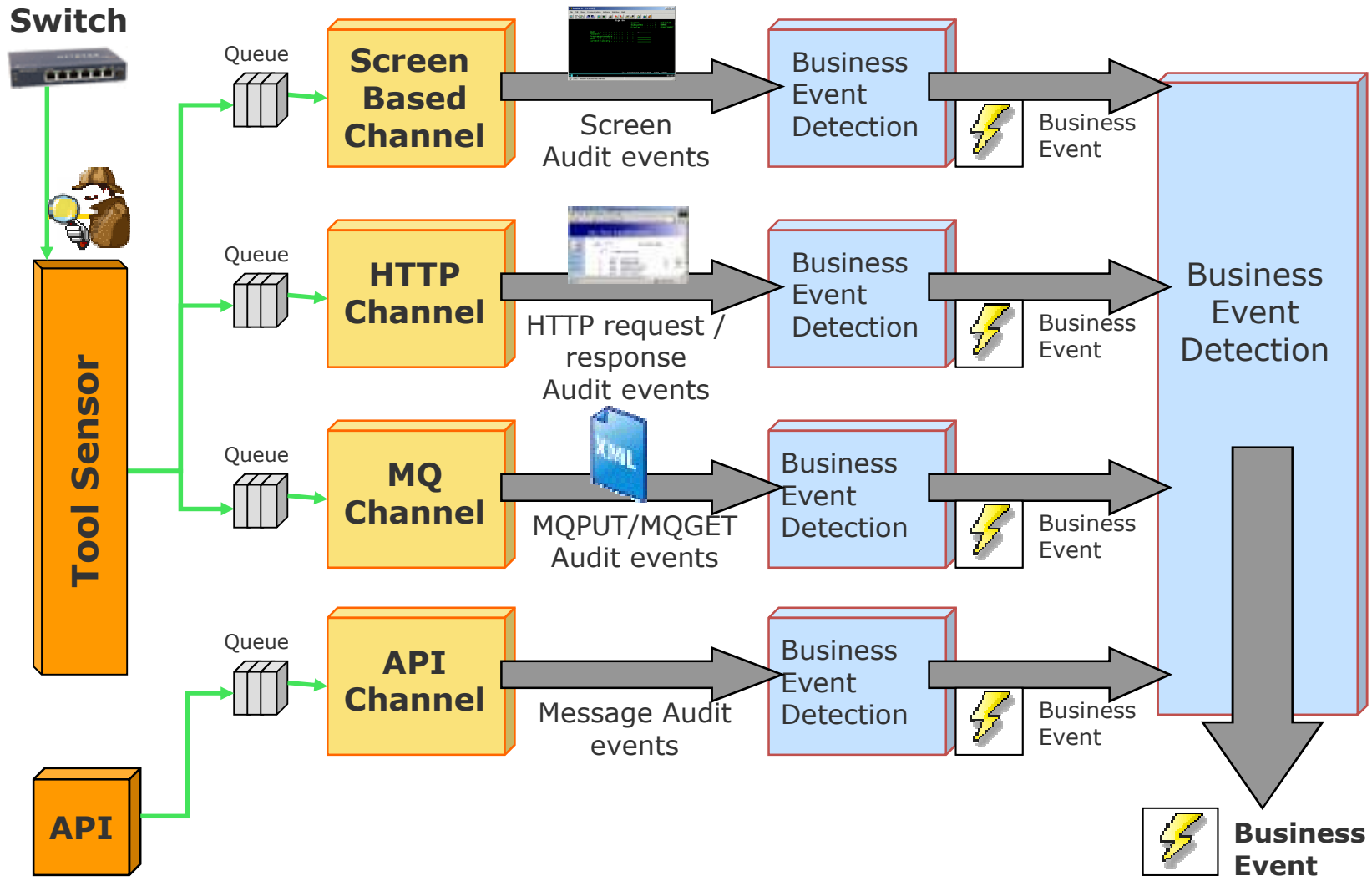
source : Intellin

Pain points and Business Event



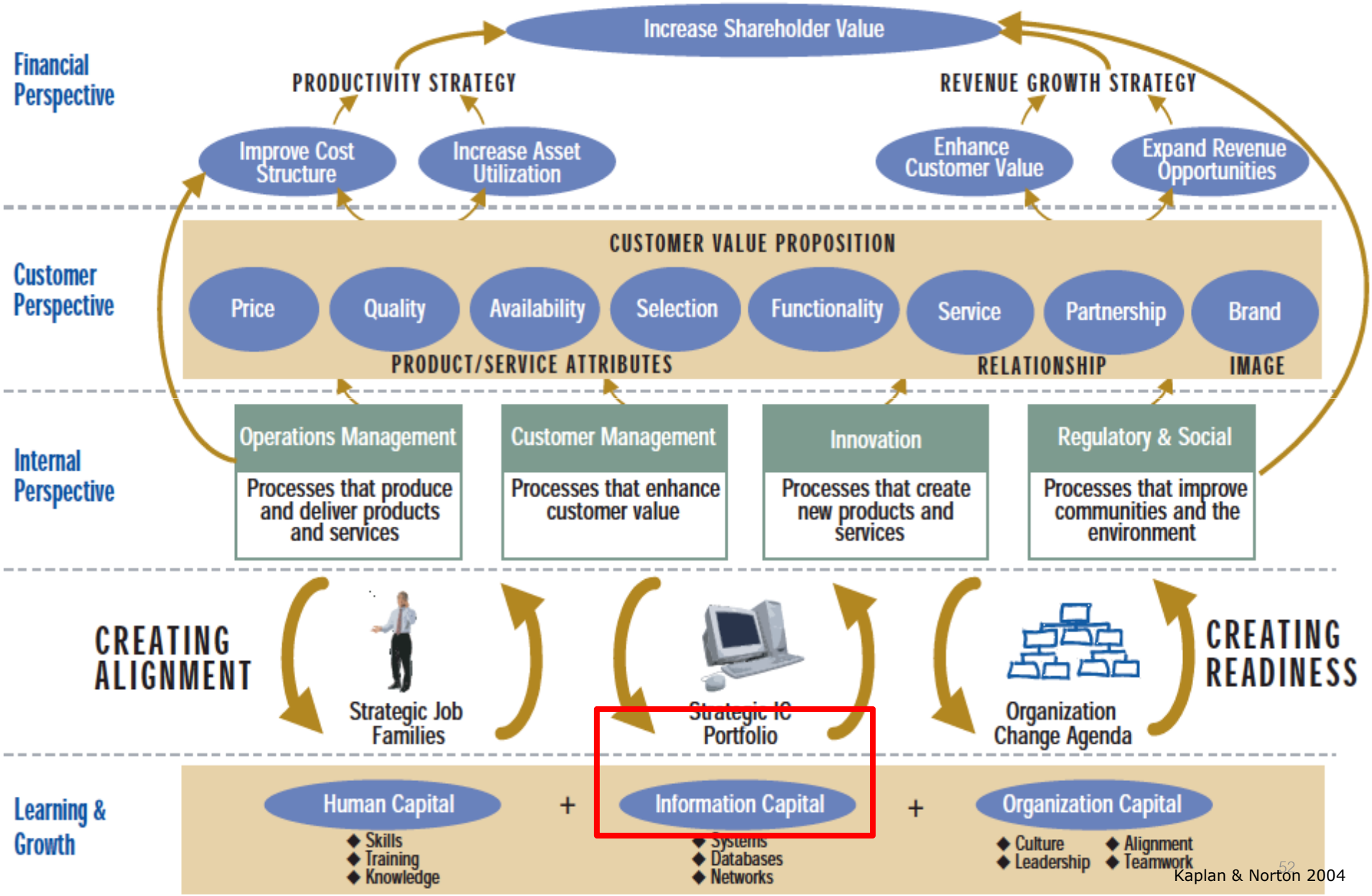
source : Intellin

Architecture Roadmap and Risk Management



source : Intellin

COBIT5 / GEIT > Value Creation -> EDM ->Dashboard



Kaplan & Norton 2004

Whistleblowing

กับการแจ้งเบาะแส การทุจริต

Automatically detect the Red Flags & Business Rules

The Paradigm Shift from

Transaction Tracking

to

"Real- Life" Behavior tracking

Source: www.itgthailand.com

ตัวอย่างเพียงพื้นฐาน บางประการ / สัญญาณเตือนภัย(Red Flag) กับ การแจ้งเบาะแส การทุจริต [Whistleblowing]

- มีการอนุมัติเกินอำนาจ
- มีการบันทึกบัญชีพัก
- มีรายการแก้ไขมากกว่าปกติ
- ลูกหนี้หลายรายมีที่อยู่ที่เดียวกัน
- พนักงานมีความสัมพันธ์กับลูกหนี้ผิดนัด เป็นพิเศษ
- เหตุผลการตัดหนี้สูญอ่อน
- ยอดหนี้ค้างชำระ /OD สูง
- ค่าเบี้ยเลี้ยง หรือค่าใช้จ่ายสูงมากผิดปกติ
- ค่าธรรมเนียม รายรับน้อยลง ผิดปกติ
- เอกสารสูญหาย โดยเฉพาะ แบบฟอร์มสำคัญ เช่น passbook, cashier cheque

Source: www.itgthailand.com

ตัวอย่าง เพียงพื้นฐานบางประการ / สัญญานเตือนภัย (Red Flag) (ต่อ)

- การรวมอำนาจหน้าที่ในการอนุมัติ ปฏิบัติงาน และรายงานสำคัญไว้ในบุคคล เดียวกัน (ขาด การแบ่งแยกหน้าที่)
- การประเมินผลไม่เพียงพอ
- การขาดมาตรฐานในการพิจารณาผลงานและโครงการ
- วิธีการปฏิบัติงานที่ไม่ชัดเจนและสับสน
- การขาดการสอบทานอิสระเกี่ยวกับความถูกต้องของการบันทึกรายการและรายงานต่าง ๆ
- การขาดการป้องกันดูแลทรัพย์สิน และทรัพยากรอย่างเพียงพอ
- การขาดการระบุหน้าที่ความรับผิดชอบที่ชัดเจน
- +++++++++

Source: www.itgthailand.com

โอกาสเปิดช่องทุจริต กับ Whistleblowing

- อำนาจหน้าที่ไม่ชัดเจน
- ไม่มีคู่มือการปฏิบัติงานเป็นลายลักษณ์อักษร
- การลงบัญชี และการบันทึกไม่ครบถ้วน
- ทำงานคนเดียว เบ็ดเสร็จ
- ขาดการหมุนเวียนงาน
- นโยบายการบุคคลอ่อนแอ
- การวัดผลงานไม่ชัดเจน
- ระบบการกระทบยอดไม่เหมาะสม
- ระบบการรายงานไม่ได้เน้นรายการที่ผิดปกติ ควรติดตาม
- อื่น ๆ +++++++++

Source: www.itgthailand.com

Whistleblowing & Business Rules for Business Control

Business rule is a statement that defines or constrains some aspect of the business.

It is intended to assert business structure or to control or influence the behavior of the business.

Individual **business rules** that describe the same facet of an enterprise are usually arranged into **business rule-sets**.

Business rules describe the operations, definitions and constraints that apply to an organization in achieving its goals.

For example a **business** rule might state that *no credit check is to be performed on return customers*.++

Others could define a tenant in terms of solvency or list preferred suppliers and supply schedules.+++

These **rules** are then used to help the organization to better achieve goals, communicate among principals and agents, communicate between the organization and interested third parties, demonstrate fulfillment of legal obligations, operate more efficiently, automate operations, perform analysis on current practices, etc

Example of

Business Rules / Banking

การกำหนดเงื่อนไข (business rules) พื้นฐานเพื่อการติดตามพฤติกรรม

1. สำหรับระบบ Core Banking (internal fraud)

- รายการที่น่าสงสัย
  - การฝากประจำ แล้วมีการถอนออก โดย teller คนเดียวกัน
  - การทำรายการ reverse รายการ
  - การเปลี่ยนแปลงบรรทัดบนสมุดคู่ฝาก
  - การทำฝาก/โอน เข้าบัญชี ของพนักงาน หลังจากทำรายการถอน
  - การฝาก/โอน แบบย้อนหลัง (back date)
  - การถอนเงินจากบัญชีที่ไม่มีชื่อบัญชี
  - การเปลี่ยนแปลงชื่อบัญชี ของลูกค้า ที่ผิดสังเกต

การกำหนดเงื่อนไข (business rules) เพื่อการติดตาม

1. สำหรับระบบ Core Banking (ต่อ)

- รายการที่น่าสงสัย (ต่อ)
  - การทำรายการ ยกเลิก misc code ต่างๆ ได้แก่ 17(ห้ามถอน),18(ถึงแก่กรรม), 19 (ศาลสั่งพิทักษ์ทรัพย์) แล้วถอนเงินออก
  - การทำรายการยกเลิก (reverse)
  - การเปลี่ยนแปลงสถานะเช็ค จาก “paid” เป็น “unpaid” แล้วถอนเงินออก
  - การเปลี่ยนแปลงสถานการณ์คิดดอกเบี้ย
  - การเพิ่ม หรือลดดอกเบี้ย accrued
  - การถอนเงินจากบัญชีที่ inactive

การกำหนดเงื่อนไข (business rules)

1. สำหรับระบบ Core Banking (ต่อ)

- การไม่ปฏิบัติตามระเบียบ
  - สำหรับสาขาย่อยที่เปิดทำการในวันหยุด การรับฝาก/ถอน/โอน เกินวงเงินที่กำหนด
  - การทำรายการ หรือเปิดเข้าระบบนอกเวลาทำการ
  - การไม่ทำรายการ sign off ในช่วงพัก

- www.itgthailand.com

การกำหนดเงื่อนไข (business rules)

2. สำหรับระบบ Internet Banking (external fraud)

- รายการที่น่าสงสัย
  - การทำรายการชำระเงินมือถือ แบบเติมเงิน หรือเติมเงินบัตรเงินสด บ่อย ๆ
  - ลูกค้าหลายคนมีการทำรายการมาจากเครื่องเดียวกัน
  - ลูกค้ามีการ sign on เข้าระบบ จากหลาย ๆเครื่องที่ไม่น่าจะอยู่ใน บริเวณเดียวกัน
  - มีการทำรายการมาจากต่างประเทศ
  - มีการโอนเงินเข้าบัญชีเดียว หลายครั้งในวันเดียว

การกำหนดเงื่อนไข (business rules)

2. สำหรับระบบ Internet Banking (ต่อ)

- รายการที่น่าสงสัย (ต่อ)
  - การทำรายการสมัคร KOL โดยสมัครด้วยเลขที่บัตร ATM หลาย ๆเบอร์ และมีการทดลองใส่ pin no ที่ไม่ถูกต้อง
  - การทำรายการมาจาก IP address หรือเครื่องที่เป็น black list
  - และอีกมาก +++++

อย่ากลัว

ความผิดพลาด
ที่สุจริต

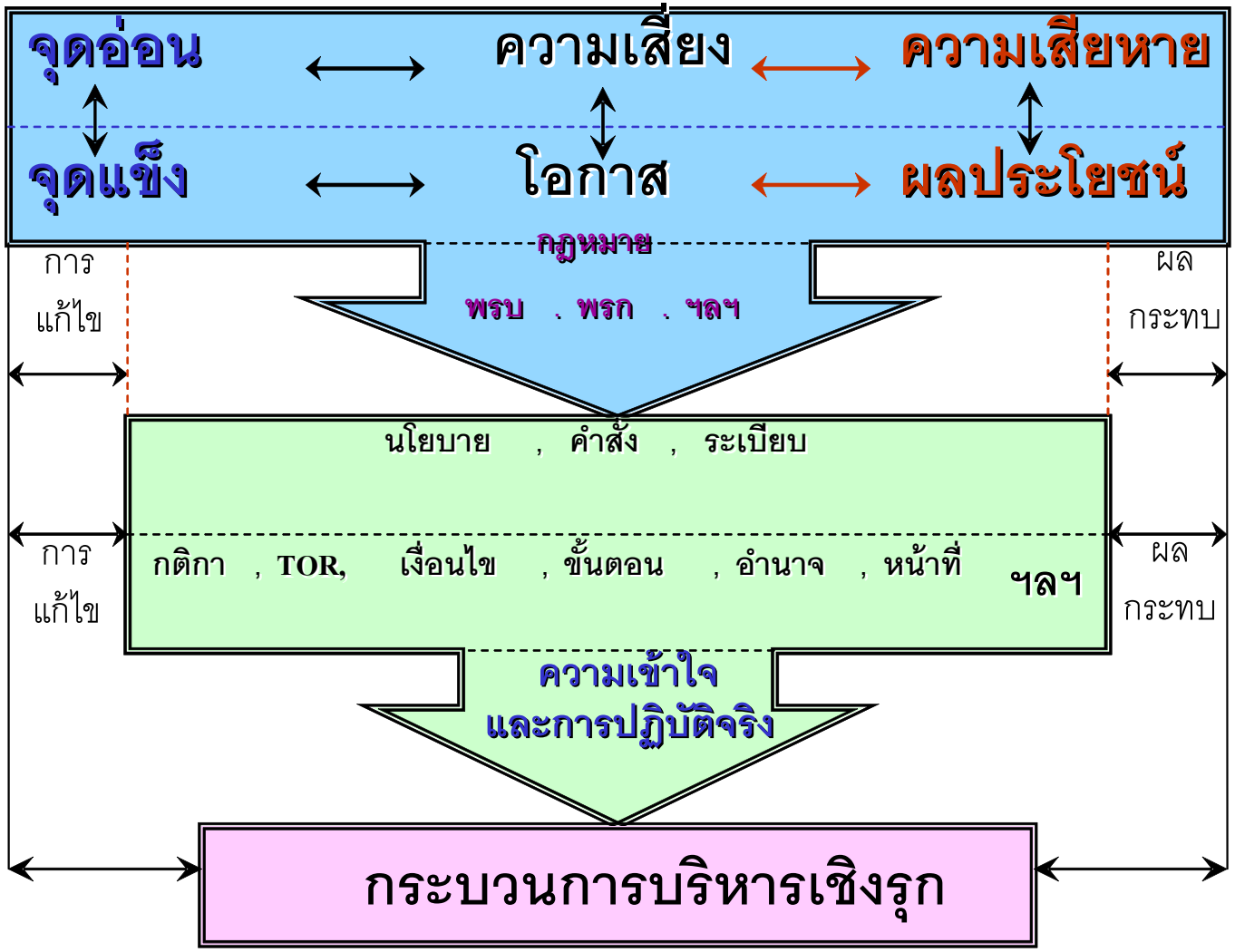
↕

Fiduciary Duty

ค่านิยมสมัยใหม่ และ การสร้างวัฒนธรรมขององค์กร กับ iGRC

GOOD ORGANIZATION	GREAT ORGANIZATION
1. Directives Leadership	1. Visionary Leadership
2. Functional Perspective	2. Systems Perspective
3. Focus on Next Quarter's Result	3. Focus on the Future
4. Compliance with Regulation	4. Social Responsibility
5. Product & Service Driven	5. Customer Driven Excellence
6. Response in Time Allotted	6. Agility
7. Focus on Bottom Line	7. Focus on Results and Creating Value
8. Suppliers and Unions as Adversaries	8. Valuing Employees and Partners
9. Meet Standard or Status Quo	9. Organizational and Personal Learning
10. Management by Intuition	10. Management by Fact
11. Employees Follow Procedures	11. Managing for Innovation

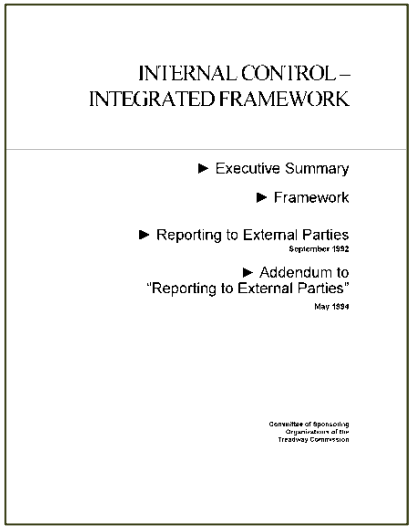
X-Ray ความรู้เท่าทันในการบริหารความเสี่ยงกับ การทุจริต ความเสียหาย และโอกาสการพัฒนา ขององค์กร แบบบูรณการ กับ GEIT



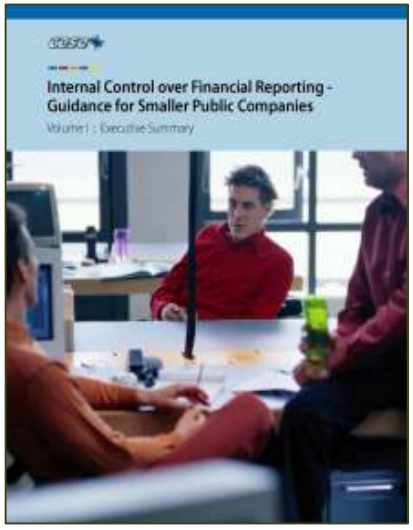
ที่มา : www.itgthailand.com

การบริหารความเสี่ยงจากการทุจริต ตามแนวทาง COSO

COSO Overview – Internal Control



1992



2006

2009

2013

เอกสาร ประกอบในกรณี เวลาไม่อำนวย

Questions?

Update expected to increase ease of use and broaden application

What is ***not*** changing...

- Core definition of internal control
- Three categories of objectives and five components of internal control
- Each of the five components of internal control are required for effective internal control
- Important role of judgment in designing, implementing and conducting internal control, and in assessing its effectiveness

What is changing...

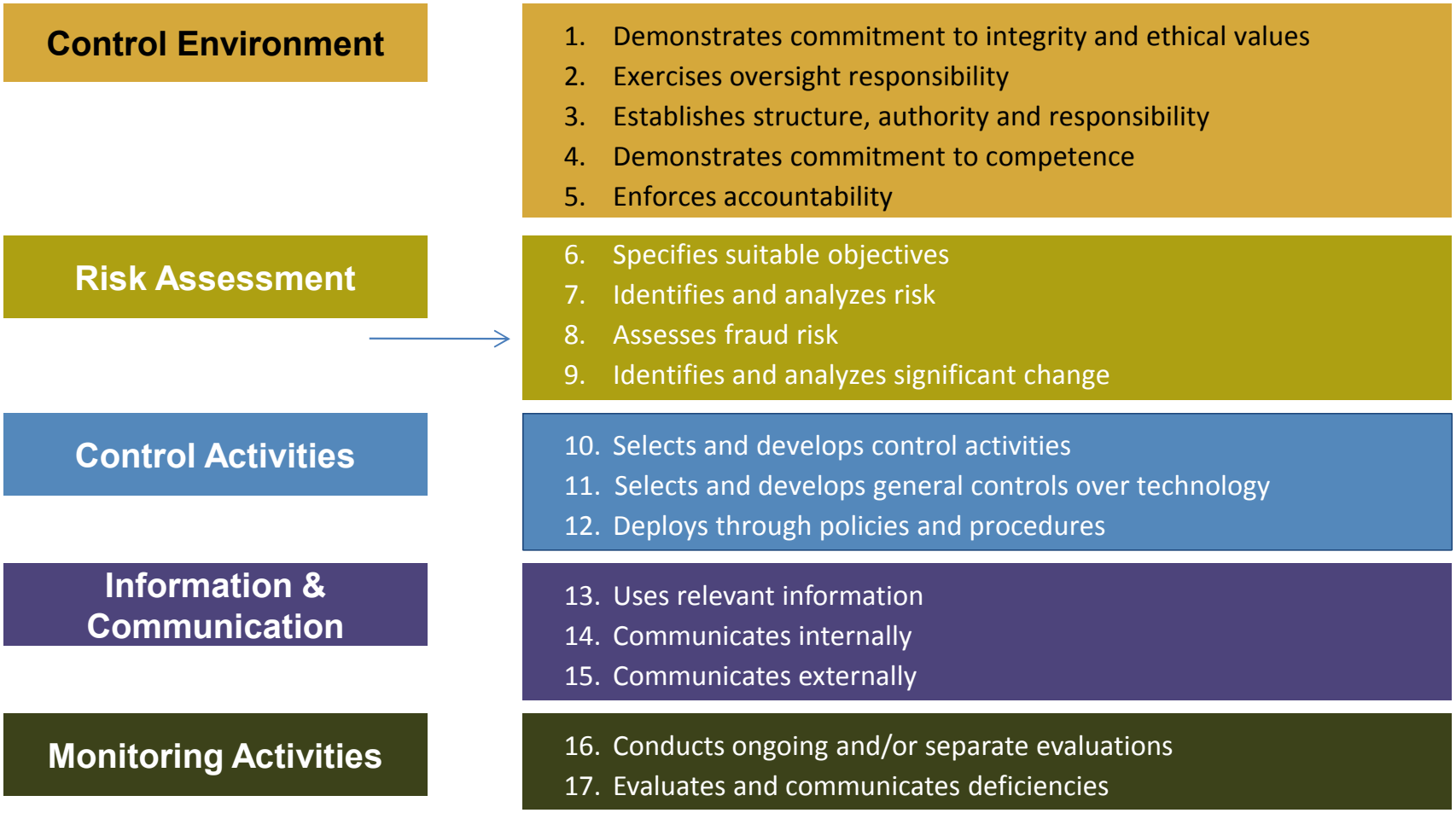
- Changes in business and operating environments considered
- Operations and reporting objectives expanded
- Fundamental concepts underlying five components articulated as principles
- Additional approaches and examples relevant to operations, compliance, and non-financial reporting objectives added

Update considers changes in business and operating environments

Environments changes...	*...have driven Framework updates*
Expectations for governance oversight	
Globalization of markets and operations	
Changes and greater complexity in business	
Demands and complexities in laws, rules, regulations, and standards	
Expectations for competencies and accountabilities	
Use of, and reliance on, evolving technologies	
Expectations relating to preventing and detecting fraud	

COSO Cube (2013 Edition)

Update articulates principles of effective internal control



Update articulates principles of effective internal control (continued)

Control Environment

1. The organization demonstrates a commitment to integrity and ethical values.
2. The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.
3. Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.
4. The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.
5. The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives.

Update articulates principles of effective internal control (continued)

Risk Assessment

6. The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.
7. The organization identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.
8. **The organization considers the potential for fraud in assessing risks to the achievement of objectives.**
9. The organization identifies and assesses changes that could significantly impact the system of internal control.

Update articulates principles of effective internal control (continued)

Control Activities

10. The organization selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.
11. The organization selects and develops general control activities over technology to support the achievement of objectives.
12. The organization deploys control activities through policies that establish what is expected and procedures that put policies into place.

Update articulates principles of effective internal control (continued)

Information & Communication

13. The organization obtains or generates and uses relevant, quality information to support the functioning of internal control.

14. The organization internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.

15. The organization communicates with external parties regarding matters affecting the functioning of internal control.

Update articulates principles of effective internal control (continued)

Monitoring Activities

16. The organization selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.
17. **The organization evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.**

Update clarifies requirements for effective internal control

- **Effective internal control provides reasonable assurance regarding the achievement of objectives and requires that:**
  - **Each component and each relevant principle is present and functioning**
  - **The five components are operating together in an integrated manner**

- Each principle is suitable to all entities; all principles are presumed relevant except in rare situations where management determines that a principle is not relevant to a component (e.g., governance, technology)
- Components operate together when all components are present and functioning and internal control deficiencies aggregated across components do not result in one or more major deficiencies
- A major deficiency represents an internal control deficiency or combination thereof that severely reduces the likelihood that an entity can achieve its objectives

Update describes important characteristics of principles, e.g.,

Control Environment

1. The organization demonstrates a commitment to integrity and ethical values.

Points of Focus:

- Sets the Tone at the Top
- Establishes Standards of Conduct
- Evaluates Adherence to Standards of Conduct
- Addresses Deviations in a Timely Manner

- Points of focus may not be suitable or relevant, and others may be identified
- Points of focus may facilitate designing, implementing, and conducting internal control
- There is *no* requirement to separately assess whether points of focus are in place

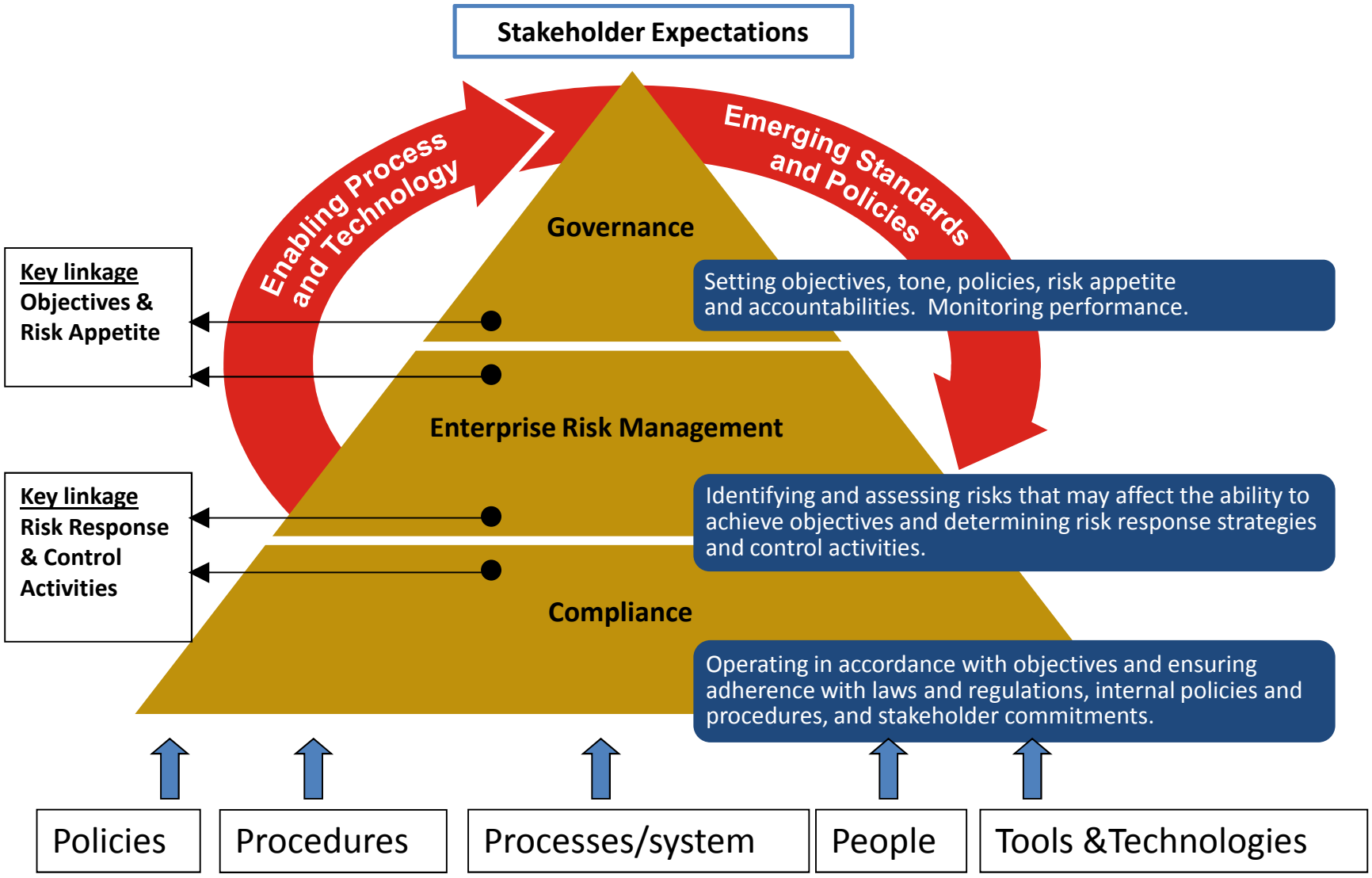
Update describes the role of controls to effect principles

- The Framework does not prescribe controls to be selected, developed, and deployed for effective internal control
- An organization's selection of controls to effect relevant principles and associated components is a function of management judgment based on factors unique to the entity
- A major deficiency in a component or principle cannot be mitigated to an acceptable level by the presence and functioning of other components and principles
- However, understanding and considering how controls effect multiple principles can provide persuasive evidence supporting management's assessment of whether components and relevant principles are present and functioning

Update describes how various controls effect principles, e.g.,

Component	**Control Environment**		
Principle	1. The organization demonstrates a commitment to integrity and ethical values.		
Controls embedded in other components may effect this principle	Human Resources review employees' confirmations to assess whether standards of conduct are understood and adhered to by staff across the entity *Control Environment*	Management obtains and reviews data and information underlying potential deviations captured in whistleblower hot-line to assess quality of information *Information & Communication*	Internal Audit separately evaluates Control Environment, considering employee behaviors and whistleblower hotline results and reports thereon *Monitoring Activities*

An Integrated Approach To Governance, Risk & Compliance



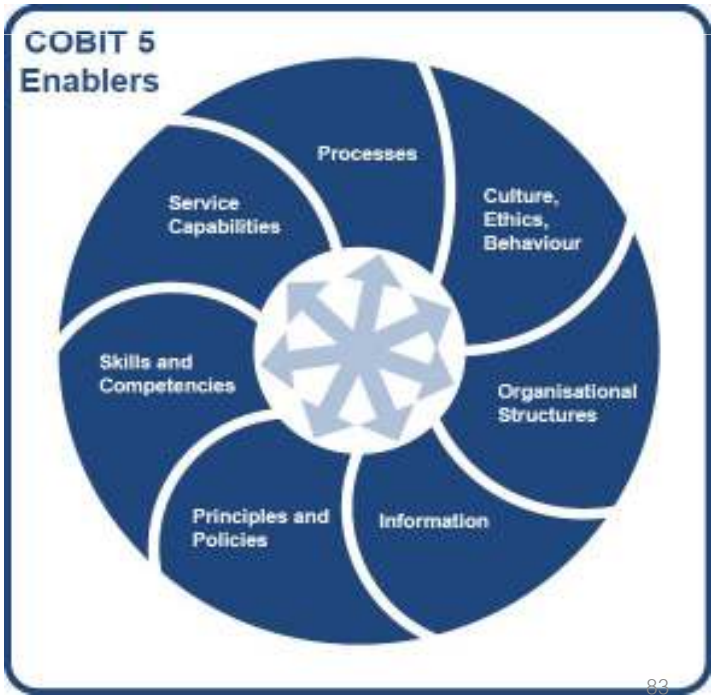
COBIT 5 for Regulators and Operators
แนวความคิดในการนำ GEIT ประยุกต์เพื่อการใช้งานและ บริบทที่เกี่ยวข้อง

ความเข้าใจกับการพิจารณา*บริบท*ขององค์กร เพื่อการกำกับ และการบริหารจัดการ

GEIT เป็นกรอบที่ทุกองค์กรต้องออกแบบแผนการนำไปใช้ หรือทำแผนการทำงาน เพื่อให้บรรลุเป้าหมาย (Road Map) ที่สอดคล้องกับปัจจัยที่เป็นสภาพแวดล้อมองค์กร ทั้งภายในและภายนอก เช่น

- จริยธรรม และวัฒนธรรม
- กฎหมาย มาตรฐาน ระเบียบข้อบังคับ และนโยบาย
- ภารกิจ วิสัยทัศน์ และคุณค่า
- นโยบายและ แนวปฏิบัติด้านการกำกับดูแล
- แผนธุรกิจและกลยุทธ์ที่ตั้งไว้
- ต้นแบบสำหรับปฏิบัติงานและระดับวุฒิภาวะ
- รูปแบบ (Style) ในการบริหารจัดการ
- ความเสี่ยงที่ยอมรับได้
- ความสามารถและความพร้อมของทรัพยากร
- แนวปฏิบัติเฉพาะประเภทธุรกิจ

7 Enablers to Enterprise Goals



COBIT 5 for Regulators and Operators
แนวความคิดในการนำ GEIT ประยุกต์เพื่อการใช้งาน

ข้อแนะนำ / ข้อสังเกต บางประการ

- GEIT ออกแบบมาเพื่อเป็นแนวทางในการหลีกเลี่ยงการเผชิญอันตรายแอบแฝงที่มักจะพบอยู่เป็นปกติของกระบวนการทำงาน รวมทั้งในมุมมองจุดอ่อน ที่อาจมีการทุจริตได้
- การพัฒนาการกำกับให้ดีขึ้นอย่างต่อเนื่อง ควรประกอบด้วย
  - การประเมินตนเอง การวัดผล และเครื่องมือในการวิเคราะห์
  - การนำเสนอที่พุ่งเป้าไปถึงผู้รับสารที่หลากหลาย
  - คำจำกัดความที่ควรเข้าใจตรงกัน
  - การจัดทำเหตุผลทางธุรกิจ เพื่อสนับสนุนการนำการกำกับดูแลและการบริหารจัดการด้านไอทีระดับองค์กร ไปใช้และปรับปรุงให้ดีขึ้น
  - การรับรู้จุดที่มีปัญหา (Pain Point) และเหตุการณ์จุดชวน (Trigger Events)
  - การสร้างสภาพแวดล้อมที่เหมาะสมสำหรับการนำไปใช้งาน
  - ใช้ประโยชน์จาก COBIT5 / GEIT ในการระบุถึงช่องว่างและแนวทางการพัฒนาปัจจัยเอื้อ เช่น นโยบาย กระบวนการ หลักการ โครงสร้างองค์กร บทบาทและหน้าที่ความรับผิดชอบ

Questions?

ท่านพร้อมแล้วยังครับ สำหรับการก้าวสู่ กรอบการดำเนินงานทางธุรกิจ สำหรับการกำกับดูแลและการบริหารไอที ระดับองค์กร / GEIT – Governance of Enterprise IT


Thank you
www.itgthailand.com
e-mail : suvanasarn@gr