ภาพรวมของการตรวจสอบภายใน

โดย

กองตรวจสอบภาครัฐ

กรมบัญชีกลาง

พระราชบัญญัติวินัยการเงินการคลังของรัฐ พ.ศ. ๒๕๖๑

มาตรา ๗๙

ให้หน่วยงานของรัฐจัดให้มีการตรวจสอบภายใน การควบคุมภายใน และการบริหารจัดการความเสี่ยงโดยถือปฏิบัติตามมาตรฐานและหลักเกณฑ์ที่กระทรวงการคลังกำหนด

The Institute of Internal Auditors

- The International Professional Practices Framework (IPPF)
  - Mandatory Guidance
  - Recommended Guidance

Mandatory Guidance

- Core Principles for the Professional Practice of Internal Auditing
- Definition of Internal Auditing
- Code of Ethics
- International Standards for the Professional Practice of Internal Auditing

Recommended Guidance

- Implementation Guidance
- Supplemental Guidance

Mission of Internal Audit

- เพื่อเพิ่มและปกป้องคุณค่าขององค์กร โดยการให้ความเชื่อมั่น ให้คำแนะนำและให้ความเข้าใจอย่างท่องแท้ บนพื้นฐานของความเสี่ยง
- To enhance and protect organizational value by providing risk-based and objective assurance, advice, and insight.

+เพิ่มคุณค่า – ให้ความรู้ความเข้าใจในการพัฒนาประสิทธิผลของกระบวนการหรือการลดต้นทุน

+ปกป้องคุณค่า – ระบุงาน/กิจกรรมที่ความเสี่ยงยังไม่ได้รับการจัดการ

+ผ่าน 3 กิจกรรม

Source : The institute of Internal Auditors

Core Principles

หลักสำคัญที่ทำให้การตรวจสอบภายในมีประสิทธิผล

1. Demonstrates integrity.
2. Demonstrates competence and due professional care.
3. Is objective and free from undue influence (independent).
4. Aligns with the strategies, objectives, and risks of the organization.
5. Is appropriately positioned and adequately resourced.
6. Demonstrates quality and continuous improvement.
7. Communicates effectively.
8. Provides risk-based assurance.
9. Is insightful, proactive, and future-focused.
10. Promotes organizational improvement.

Source : The institute of Internal Auditors

ความหมายของการตรวจสอบภายใน

การตรวจสอบภายใน คือ การให้ความเชื่อมั่นและการให้คำปรึกษา อย่างเที่ยงธรรมและเป็นอิสระ เพื่อเพิ่มคุณค่าและปรับปรุงการดำเนินงานขององค์กรให้ดีขึ้น การตรวจสอบภายในช่วยให้องค์กรบรรลุเป้าหมายและวัตถุประสงค์ที่กำหนดไว้ ด้วยการประเมินและปรับปรุงประสิทธิผลของกระบวนการบริหารความเสี่ยง การควบคุม และการกำกับดูแลอย่างเป็นระบบ

บริการให้ความเชื่อมั่น

หมายถึง การตรวจสอบหลักฐานต่าง ๆ อย่างเที่ยงธรรม เพื่อนำมาประเมินผลอย่างเป็นอิสระในกระบวนการบริหารความเสี่ยง การควบคุม และการกำกับดูแลกิจการที่ดีของส่วนราชการ

บริการให้คำปรึกษา

หมายถึง กิจกรรมการให้คำแนะนำ และการให้บริการ ที่เกี่ยวข้องแก่ส่วนราชการ ลักษณะและขอบเขตของงานเป็นไปตามความตกลงร่วมกันกับส่วนราชการ โดยมีวัตถุประสงค์เพื่อเพิ่มคุณค่าให้หน่วยงานของรัฐ โดยการปรับปรุงกระบวนการ การกำกับดูแล การบริหารความเสี่ยง และการควบคุม

จรรยาบรรณ

1.หลักการ (Principles)

2. หลักปฏิบัติ (Rules of Conduct)

จรรยาบรรณ – หลักการ

1. ความซื่อสัตย์ (Integrity)

สร้างความไว้เนื้อเชื่อใจ / ทำให้วิจารณญาณของผู้ตรวจสอบภายในเป็นที่น่าเชื่อถือ

2. ความเที่ยงธรรม (Objectivity)

ความเที่ยงธรรมเยี่ยงผู้ประกอบวิชาชีพ / เป็นกลางไม่ลำเอียง
/ ไม่ปล่อยให้อคติหรือบุคคลอื่นมีอิทธิพลเหนือการประเมิน

3. การรักษาความลับ (Confidentiality)

เคารพคุณค่าและสิทธิของผู้เป็นเจ้าของในข้อมูล
/ ไม่เปิดเผยข้อมูลโดยปราศจากอำนาจหน้าที่ที่เหมาะสม

4. ความสามารถในหน้าที่ (Competency)

ใช้ความรู้ ทักษะ และประสบการณ์ที่จำเป็นในการปฏิบัติงานตรวจสอบภายใน

จรรยาบรรณ – หลักปฏิบัติ

1. ความซื่อสัตย์ (Integrity)

1.1 ซื่อสัตย์ ขยันหมั่นเพียร และมีสำนึกรับผิดชอบ

1.2 ปฏิบัติตามกฎหมายและเปิดเผยข้อมูลตามที่กฎหมาย

1.3 ไม่มีส่วนร่วมโดยเจตนาในกิจกรรมที่ขัดต่อกฎหมาย หรือการกระทำที่อาจเสื่อมเสีย

1.4 เคารพและสนับสนุนวัตถุประสงค์ที่ถูกต้องตามกฎหมายและหลักจริยธรรม

จรรยาบรรณ – หลักปฏิบัติ

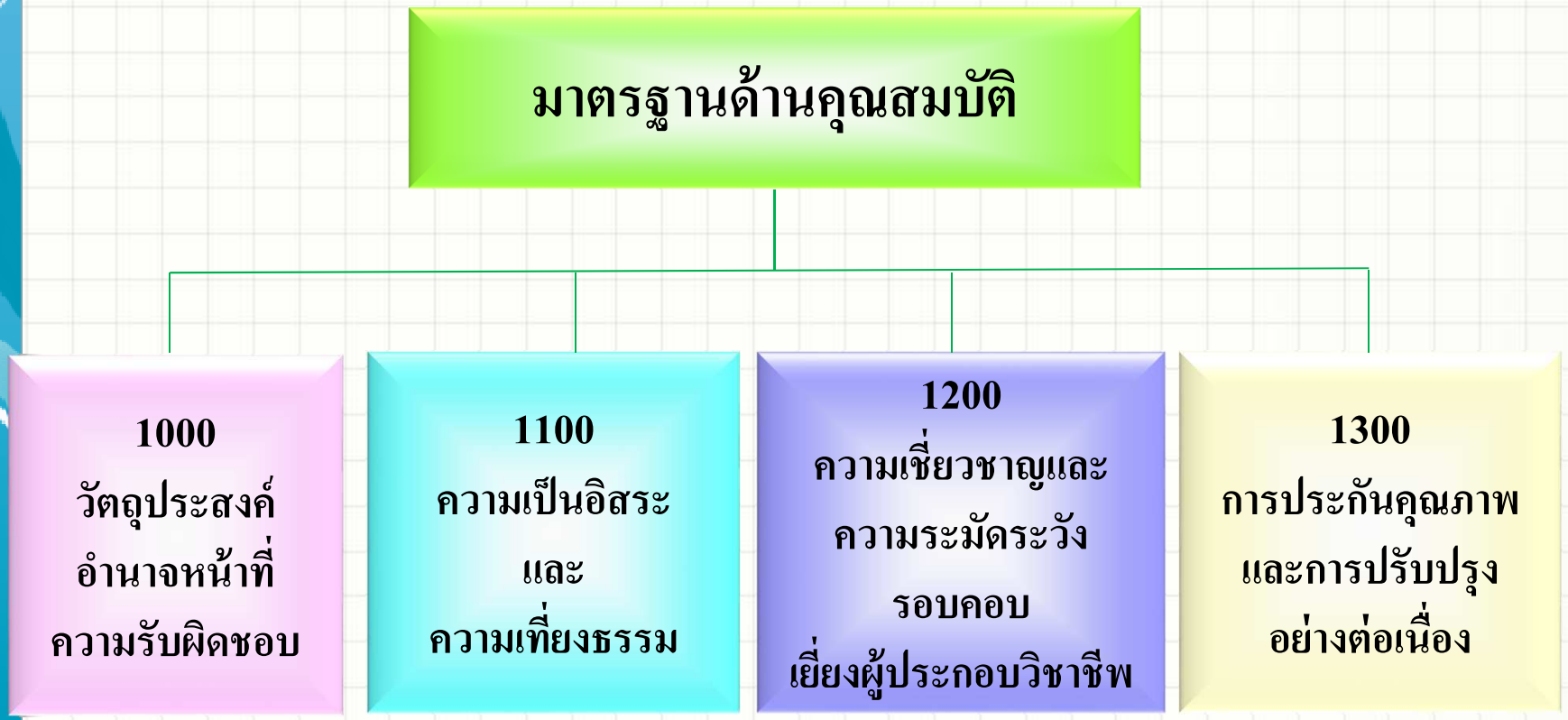
2. ความเที่ยงธรรม (Objectivity)

2.1 ไม่มีส่วนร่วมในกิจกรรมหรือความสัมพันธ์
ที่บั่นทอนหรืออาจบั่นทอนการประเมินอย่างเป็นกลาง ไม่ลำเอียงของตน

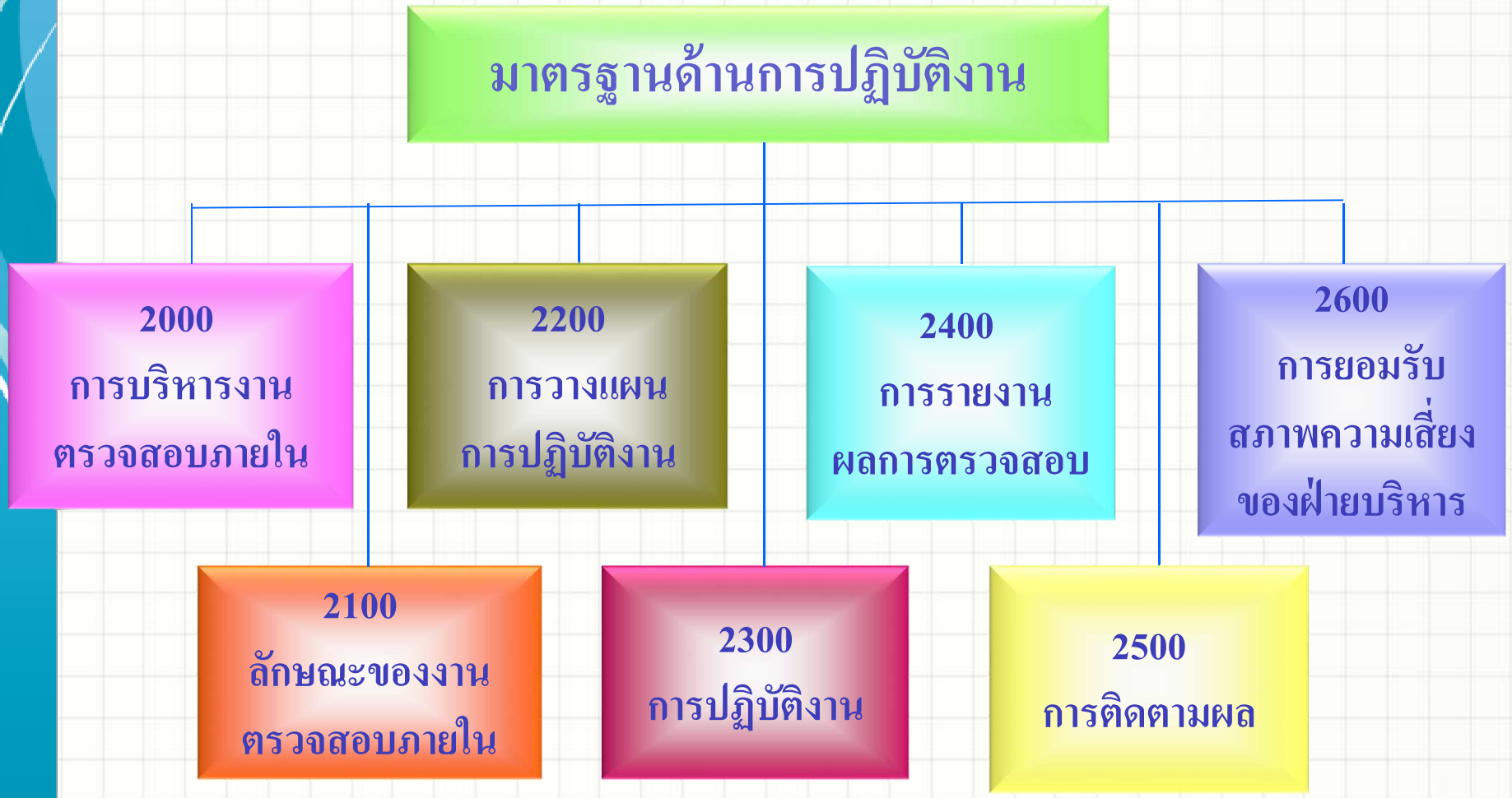
2.2 ไม่รับสิ่งตอบแทนใดๆ ที่บั่นทอนหรืออาจบั่นทอน
วิจารณญาณของผู้ประกอบวิชาชีพ

2.3 เปิดเผยความจริงทั้งหมดในการปฏิบัติงาน

มาตรฐานการตรวจสอบภายใน : มาตรฐานด้านคุณสมบัติ



มาตรฐานการตรวจสอบภายใน : มาตรฐานด้านการปฏิบัติงาน



การกำหนดรหัส

ABnn.Cn

A – 1 มาตรฐานคุณสมบัติ 2 มาตรฐานการปฏิบัติงาน

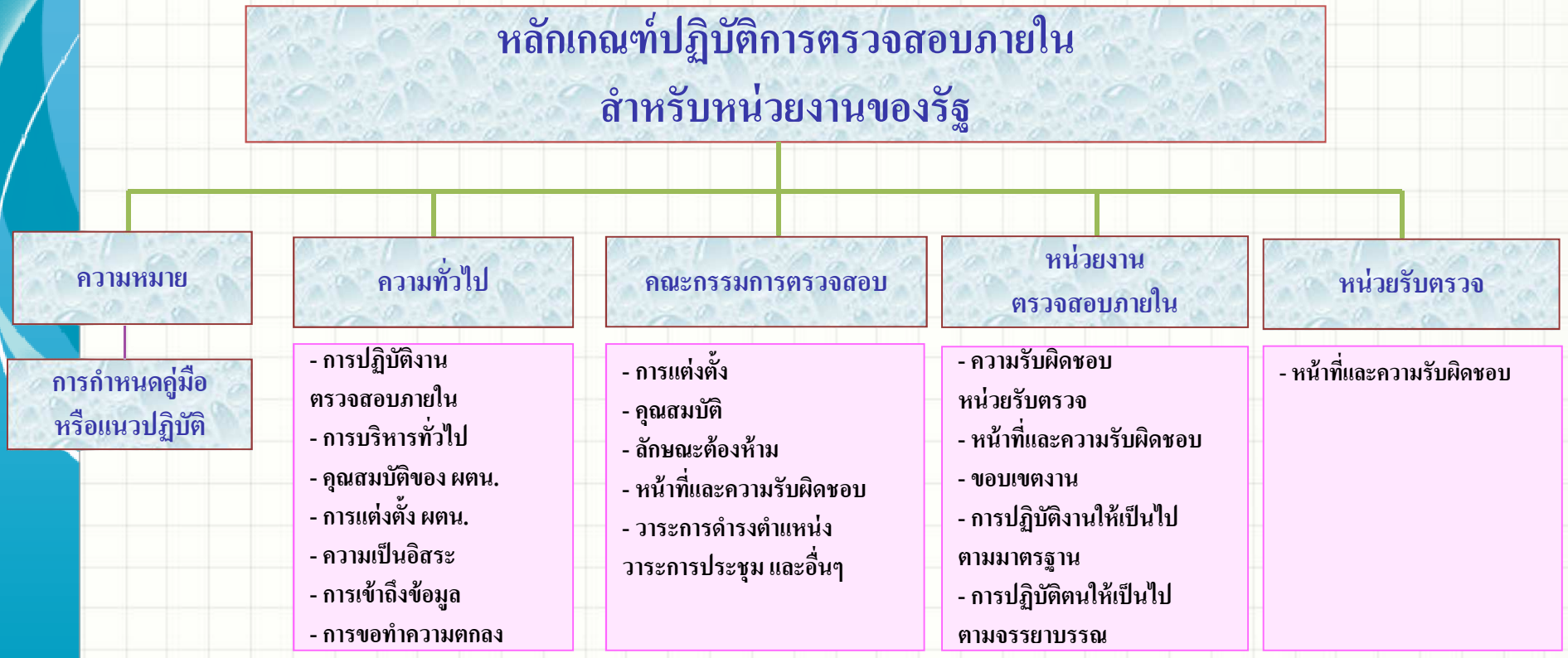
B – 0 – 3 สำหรับมาตรฐานคุณสมบัติ

0 – 6 สำหรับมาตรฐานการปฏิบัติงาน

C – A การให้บริการความเชื่อมั่น

C การให้บริการให้คำปรึกษา

หลักเกณฑ์ปฏิบัติการตรวจสอบภายใน : โครงสร้าง



Three lines Model

หลักการที่ 1 ธรรมาภิบาล

หลักการที่ 2 บทบาทของผู้กำกับดูแล

หลักการที่ 3 บทบาทของฝ่ายบริหารและด่านที่ 1 และ 2

หลักการที่ 4 บทบาทของด่านที่ 3

หลักการที่ 5 ความเป็นอิสระของด่านที่ 3

หลักการที่ 6 การสร้างและปกป้องคุณค่า

ความสัมพันธ์ระหว่างการตรวจสอบภายใน การบริหารจัดการความเสี่ยง และการควบคุม

การตรวจสอบภายในมีหน้าที่ในการประเมินผลการบริหารความเสี่ยงและการควบคุมว่ามีประสิทธิผลและให้คำแนะนำคณะกรรมการหรือผู้บริหารในการปรับปรุงกระบวนการ

การพัฒนาความรู้อย่างต่อเนื่อง

- CPD : Continuing Professional Development / CPE : Continuing Professional Education

แผนการตรวจสอบ : Risk – based Audit Plan

- เข้าใจองค์กร
- ระบุ ประเมิน จัดลำดับความเสี่ยง – Audit Universe / Risk Factors
- การประสานงานกับผู้ให้ความเชื่อมั่นอื่น – Assurance Map
- ประมาณการทรัพยากร
- ร่างแผนการตรวจสอบ
- เสนอแผนต่อหัวหน้าหน่วยงานของรัฐ

แผนการปฏิบัติงาน : Engagement Plan

- เข้าใจ Auditable Unit
- ประเมินความเสี่ยงเบื้องต้น รวมถึงความเสี่ยงด้านการทุจริต
- กำหนดวัตถุประสงค์และขอบเขต

  Business Objective -> Business Risk -> Audit Objective
- กำหนดเกณฑ์ที่ใช้ในการตรวจสอบ
- จัดสรรทรัพยากร - เพียงพอ และ เหมาะสม
- แนวทางการปฏิบัติงาน : Engagement Work Program
- ร่างแผนการปฏิบัติงาน
- อนุมัติแผนการปฏิบัติงาน

Computer assisted audit techniques : CAATs

- Excel and Word knowledge : COUNTIF, VLOOKUP
- ระบุข้อมูล นำเข้าข้อมูล ทดสอบข้อมูล รายงาน
- Data Analytics

IT Audit

ISACA - Certified Information Systems Auditor (CISA) Certification

- Cybersecurity Audit Certificate

การตรวจสอบ – ธรรมาภิบาล

- โครงสร้างพื้นฐาน
- ระบบงาน
- การบริหารจัดการและใช้ข้อมูล นโยบาย กระบวนการปฏิบัติงาน
- การควบคุมภายใน

ประเภทของ IT Control

- General Controls / Application Controls
- Governance Controls / Management Controls / Technical Controls
- Prevention Controls / Detection Controls / Prevention Controls

แหล่งที่มาของข้อมูล : GTAG 1 – Information Technology Risk and Controls

Examples : IT Risks

- Fraud
- Error
- Service Interruption and delays
- Disclosure of Confidential Information
- Intrusion
- Information Theft
- Information Manipulation
- Malicious software : Virus, Worm, Trojan
- Denial-of-service
- Web Site Defacements
- Extortion

Examples : IT Controls

- Physical Controls
- Technical controls
- Administrative Controls
- Segregation of duties
- Development and Maintenance Plans
- Biometric Identification
- Audit trail
- Backup
- Encryption
- Contingency plan

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์
เรื่อง แนวทางนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย
ด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553

หน่วยงานของรัฐต้องจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ อย่างน้อยปีละ 1 ครั้ง โดยผู้ตรวจสอบภายในหน่วยงานของรัฐ (Internal auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External auditor)

หน่วยงานของรัฐต้องกำหนดความรับผิดชอบที่ชัดเจน กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใดๆ แก่องค์กร ทั้งนี้ ให้ผู้บริหารระดับสูงสุดของหน่วยงาน (CEO) เป็นผู้รับผิดชอบต่อความเสี่ยงความเสียหาย หรืออันตรายที่เกิดขึ้น (ปรับปรุงแก้ไขตาม (ฉบับที่ 2) พ.ศ. 2556)

การทุจริต Fraud

1210.A2 – ผู้ตรวจสอบภายในต้องมีความรู้เพียงพอที่จะประเมินความเสี่ยงของการเกิดทุจริต และวิถีทางใน การบริหารจัดการทุจริตขององค์กร แต่ไม่จำเป็นต้องมีความเชี่ยวชาญเทียบเท่ากับผู้มีหน้าที่โดยตรงในการ ตรวจจับและสอบสวนการทุจริต

2120.A2 – หน่วยงานตรวจสอบภายในต้องประเมินความเป็นไปได้ของการเกิดการทุจริต และวิธีจัดการกับ ความเสี่ยงจากการทุจริตขององค์กร

2210.A2 – ในการกำหนดวัตถุประสงค์ของงานที่ได้รับมอบหมาย ผู้ตรวจสอบภายในต้องคำนึงถึงความเป็นไป ได้ที่จะเกิดข้อผิดพลาด การทุจริต การไม่ปฏิบัติตามกฎระเบียบ และความเสี่ยงอื่นๆ ที่มีนัยสำคัญ

การทุจริต Fraud

สาเหตุ

- มีแรงจูงใจ
- รู้วิธีการ
- มีโอกาส

ตัวอย่าง

- Lapping
- Skimming
- Check Kiting
- Fraud Disbursement
- Corruption – Procurement
- Bribery
- Information misrepresentation

ตัวอย่าง การควบคุมภายในด้านการเงิน

- การอนุมัติรายการ
- การสอบทาน
- การเก็บรักษาทรัพย์สิน
- การกระทบยอด
- การแบ่งแยกหน้าที่
- การสับเปลี่ยนหมุนเวียนงาน

การแบ่งแยกหน้าที่

- การอนุมัติ
- การปฏิบัติ
- การบันทึกบัญชี
- การเก็บรักษา