สรุปการอบรม Compliance and Compliance Audit

ณ โรงแรมอะริสตั้น สุขุมวิท 24 กรุงเทพฯ ในวันที่ 3 สิงหาคม 2562

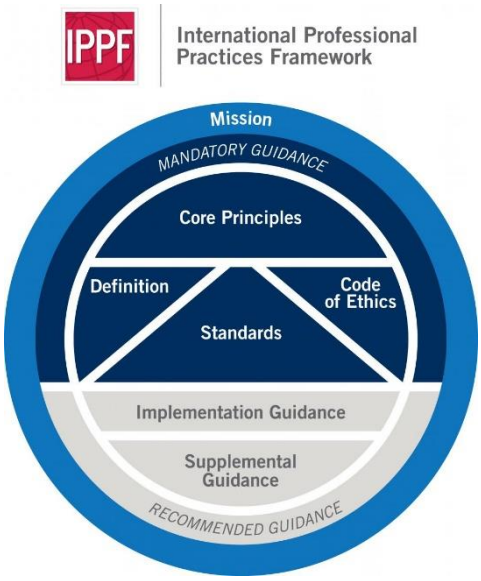
บรรยาย : คุณภูวนัย ชมรุ่ง จัดโดย : สมาคมผู้ตรวจสอบภายในแห่งประเทศไทย

Compliance คือ การกำกับกฎหมายและกฎระเบียบขององค์กร

Compliance Audit คือ การตรวจสอบการปฏิบัติตามข้อกำหนดขององค์กร

กรอบการปฏิบัติงาน มาตรฐาน หน้าที่ และภารกิจ

กรอบการปฏิบัติงานวิชาชีพตรวจสอบภายในระดับสากล (IPPF)



พันธกิจ (Mission) : เพื่อส่งเสริมและปกป้องคุณค่าในทางองค์กร โดยการให้ความเชื่อมั่นและให้คำปรึกษาอย่างเที่ยงธรรมและลึกซึ้ง โดยอาศัยเรื่องความเสี่ยงเป็นพื้นฐาน

คำนิยาม (Definition) : การตรวจสอบภายใน คือ การให้ความเชื่อมั่นและให้คำปรึกษาอย่างเที่ยงธรรมและเป็นอิสระเพื่อเพิ่มมูลค่าและปรับปรุงการดำเนินงานขององค์กร การตรวจสอบภายในช่วยให้องค์กรบรรลุเป้าหมายด้วยการประเมินและปรับปรุงประสิทธิผลของกระบวนการบริหารความเสี่ยง การควบคุมและการกำกับดูแลอย่างเป็นระบบ และเป็นระเบียบ

หลักจรรยาบรรณ (Code of Ethics) :

ความซื่อสัตย์ (Integrity)	ปฏิบัติหน้าที่ของตนด้วยความซื่อสัตย์ ขยันหมั่นเพียร และมีสำนึกรับผิดชอบ
ความเที่ยงธรรม (Objectivity)	เปิดเผยความจริงทั้งหมดที่ทราบ ซึ่งหากละเว้นไม่เปิดเผยแล้วอาจทำให้รายงานผลการตรวจสอบบิดเบือนไป
การรักษาความลับ (Confidentiality)	รอบคอบในการใช้และปกป้องข้อมูล ที่ได้มาระหว่างการปฏิบัติหน้าที่
ความสามารถในหน้าที่ (Competency)	พัฒนาความชำนาญ ประสิทธิผล และคุณภาพของบริการอย่างต่อเนื่อง

มาตรฐานสากลการปฏิบัติงานวิชาชีพการตรวจสอบภายใจ (Standards) :

ส่วนประกอบของ IIA Standards

ขึ้นต้นด้วยรหัส

1xxx คือ มาตรฐานคุณลักษณะงาน (Attribute Standards) แบ่งเป็น 4 มาตฐานย่อย ได้แก่ รหัส 1000 วัตถุประสงค์ อำนาจและภารหน้าที่

1100 ความเป็นอิสระและความเที่ยงธรรม

1200 ความเชี่ยวชาญและการใช้ความระมัดระวังในการประกอบวิชาชีพ

1300 โครงการประกันคุณภาพและปรับปรุงงาน

2xxx คือ มาตรฐานการปฏิบัติงาน (Performance Standards) ประกอบด้วย

รหัส 2000 การบริหารหน่วยงานตรวจสอบภายใน

2100 ลักษณะงาน การปฏิบัติตามกฎหมาย ระเบียบข้อบังคับ นโยบาย วิธีการปฏิบัติงานและสัญญา ได้แก่

2110 การกำกับดูแล เพื่อให้บรรลุวัตถุประสงค์ขององค์กร

2120 การบิรหารความเสี่ยง เพื่อให้เกิดความเชื่อมั่น บรรลุวัตถุประสงค์

2130 การควบคุม เพื่อให้เกิดความเชื่อมั่นบรรลุวัตถุประสงค์ เป้าหมาย

2200 การวางแผนงานที่ได้รับมอบหมาย

2300 การปฏิบัติงานที่ได้รับมอบหมาย

2400 การสื่อสารผลการปฏิบัติงาน

2500 การปฏิบัติงานที่ได้รับมอบหมาย

2600 การสื่อสารผลการปฏิบัติงาน

1-2xxx A,C คือ มาตรฐานการนำไปใช้ (Implementation Standards)

Recommended Guidance : แนวทางที่แนะนำให้ใช้

1. แนวทางในการนำไปปฏิบัติ (Implementation Guidance : IG)

เป็นการขยายความมาตรฐานด้านคุณสมบัติและด้านการปฏิบัติงานโดยให้ข้อกำหนดในการปรับใช้กับการบริการมี 2 ลักษณะ ได้แก่

- การบริการให้ความเชื่อมั่น (Assurance Services) เกี่ยวข้องกับการประเมินหลักฐานอย่างเที่ยงธรรมในกระบวนการบริหารความเสี่ยง การควบคุมและการกำกับดูแลกิจการที่ดีขององค์กรโดยต้องปฏิบัติงานด้วยความระมัดระวังรอบคอบตามมาตรฐานวิชาชีพและเยี่ยงผู้ประกอบวิชาชีพเพื่อให้ความเห็นเพื่อปรับปรุง ขอบเขตให้ความเชื่อมั่นแต่ละงาน โดยเกี่ยวข้อง 3 ฝ่าย ได้แก่ ผู้รับตรวจ, ผู้ตรวจสอบ, และผู้ใช้รายงาน

- การบริการให้คำปรึกษา (Consulting Services) กิจกรรมการให้คำแนะนำ ลักษณะและขอบเขตเป็นไปตามความตกลงร่วมกัน โดยมีวัตถุประสงค์ Add Value & Improve เกี่ยวข้องกับ ผู้ตรวจสอบ และผู้ขอคำปรึกษา

2. แนวทางเสริม (Supplemental Guide : SG)

ความสำคัญของ การกำกับกฎหมายและกฎระเบียบองค์กร **(Compliance) & (Audit)** การตรวจสอบ

ความสำคัญของการกำกับกฎหมายและกฎระเบียบขององค์กร การปฏิบัติงานขององค์กรต้องยึดถือและปฏิบัติตามนโยบาย แผนงาน วิธีการปฏิบัติงาน กฎหมาย ระเบียบข้อบังคับ สัญญาตลอดจนข้อกำหนดอื่น ๆ ทั้งภายในและภายนอกขององค์กร เมื่อกฎหมาย ระเบียบ กฎเกณฑ์ต่าง ๆ ไม่ตายตัวมีการเปลี่ยนแปลง จะต้องมีกระบวนการตรวจสอบเพื่อติดตาม การกำกับปฏิบัติงานให้เป็นไปตามข้อกำหนดของทางการกฎหมายที่เกี่ยวข้อง สัญญาที่มีข้อผูกพันตามเพื่อไม่ให้การดำเนินงานขององค์กรมีความเสียหายอันเกิดจากการฝ่าฝืน โดยดำเนินการดังนี้

- การดำเนินการเปลี่ยนแปลงให้ครบถ้วน ทันตามที่กฎหมายกำหนด
- ควบคุมการดำเนินการเปลี่ยนแปลง
  - ติดตามให้เป็นตามแผนการปฏิบัติการ ทันวันที่กำหนดให้มีการบังคับใช้
  - ให้รายงานต่อฝ่ายบริหารเพื่อให้มั่นใจ
- นอกจากการเปลี่ยนแปลงของกฎหมาย กฎเกณฑ์ต่าง ๆ สถาบันการเงินยังมีผลิตภัณฑ์บริการที่ขยายเพิ่มขึ้น ตลอดจนขยายฐานลูกค้า ช่องทางในการจำหน่ายต่าง ๆ
  - กระบวนการออก หรือปรับปรุงผลิตภัณฑ์/บริการใหม่ ควรกำหนดให้มีการนำ Gap analysis มาวิเคราะห์การปฏิบัติตามระเบียบ ข้อบังคับทุกด้าน
  - Compliance เข้าร่วมในการควบคุมการเปลี่ยนแปลงที่เกิดขึ้นหรือไม่อย่างไร

เมื่อองค์กรไม่ให้ความสำคัญกับการกำกับกฎหมายและกฎระเบียบองค์กรอันเป็นความเสี่ยงอันเนื่องมาจากการไม่ปฏิบัติตามกฎหมาย กฎเกณฑ์ ข้อบังคับ มาตรฐาน แนวปฏิบัติที่เกี่ยวข้อง และจรรยาบรรณในดำเนินงาน ซึ่งอาจทำให้เกิดความเสียหายทางการเงินจำนวนสูง ความเสียหายต่อชื่อเสียงขององค์กร หรือการถูกทางการแทรกแซง

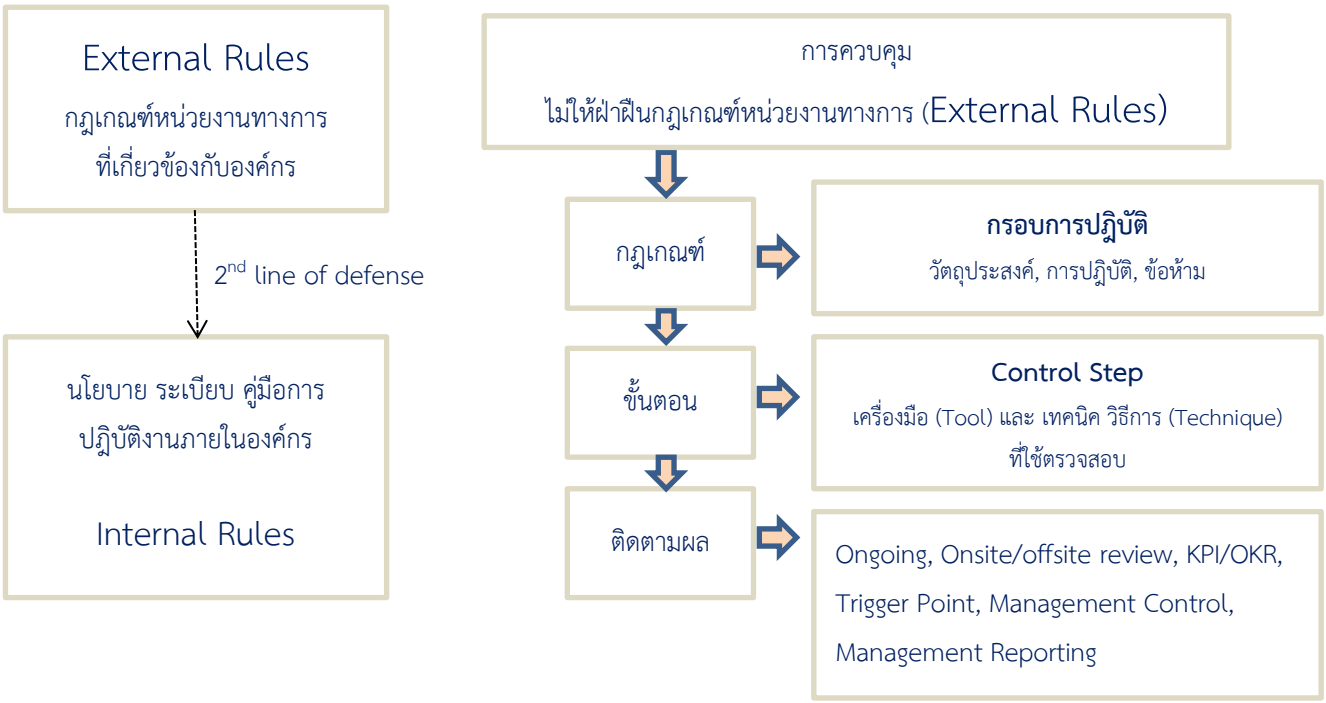
ความแตกต่างระหว่าง Compliance และ Internal audit

Compliance audit (การตรวจสอบกฎระเบียบ)	Internal audit (ตรวจขั้นตอนการปฏิบัติงาน)
- กำหนดขอบเขตวิธีการปฏิบัติ ซึ่งจะให้เป็นการปฏิบัติตามสิ่งใด สิ่งหนึ่ง หรือเรื่องใดเรื่องหนึ่ง ทั้งนี้ ต้องทำการติดตามผลว่ามีการปฏิบัติตามขอบเขตที่กำหนดหรือไม่ เป็นไปตามวัตถุประสงค์ที่กำหนดหรือไม่ - ข้อพิจารณา นโยบายการกำกับดูแลปฏิบัติงานให้เป็นไปตามกฎหมาย กฎระเบียบขององค์กร(Compliance policy), แนวทางการปฏิบัติตามนโยบายการกำกับดูแลการปฏิบัติงาน (compliance framework), ขั้นตอนการปฏิบัติตามนโยบายการกำกับดูแล และปฏิบัติงาน(compliance program) - ตัวอย่างเช่น การตรวจสอบการทำสัญญาระหว่างกัน ซึ่งต้องเป็นไปตามข้อกำหนดของทางกฎหมายที่เกี่ยวข้อง สัญญาที่มีข้อผูกพันตามเพื่อไม่ให้การดำเนินงานมีความเสียหายอันเกิดจากการฝ่าฝืน	- วิธีการในการพิสูจน์ข้อเท็จจริงที่ต้องมีหลักฐาน ที่แน่ชัด เพื่อให้ผู้ตรวจสอบสามารถให้ความเห็นในเรื่องนั้น ๆ ได้ - ลักษณะงาน ภายในองค์กร (Governance), ความเสี่ยงที่อาจเกิดขึ้น (Risk), การควบคุมภายใน(Control) - ตัวอย่างเช่น การตรวจสอบขั้นตอนการปฏิบัติงานของหน่วยงานในองค์กร โดยการประเมินความเสี่ยง เพื่อให้ได้มาซึ่งความเสี่ยงสูงเข้าไปตรวจสอบ เพื่อให้มั่นใจได้ว่าสามารถควบคุมการปฏิบัติงานได้อย่างมีประสิทธิภาพและประสิทธิผลสูงสุด
บทบาท Three lines of Defense (3LoD) ได้แก่ - 1st Line : Risk Owner หน่วยงานธุรกิจและหน่วยงานที่สนับสนุนต่าง ๆ เป็นเจ้าของความเสี่ยงหลักและรับผิดชอบความเสี่ยงทั้งหมดที่เกิดขึ้นจากกิจกรรมทางธุรกิจและหรือกระบวนการ - 2nd Line : Risk Controller เจ้าของกระบวนการบริหารความเสี่ยง มีหน้าที่รับผิดชอบในการออกแบบกรอบการควบคุมความเสี่ยงและการประเมินความเสี่ยงอย่างเป็นอิสระ - 3rd Line : Group/Internal Audit (Assurance service) หน่วยงานภายใน มีความเป็นอิสระและเป็นกลางเพื่อประเมินประสิทธิผลของการบริหารความเสี่ยง การควบคุมภายในและกระบวนการกำกับดูแล	

การกำกับดูแล และการตรวจสอบ *ควรปฏิบัติงานตามหลักการประเมินความเสี่ยง (Risk Based Audit)*

คุณสมบัติที่สำคัญของ Internal Auditor

1. เข้าใจการบริหารความเสี่ยง
2. รอบรู้ข้อบังคับที่เกี่ยวข้องกับองค์กร สามารถใช้ Compliance Universe เพื่อประเมินความครบถ้วนของกฎเกณฑ์ทั้งหมดที่เกี่ยวข้องกับองค์กรและนำมาใช้ประกอบการวางแผนงานตาม Risk-based เพื่อจะได้แน่ใจว่างานครอบคลุมความเสี่ยง
3. เข้าใจการควบคุมและประเมินการควบคุม



การระบุและประเมินความรุนแรงของความเสี่ยง

องค์กรจัดทำ Compliance Universe โดยการระบุความเสี่ยงใหม่ และความเสี่ยงที่เปลี่ยนแปลงไปที่สอดคล้องกับกลยุทธ์ขององค์กร

ความเสี่ยง อาจเกิดจาก

- การเปลี่ยนวัตถุประสงค์ของธุรกิจ เช่น ใช้กลยุทธ์ใหม่ขององค์กร
- การเปลี่ยนกฎหมายข้อบังคับเกี่ยวกับธุรกิจ
- เป็นเรื่องที่ไม่รู้มาก่อน
- เป็นเรื่องที่รู้มาก่อนแต่เพิ่งมีผลกระทบกับธุรกิจ

ความรุนแรงของความเสี่ยง (Severity) นิยมพิจารณาจากความน่าจะเกิด (Likelihood) และผลกระทบ (Impact) หรือปัจจัยอื่น ตัวอย่างเช่น :

ความน่าจะเกิด หมายถึง โอกาสความเป็นไปได้ที่จะเกิดความเสี่ยง อาจกำหนดตามค่าความน่าจะเกิดตามช่วงเวลา หรือตามค่าความถี่ที่จะเกิด ซึ่งมีหลายวิธี เช่น กำหนดเป็นช่วงระดับตามอัตราร้อยละ ตามความถี่

ผลกระทบ หมายถึง ผลลัพธ์หรือผลกระทบของความเสี่ยง ซึ่งอาจกำหนดเป็นจำนวน ค่าช่วงของผลกระทบจากความเสี่ยงนั้น และอาจมีค่าบวกหรือลบ

การปฏิบัติตามเกณฑ์ (Compliance Function) มีดังนี้

- ระบุความเสี่ยงด้านการปฏิบัติตามกฎเกณฑ์ ควรระบุเอกสารและประเมินความเสี่ยงด้านการปฏิบัติตามกฎเกณฑ์ที่เกี่ยวข้องกับกิจกรรมทางธุรกิจ รวมถึงแนวทางปฏิบัติทางธุรกิจการจัดตั้งธุรกิจหรือการเปลี่ยนแปลงสำคัญขององค์กร

- เป็นศูนย์กลางในการให้คำแนะนำและที่ปรึกษา เกี่ยวกับกฎหมาย กฎเกณฑ์ต่าง ๆ แก่ผู้บริหารระดับสูงและพนักงาน

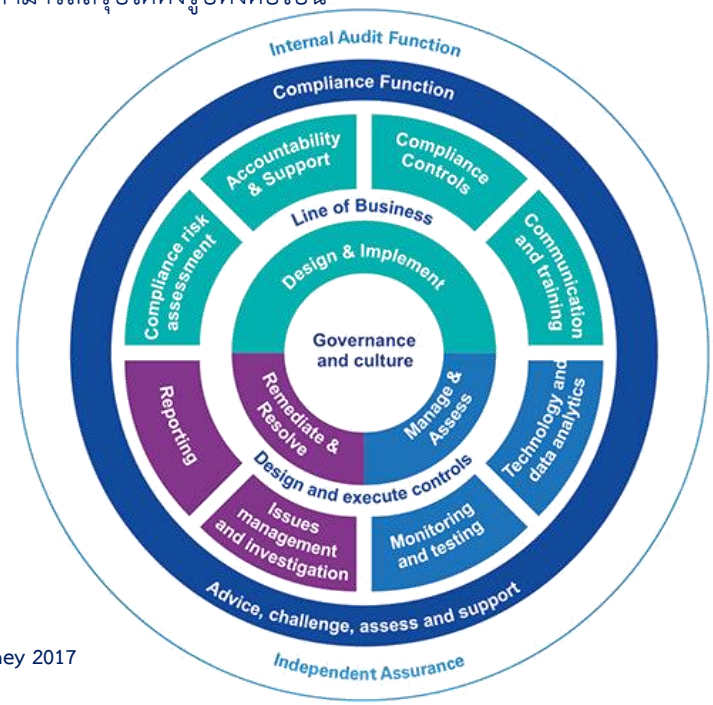
- การทดสอบการปฏิบัติงาน
- รายงานผลการปฏิบัติงาน

- พิจารณาวิธีการวัดความเสี่ยงด้านการปฏิบัติตามกฎเกณฑ์

- ประสานงานกับหน่วยงานบริหารความเสี่ยงและหน่วยงานที่เกี่ยวข้อง เพื่อจัดทำและดำเนินการตามแผน

- ประเมินความเหมาะสมของขั้นตอนและแนวทางตามกฎเกณฑ์เพื่อติดตามและเสนอแนะเพื่อแก้ไข

แนวทางการปฏิบัติตามนโยบาย การกำกับดูแล การปฏิบัติงานให้เป็นไปตามกฎหมาย กฎ ระเบียบ ขององค์กร (Compliance Framework) สามารถสรุปได้ดังรูปดังต่อไปนี้



อ้างอิง : KPMG, the Compliance journey 2017

หลักการและเทคนิคการตรวจสอบ Compliance Audit (Audit Universe, Audit Planning)

ประเภทของการตรวจสอบ Assurance Service

- การตรวจสอบการดำเนินงาน (Operation Audit)
- การตรวจสอบผลการปฏิบัติงาน (Performance Audit)
- การตรวจสอบการปฏิบัติตามกฎระเบียบ (Compliance Audit) เป็นการตรวจสอบการปฏิบัติงานต่าง ๆ ขององค์กรว่าเป็นไปตามนโยบาย กฎหมาย ระเบียบ ข้อบังคับ คำสั่ง มติคณะรัฐมนตรีที่เกี่ยวข้อง ตามข้อกำหนดทั้งจากภายนอกและภายในองค์กร รวมถึงการปฏิบัติตามระเบียบปฏิบัติขององค์กรและปฏิบัติตามสัญญาต่าง ๆ ที่มีกับคู่สัญญา การตรวจสอบประเภทนี้ อาจจะทำการตรวจสอบโดยเฉพาะหรือถือเป็นส่วนหนึ่งของการตรวจอสอบทางการเงิน หรือการตรวจสอบการดำเนินงาน
- การตรวจสอบทางการเงิน (Financial Audit)
- การตรวจสอบสารสนเทศ (Information Technology Audit)

แนวคิดสำคัญของ Compliance Audit

- ไม่เน้นตรวจสอบว่ามี “การทำผิด” หรือไม่
- เน้นตรวจสอบว่ามี “กระบวนการป้องกัน ไม่ให้เกิดการฝ่าฝืนกฎเกณฑ์ทางการ”
- เน้นตรวจสอบว่ามี “กระบวนการ Detective control” เพื่อแก้ไขการฝ่าฝืนได้ทันที
- เน้นตรวจสอบว่ามี “จุดอ่อน” ในการจัดการ Compliance Risk หรือไม่

การรายงาน และการติดตามผล

องค์ประกอบของข้อสังเกต/ข้อตรวจพบ

- สิ่งที่เป็นอยู่ (Condition) หมายถึง สิ่งที่ตรวจพบว่ามีการปฏิบัติที่เป็นหรือไม่เป็นไปตามกฎระเบียบ ข้อบังคับ หรือสิ่งที่ขัดแย้งกับหลักเหตุผล หรือ หลักวิชาการที่ดี
- สิ่งที่ควรเป็น (Criteria) หมายถึง มาตรฐาน (Standard) มาตรฐานวิชาชีพ กฎ ระเบียบ กฎหมาย ข้อบังคับเกี่ยวกับเรื่องนั้น หลักวิชาการที่ดี หรือหลักสามัญสำนึกที่ยอมรับกันทั่วไป
- สาเหตุที่ทำให้เกิด (Cause) หมายถึง สาเหตุที่ทำให้สิ่งที่เป็นอยู่ต่างจากสิ่งที่ควรเป็น ผู้ตรวจสอบควรค้นหาสาเหตุที่แท้จริง เพื่อเป็นแนวทางในการปรับปรุงแก้ไขต่อไป
- ผลกระทบที่เกิดขึ้นหรือที่อาจเกิดขึ้น (Effect) หมายถึง ความเสียหายที่เกิดขึ้นแล้ว หรือความสี่ยงที่อาจเกิดขึ้นซึ่งอาจนำเสนอในลักษณะเชิงปริมาณ เช่น เป็นจำนวนเงิน ผลผลิต หรือเป็นหน่วยวัดอื่น ๆ
- ข้อเสนอแนะ (Recommendation) หมายถึง สิ่งที่ตรวจพบที่นำเสนอในรายงาน ซึ่งอาจเป็นข้อเสนอแนะที่ช่วยให้การปฏิบัติงานรัดกุม สะดวก และมีประสิทธิภาพยิ่งขึ้น หรือเร่งรัดให้ปฏิบัติตามมาตรฐาน เพื่อป้องกันไม่ให้เกิดความเสี่ยง

ตัวอย่าง :

สิ่งที่เป็นอยู่	สิ่งที่ควรเป็น	สาเหตุ	ผลกระทบ	ข้อเสนอแนะ
ไม่มีเอกสารหลักฐานแสดงตนของลูกค้าเพื่อเปิดบัญชีเงินฝาก	มีเอกสารหลักฐานการแสดงตนของลูกค้าก่อนเปิดบัญชีทุกครั้ง เช่น บัตรประชาชน	พนักงานไม่ทราบขั้นตอนการเปิดบัญชี	อาจจะถูกต้องระวางโทษปรับไม่เกินหนึ่งล้านบาท และปรับอีกไม่เกินวันละหนึ่งหมื่นบาท ตลอดเวลาที่ยังฝ่าฝืนอยู่ หรือจนกว่าจะได้ปฏิบัติให้ถูกต้อง	ควรจัดให้มีการอบรมพนักงาน

ข้อควรปฏิบัติในการรายงานผลการตรวจสอบ

- ควรรายงานโดยไม่ชักช้า
- การรายงาน ควรรวมถึงวัตถุประสงค์ ขอบเขต ข้อสรุปและข้อเสนอแนะเพื่อการปรับปรุงงาน
- ควรมีความเห็นในการสรุปภาพรวมตามความเหมาะสม
- ควรรายงานผลงานที่น่าพอใจของผู้รับตรวจด้วย
- คุณภาพรายงาน ควรมีความถูกต้อง เที่ยงธรรม กระชับ สร้างสรรค์ ครบถ้วน และทันการ

ผู้เข้ารับการอบรม/และผู้จัดทำสรุป :

นางสาวศุภลักษณ์ บุญนะรา ตำแหน่งนักวิชาการตรวจสอบภายใน

นางสาวสุวภัทร ขวัญเมือง ตำแหน่งนักวิชาการตรวจสอบภายใน