



สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย (คปภ.)  
การประชุมชี้แจงโครงการศึกษาและพัฒนาแนวทางการตรวจสอบ  
ระบบเทคโนโลยีสารสนเทศ (IT Audit Kick off Meeting)

# หัวข้อนำเสนอ

- บทสรุปสำหรับผู้บริหาร
- ผลการสำรวจ 2017 Hot Topics for IT Internal Audit in Financial Services
- ประสพการณ์และผลงานอ้างอิง
- ขอบเขตงานและแนวทางการดำเนินงาน
- แผนงานโครงการ

# บทสรุปสำหรับผู้บริหาร

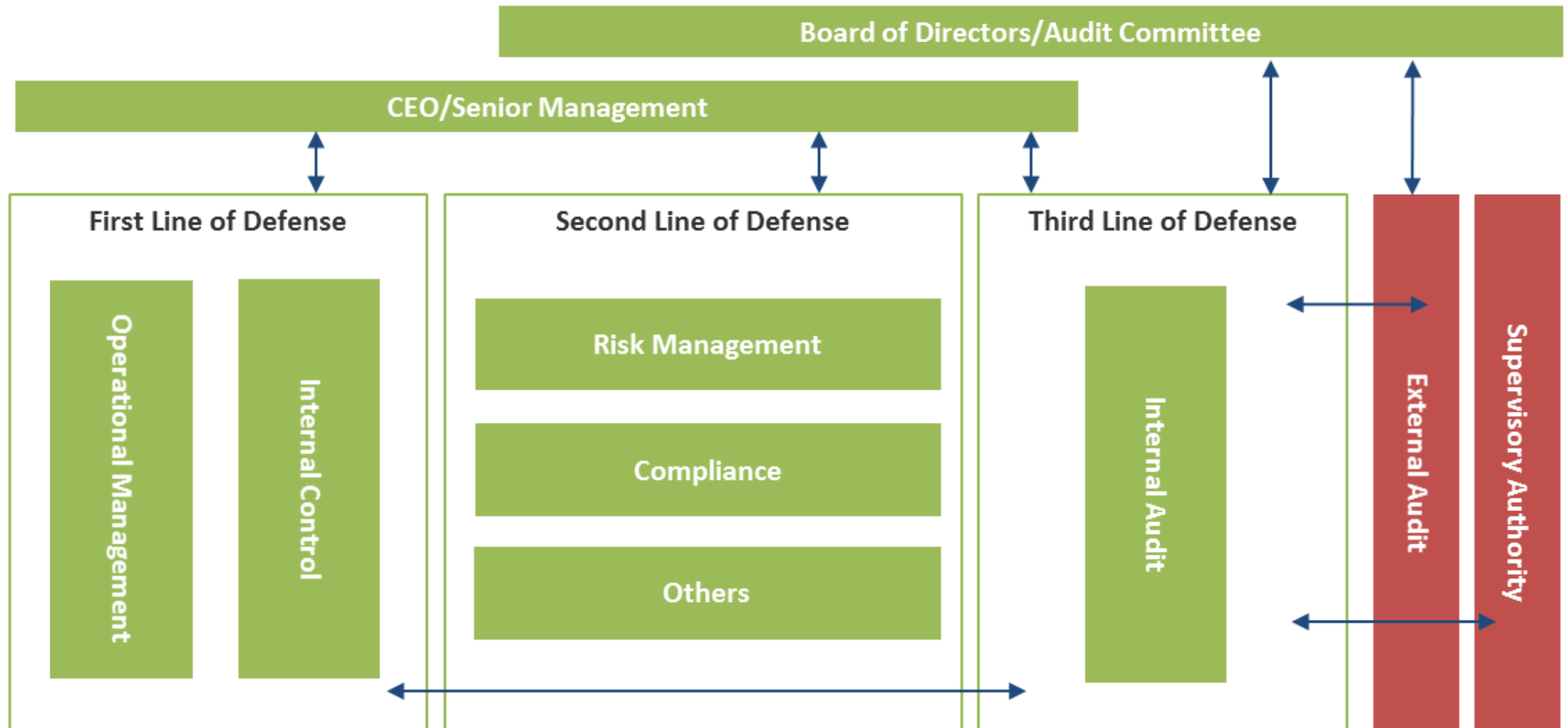
# บทสรุปสำหรับผู้บริหาร

ภายใต้แผนพัฒนาการประกันภัย ฉบับที่ 3 (พ.ศ. 2559–2563) ได้กำหนดมาตรการเพื่อเพิ่มศักยภาพให้กับอุตสาหกรรมประกันภัย โดยการส่งเสริม สนับสนุน และกำกับการใช้เทคโนโลยีดิจิทัล ในการดำเนินธุรกิจ เช่น ระบบเทคโนโลยีสารสนเทศสำหรับการปฏิบัติงาน การทำธุรกรรมผ่านสื่ออิเล็กทรอนิกส์ (E-Insurance) การชดเชยค่าสินไหมทดแทนผ่านสื่ออิเล็กทรอนิกส์ (E-Claim) เป็นต้น ทั้งนี้ การพัฒนาเพื่อมุ่งสู่ระบบดิจิทัลข้างต้น ย่อมส่งผลกระทบต่อกิจกรรมที่สำคัญของบริษัทประกันภัย อันประกอบด้วยระบบการรับประกันภัย ระบบการเงินและบัญชี ระบบการจ่ายค่าสินไหมทดแทนและการจ่ายผลประโยชน์ ตามกรมธรรม์ประกันชีวิต ซึ่งกระบวนการดังกล่าว มีความเสี่ยงที่อาจกระทบต่อความมั่นคงในการดำเนินธุรกิจของบริษัทประกันภัย และส่งผลต่อเนื่องไปยังการคุ้มครองสิทธิประโยชน์ของผู้เอาประกันภัยในอนาคต

สำนักงาน คปภ. จึงจำเป็นต้องเร่งศึกษาและพัฒนาแนวทางการตรวจสอบเทคโนโลยีสารสนเทศ (IT audit) เพื่อสร้างเครื่องมือในการกำกับดูแลและตรวจสอบบริษัทประกันภัย พร้อมทั้งพัฒนาองค์ความรู้และทักษะของบุคลากรด้านตรวจสอบ ให้สามารถปฏิบัติงานด้าน IT Audit ได้อย่างมีประสิทธิภาพ รวมถึงเพื่อส่งเสริมให้บริษัทประกันภัยมีการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ที่มีมาตรฐานและเป็นที่ยอมรับในระดับสากล

สำนักงาน คปภ. จึงจัดจ้างบริษัท ดีลอยท์ ทูช ไร้มัทสึ ซายยส ที่ปรึกษา จำกัด (บริษัทที่ปรึกษา) ดำเนินงานโครงการศึกษาและพัฒนาแนวทางการตรวจสอบระบบเทคโนโลยีสารสนเทศ และร่วมกันตรวจสอบระบบเทคโนโลยีสารสนเทศ (IT Audit Co-sourcing)

# Three Lines of Defense



Source: Institute of Internal Auditors: The Three Lines of Defense in Effective Risk Management and Control

# ผลการสำรวจ

**Deloitte.**



## **Storming ahead**

2017 Hot Topics for IT Internal  
Audit in Financial Services

An internal audit viewpoint

# 2017 Hot Topics for IT Internal Audit in Financial Services

## Top 5 Risk

Rank	๒๐๑๗	๒๐๑๖	๒๐๑๕	๒๐๑๔
๑	Cyber Security	Cyber Security	Cyber Security	Large Scale Change
๒	Strategic Change	Strategic Change	IT Disaster Recovery & Resilience	IT Governance & IT Risk Management
๓	Data Management & Data Governance	Third-Party Management	Large Scale Change	Identity & Access Management
๔	Third-Party Management	IT Disaster Recovery & Resilience	Enterprise Technology Architecture	Data Management & Data Governance
๕	IT Disaster Recovery & Resilience	Data Management & Data Governance	Third-Party Management	Third-Party Management

# 2017 Hot Topics for IT Internal Audit in Financial Services

## By Sector

Rank	Financial Services	Retail Banking	Capital Market	Insurance/ Investment Management
๑	Cyber Security	Cyber Security	Large Scale/ Strategic Change	<b>Cyber Security</b>
๒	Strategic Change	Large Scale/ Strategic Change	Cyber Security	<b>Third-Party Management</b>
๓	Data Management & Data Governance	Data Management & Data Governance	Enterprise Technology Architecture/ Merger/ Integration/ Obsolescence	<b>IT Governance &amp; IT Risk Management</b>
๔	Third-Party Management	IT Governance & IT Risk Management	Third-Party Management	<b>Merger/ Integration</b>
๕	IT Disaster Recovery & Resilience	Information Security	Data Management & Data Governance	<b>Large Scale/ Strategic Change</b>



# 2017 Hot Topics for IT Internal Audit in Financial Services

## Challenges for Insurance Sector

Rank	Financial Services	Retail Banking	Capital Market	Insurance/ Investment Management
1	Cyber Security	Cyber Security	Large Scale/ Strategic Change	Cyber Security
2	Strategic Change	Large Scale/ Strategic Change	Cyber Security	Third-Party Management
3	Data Management & Data Governance	Data Management & Data Governance	Enterprise Technology Architecture/ Merger/ Integration/ Obsolescence	IT Governance & IT Risk Management
4	Third-Party Management	IT Governance & IT Risk Management	Third-Party Management	Merger/ Integration
5	IT Disaster Recovery & Resilience	Information Security	Data Management & Data Governance	Large Scale/ Strategic Change



The insurance sector is facing similar challenges, focusing on **streamlining their complex legacy environments** and establishing appropriate **governance and risk frameworks** to manage the **risks arising from the use of new technologies**. Interestingly, the topic of Data Management and Governance is not in the Top 10 for insurance firms, possibly due to prior years' attention over data through Solvency II initiatives.



# 2017 Hot Topics for IT Internal Audit in Financial Services

## Internal Audit Viewpoints – Top Spots

๑. Cyber Security
๒. Strategic Change
๓. Data Management & Data Governance
๔. Third-Party Management
๕. IT Disaster Recover & Resilience
๖. IT Governance & IT Risk Management
๗. Information Security
๘. Enterprise Technology Architecture
๙. Cloud Computing
๑๐. Digital & Mobile Risk



# ประสบการณ์และผลงานอ้างอิง

# ประสบการณ์และผลงานอ้างอิงที่สำคัญ

## ผลงานอ้างอิงที่สำคัญที่เกี่ยวข้องกับหน่วยงานกำกับดูแล

ธนาคารแห่งประเทศไทย	ปี 2560	เป็นที่ปรึกษาในการให้ข้อเสนอแนะและความเห็นในการจัดทำประกาศและแนวปฏิบัติ (Implementation Guideline) ด้านการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ และ Cyber Resiliency Assessment Framework ของ สถาบันการเงิน
ธนาคารแห่งประเทศไทย	ปี 2559	เป็นผู้ตรวจสอบในการตรวจประเมินเสถียรภาพของระบบเทคโนโลยีสารสนเทศที่รองรับระบบรองรับการโอนเงินมูลค่าสูง โดยอ้างอิงมาตรฐานสากล และแนวปฏิบัติที่ดี (Good Practice)
ธนาคารแห่งประเทศไทย	ปี 2557	เป็นที่ปรึกษาในการจัดทำแนวปฏิบัติที่ดีสำหรับการควบคุมความเสี่ยงของระบบงานเทคโนโลยีสารสนเทศที่สนับสนุน online banking และ e-money (IT Best Practices)
ธนาคารแห่งประเทศไทย	ปี 2556	เป็นที่ปรึกษาในการจัดทำแนวปฏิบัติที่ดีสำหรับการควบคุมความเสี่ยงของระบบงานเทคโนโลยีสารสนเทศที่สนับสนุนธุรกรรมฝาก ถอน โอน (IT Best Practices)

# ประสบการณ์และผลงานอ้างอิงที่สำคัญ

## ผลงานอ้างอิงงานตรวจสอบด้านเทคโนโลยีสารสนเทศ และการให้คำปรึกษา ในการตรวจสอบและความปลอดภัยด้านเทคโนโลยีสารสนเทศ

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)	ปี 2558	เป็นผู้ตรวจสอบในการตรวจสอบระบบเทคโนโลยีสารสนเทศ
รัฐวิสาหกิจขนาดกลาง	ปี 2558	เป็นผู้ตรวจสอบในการตรวจสอบระบบเทคโนโลยีสารสนเทศ
กลุ่มบริษัท ปตท.	ปี 2556-2560	เป็นที่ปรึกษาและดำเนินการติดตั้งระบบ Continuous Control Monitoring System (CCMS) ของ บริษัท ปตท. จำกัด (มหาชน)
ผู้ให้บริการด้านเทคโนโลยีสารสนเทศแก่ธนาคารขนาดกลาง	ปี 2558	เป็นผู้ตรวจสอบในการสอบทาน Security Baseline
ผู้ให้บริการด้านเทคโนโลยีสารสนเทศแก่ธนาคารขนาดกลาง	ปี 2556	เป็นผู้ตรวจสอบในการสอบทาน IS Security Policy Security Baseline

# ประสบการณ์และผลงานอ้างอิงที่สำคัญ

## ผลงานอ้างอิงงานตรวจสอบด้านเทคโนโลยีสารสนเทศ และการให้คำปรึกษา ในการตรวจสอบและความปลอดภัยด้านเทคโนโลยีสารสนเทศ

ธนาคารขนาดกลาง	ปี 2555	เป็นผู้ตรวจสอบในการตรวจสอบระบบเทคโนโลยีสารสนเทศร่วมกับฝ่ายตรวจสอบภายในของธนาคาร (IT Audit Co-sourcing)
บริษัท ทางยกระดับดอนเมือง จำกัด (มหาชน)	ปี 2555	เป็นผู้ตรวจสอบในการตรวจสอบสถานะโครงสร้างระบบเทคโนโลยีสารสนเทศ (IT Architecture)
ธนาคารขนาดกลาง	ปี 2552	เป็นที่ปรึกษาเพื่อให้คำแนะนำด้านการตรวจสอบภายในระบบสารสนเทศ
บริษัทไปรษณีย์ไทย จำกัด	ปี 2551	เป็นผู้ตรวจสอบในการสอบทานคุณภาพงานตรวจสอบภายในและการตรวจสอบระบบสารสนเทศ

# ขอบเขตงานและแนวทางการดำเนินงาน

# ขอบเขตงานและแนวทางการดำเนินงาน





# ขอบเขตงานและแนวทางการดำเนินงาน

## 1. การจัดทำประวัติข้อมูลระบบเทคโนโลยีสารสนเทศของบริษัทประกันภัย (Risk Profile) และแผนการตรวจสอบ

### วัตถุประสงค์

เก็บรวบรวมข้อมูลที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ของบริษัทประกันชีวิตและบริษัทประกันวินาศภัย เพื่อนำมาประเมินความเสี่ยงทางด้านเทคโนโลยีสารสนเทศ และกำหนดขอบเขตและแผนการตรวจสอบระบบเทคโนโลยีสารสนเทศตามแนวทางการความเสี่ยง (Risk Based Audit) โดยครอบคลุมทั้งการตรวจสอบการควบคุมทั่วไปด้านเทคโนโลยีสารสนเทศ (IT General Controls) และการตรวจสอบการควบคุมเฉพาะระบบงาน (Application Controls)

### แนวทางการดำเนินงาน

1. จัดทำแบบสอบถามเพื่อใช้ในการเก็บข้อมูลที่เกี่ยวข้องกับระบบคอมพิวเตอร์ และสภาพแวดล้อมทางด้านเทคโนโลยีสารสนเทศ โดยครอบคลุมกระบวนการธุรกิจที่สำคัญ
2. จัดประชุมกับบริษัทประกันชีวิต และบริษัทประกันวินาศภัย เพื่อทำความเข้าใจวิธีการออกแบบสอบถาม
3. ประเมินความเสี่ยงทางด้านเทคโนโลยีสารสนเทศโดยอ้างอิงจาก Risk Map และข้อมูลจากแบบสอบถาม
4. จัดทำเอกสารประวัติข้อมูลระบบเทคโนโลยีสารสนเทศของบริษัทประกันภัย (Risk Profile)
5. จัดทำแผนการตรวจสอบประกอบด้วยแผนการตรวจสอบระยะยาว 3 ปี และแผนการตรวจสอบประจำปี ซึ่งให้ครอบคลุมความเสี่ยงที่ได้จากการประเมินความเสี่ยง โดยกำหนด กิจกรรมหรือกระบวนการตรวจสอบ วัตถุประสงค์ ระดับความเสี่ยง ระยะเวลาในการตรวจสอบแต่ละกิจกรรม (Mandays) และบุคลากรที่เหมาะสมและมีประสิทธิภาพ ให้เป็นไปตามมาตรฐานวิชาชีพสากล

# ขอบเขตงานและแนวทางการดำเนินงาน

## 2. การจัดทำคู่มือการตรวจสอบ (Audit Manual) และแนวทางการตรวจสอบ (Audit Program)

### วัตถุประสงค์

เพื่อจัดทำคู่มือการตรวจสอบ (Audit Manual) และแนวทางการตรวจสอบ (Audit Program) ที่สอดคล้องกับมาตรฐานสากลเพื่อใช้เป็นแนวทางในการปฏิบัติงานตรวจสอบ

### แนวทางการดำเนินงาน

1. จัดทำคู่มือการตรวจสอบเทคโนโลยีสารสนเทศและแนวทางการตรวจสอบด้านการตรวจสอบการควบคุมทั่วไปด้านเทคโนโลยีสารสนเทศ (IT General Controls) และการตรวจสอบการควบคุมเฉพาะระบบงาน (IT Application Controls)\* ของระบบงานด้านเทคโนโลยีสารสนเทศ
2. จัดประชุมเพื่อรับความเห็นจากภาคเอกชน สำหรับร่างกรอบการตรวจสอบเทคโนโลยีสารสนเทศ
3. แก้ไขคู่มือการตรวจสอบเทคโนโลยีสารสนเทศและแนวทางการตรวจสอบด้านการตรวจสอบการควบคุมทั่วไปด้านเทคโนโลยีสารสนเทศ (IT General Controls) และการตรวจสอบการควบคุมเฉพาะระบบงาน (IT Application Controls) ของระบบงานด้านเทคโนโลยีสารสนเทศ ตามความเห็นจากภาคเอกชน (บริษัทประกันภัย) (ถ้ามี)

# ขอบเขตงานและแนวทางการดำเนินงาน

## 3. การจัดฝึกอบรม

### วัตถุประสงค์

เพื่อเตรียมความพร้อมให้กับเจ้าหน้าที่ของสำนักงาน คปภ. ในหัวข้อที่จำเป็นต่อการตรวจสอบ (Class room training)

### แนวทางการดำเนินงาน

1. จัดเตรียมเอกสารการฝึกอบรมเกี่ยวกับการตรวจระบบเทคโนโลยีสารสนเทศ
2. จัดฝึกอบรมความรู้เกี่ยวกับการตรวจระบบเทคโนโลยีสารสนเทศ โดยครอบคลุม
  - ความรู้เกี่ยวกับการตรวจสอบระบบเทคโนโลยีสารสนเทศพื้นฐาน จำนวน 1 วัน ให้กับเจ้าหน้าที่ของสำนักงาน คปภ. ไม่เกิน 35 คน โดยมีเนื้อหาการฝึกอบรมเกี่ยวกับความเสี่ยง (IT Risks) และการกำกับดูแลทางด้านเทคโนโลยีสารสนเทศ (IT Governance)
  - ความรู้เกี่ยวกับการตรวจสอบระบบเทคโนโลยีสารสนเทศขั้นสูง จำนวน 5 วัน ให้กับเจ้าหน้าที่ของสำนักงาน คปภ. จำนวน 20 คน โดยมีเนื้อหาการฝึกอบรมดังนี้
    - การควบคุมและการตรวจสอบการควบคุมทั่วไปด้านเทคโนโลยีสารสนเทศ (IT General Controls) และการควบคุมเฉพาะระบบงาน (Application Controls)
    - การวิเคราะห์ข้อมูล (Data Analytics) และการใช้เทคโนโลยีช่วยในการตรวจสอบ (Computer Assisted Audit Techniques – CAATs)

# ขอบเขตงานและแนวทางการดำเนินงาน

## 4. การร่วมปฏิบัติงานตรวจสอบ

### วัตถุประสงค์

เพื่อพัฒนาองค์ความรู้และทักษะของบุคลากรด้านตรวจสอบให้สามารถปฏิบัติงานด้าน IT audit ได้อย่างมีประสิทธิภาพ โดยจัดให้มีการฝึกปฏิบัติงานจริงร่วมกับเจ้าหน้าที่ของสำนักงาน คปภ. ในการตรวจสอบระบบเทคโนโลยีสารสนเทศ (การควบคุมและการตรวจสอบการควบคุมทั่วไปด้านเทคโนโลยีสารสนเทศ (IT General Controls) และการควบคุมเฉพาะระบบงาน (Application Controls))

### แนวทางการดำเนินงาน

1. จัดทำเอกสารที่ร้องขอและตารางการนัดสัมภาษณ์
2. เข้าร่วมประชุมเปิดการตรวจกับบริษัทผู้รับตรวจ เพื่อชี้แจงขอบเขตการตรวจสอบ ระยะเวลา และวิธีการตรวจสอบต่อหน่วยงานรับตรวจที่เกี่ยวข้อง
3. ดำเนินการตรวจสอบเทคโนโลยีสารสนเทศด้านการตรวจสอบการควบคุมทั่วไปด้านเทคโนโลยีสารสนเทศ (IT General Controls) และการตรวจสอบการควบคุมเฉพาะระบบงาน (IT Application Controls)\* ของระบบงานด้านเทคโนโลยีสารสนเทศ
4. ประชุมสรุปผลการตรวจสอบกับหน่วยงานรับตรวจที่เกี่ยวข้องกับบริษัทผู้รับตรวจ
5. จัดทำรายงานผลการตรวจสอบที่แสดงข้อตรวจพบ ผลกระทบและข้อเสนอแนะในการปรับปรุงแก้ไขที่ชัดเจน
6. จัดทำรายงานการตรวจสอบระบบเทคโนโลยีสารสนเทศฉบับสมบูรณ์ พร้อมคำชี้แจงของผู้บริหารของบริษัทผู้รับตรวจ
7. ประชุมปิดการตรวจกับผู้บริหารของบริษัทผู้รับตรวจ

# ขอบเขตงานและแนวทางการดำเนินงาน

## 5. การปรับปรุงคู่มือการตรวจสอบ การประเมินความรู้ ความสามารถ และศักยภาพของเจ้าหน้าที่ตรวจสอบ

### วัตถุประสงค์

เพื่อปรับปรุงคู่มือการตรวจสอบเพื่อให้ผู้ตรวจสอบด้านเทคโนโลยีสารสนเทศของสำนักงาน คปภ. สามารถดำเนินการตรวจสอบได้อย่างมีประสิทธิภาพในอนาคต

เพื่อวางแผนพัฒนาศักยภาพของผู้ตรวจสอบด้านเทคโนโลยีสารสนเทศของสำนักงาน คปภ.

### แนวทางการดำเนินงาน

1. นำปัญหาที่พบระหว่างการปฏิบัติงานตรวจสอบ (ถ้ามี) มาทำการปรับปรุงคู่มือการตรวจสอบ (Audit Manual) และแนวทางการตรวจสอบ (Audit Program)
2. ประเมินความรู้ ความสามารถ และศักยภาพของ ผู้ตรวจสอบด้านเทคโนโลยีสารสนเทศของสำนักงาน คปภ. ที่ร่วมปฏิบัติงานตรวจสอบ และจัดทำเอกสารรายงานผลการประเมินความรู้ ความสามารถ และศักยภาพ
3. จัดทำรายงานคำแนะนำ และแผนงานสำหรับปรับปรุงกระบวนการตรวจสอบทางด้านเทคโนโลยีสารสนเทศ ในระยะสั้น 1 ปี และระยะยาว 5 ปี โดยอ้างอิงจากผลการประเมินความรู้ ความสามารถ และศักยภาพของ ผู้ตรวจสอบด้านเทคโนโลยีสารสนเทศของสำนักงาน คปภ.

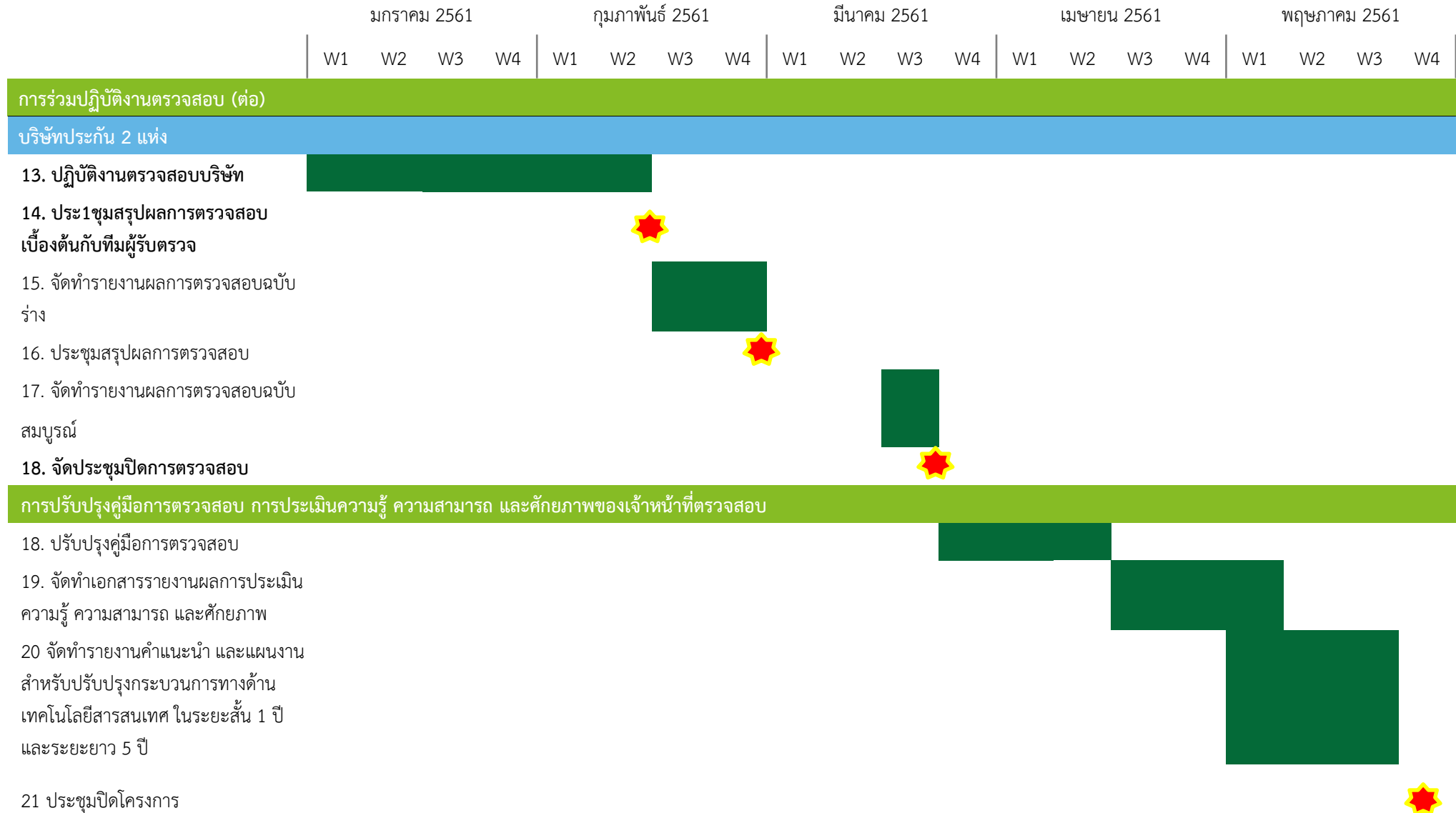
# แผนงานโครงการ

# แผนงานโครงการ



ประชุม

# แผนงานโครงการ (ต่อ)







Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee (“DTTL”), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as “Deloitte Global”) does not provide services to clients. Please see [www.deloitte.com/th/about](http://www.deloitte.com/th/about) for a more detailed description of DTTL and its member firms.

Deloitte provides audit, consulting, financial advisory, risk advisory, tax and related services to public and private clients spanning multiple industries. Deloitte serves four out of five Fortune Global 500® companies through a globally connected network of member firms in more than 150 countries and territories bringing world-class capabilities, insights, and high-quality service to address clients’ most complex business challenges. To learn more about how Deloitte’s approximately 245,000 professionals make an impact that matters, please connect with us on [Facebook](#), [LinkedIn](#), or [Twitter](#).

#### **About Deloitte Southeast Asia**

Deloitte Southeast Asia Ltd – a member firm of Deloitte Touche Tohmatsu Limited comprising Deloitte practices operating in Brunei, Cambodia, Guam, Indonesia, Lao PDR, Malaysia, Myanmar, Philippines, Singapore, Thailand and Vietnam – was established to deliver measurable value to the particular demands of increasingly intra-regional and fast growing companies and enterprises.

Comprising 290 partners and over 7,400 professionals in 25 office locations, the subsidiaries and affiliates of Deloitte Southeast Asia Ltd combine their technical expertise and deep industry knowledge to deliver consistent high quality services to companies in the region.

All services are provided through the individual country practices, their subsidiaries and affiliates which are separate and independent legal entities.

#### **About Deloitte Thailand**

In Thailand, services are provided by Deloitte Touche Tohmatsu Jaiyos Co., Ltd. and its subsidiaries and affiliates.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the “Deloitte network”) is, by means of this communication, rendering professional advice or services. No entity in the Deloitte network shall be responsible for any loss whatsoever sustained by any person who relies on this communication.