โครงการศึกษาแลกเปลี่ยนเรียนรู้และสร้างเครือข่ายการเป็นองค์กรคุณธรรมต้นแบบกับหน่วยงานภายนอก ธนาคารแห่งประเทศไทย

คำนำ

สำนักบริหารงานกลางและสำนักเครือข่ายได้จัดโครงการ "องค์กรเครือข่าย STRONG และองค์กรที่ได้รับการประเมินคุณธรรมและความโปร่งใส (ITA) กับธนาคารแห่งประเทศไทย" คณะทำงานสำนักบริหารงานกลางได้มีการรวบรวมองค์ความรู้ที่มีการแลกเปลี่ยนกับองค์กรเครือข่าย โดยมีวัตถุประสงค์เพื่อนำความรู้ ข้อมูล และเทคนิคการปฏิบัติงานมาปรับใช้กับหน่วยงานของตนเอง เป็นการสร้างเครือข่ายและสร้างการเป็นพันธมิตรและสร้างความสัมพันธ์ที่ดีต่อกัน

คณะทำงาน สำนักบริหารงานกลางหวังเป็นอย่างยิ่งว่าข้อมูลที่ได้รวบรวมไว้จะเป็นประโยชน์ต่อผู้ที่สนใจพอสมควร

คณะทำงาน
สำนักบริหารงานกลาง
๗ กรกฎาคม ๒๕๖๖

สารบัญ

โครงการศึกษาแลกเปลี่ยนเรียนรู้และสร้างเครือข่ายการเป็นองค์กรคุณธรรมต้นแบบ

กับหน่วยงานภายนอก ธนาคารแห่งประเทศไทย

เมื่อวันที่ ๒๔ พฤษภาคม ๒๕๖๖ สำนักบริหารงานกลาง สำนักวิชาการ สำนักนโยบายและแผน และสำนักพัฒนาทรัพยากรบุคคล ได้ร่วมกันจัดกิจกรรมเพื่อศึกษาแลกเปลี่ยนเรียนรู้และสร้างเครือข่ายการเป็นองค์กรคุณธรรมต้นแบบกับธนาคารแห่งประเทศไทย ทั้งนี้ธนาคารแห่งประเทศไทยได้ให้ความรู้เกี่ยวกับการบริหารความเสี่ยงของธนาคารแห่งประเทศไทย สรุปสาระสำคัญ ดังนี้

นิยามความเสี่ยง คือเหตุการณ์การกระทำใด ๆ ที่อาจเกิดขึ้นภายใต้สถานการณ์ที่ไม่แน่นอน และจะส่งผลกระทบสร้างความเสียหายความล้มเหลวหรือลดโอกาสที่จะบรรลุความสำเร็จต่อการบรรลุเป้าหมายและวัตถุประสงค์ทั้งในระดับองค์การระดับหน่วยงานและระดับบุคคลได้

การบริหารความเสี่ยง เป็นกระบวนการที่ออกแบบให้สามารถบ่งชี้เหตุการณ์ที่อาจเกิดขึ้นและมีผลกระทบต่อองค์กร เพื่อเตรียมพร้อมวางแผนและจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ให้องค์กรสามารถดำเนินงาน และบรรลุวัตถุประสงค์ที่กำหนดไว้ ทั้งนี้การบริหารความเสี่ยงไม่มีรูปแบบตายตัวขึ้นอยู่กับสถานการณ์ การวิเคราะห์ข้อมูลและการตัดสินใจที่ทันต่อเหตุการณ์

การวางแผนความเสี่ยง ธนาคารแห่งประเทศไทยได้มีวางแผนความเสี่ยง ดังนี้

ด้าน IT and Cyber Risk Management เป็นการบริหารเพื่อพัฒนาให้การดำเนินงานด้านเทคโนโลยีสารสนเทศและการสื่อสาร ที่ต้องมีการพัฒนาและใช้งานได้อย่างต่อเนื่อง เพื่อสนับสนุนภารกิจ

ของหน่วยงานภายในองค์กร ช่วยป้องกันหรือลดเหตุการณ์ที่จะทำให้เกิดความเสียหายต่อระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กร ซึ่งการบริหารความเสี่ยงเป็นกระบวนการที่ออกแบบให้สามารถบ่งชี้เหตุการณ์ที่อาจเกิดขึ้นและมีผลกระทบต่อองค์กร เพื่อเตรียมความพร้อมและจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ให้องค์กรสามารถดำเนินงานและบรรลุวัตถุประสงค์ที่กำหนดไว้ ทั้งนี้ธนาคารแห่งประเทศไทยได้มีการป้องกันและพัฒนาระบบรักษาความปลอดภัยให้มีความทันสมัยและป้องกันหลายชั้นเพื่อป้องกัน Hacker โจรกรรมข้อมูลต่าง ๆ

การบริหารความเสี่ยงด้าน IT ของธนาคารแห่งประเทศไทย

๑. มีการกำกับดูแลโดยโครงสร้าง ๓ Line of Defense ที่เป็นอิสระและถ่วงดุลอำนาจอย่างเหมาะสม

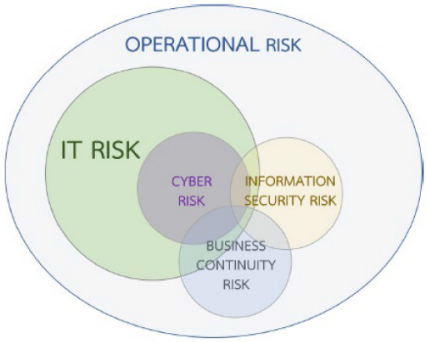
๒. มีกลไกสนับสนุนการกำกับดูและและบริหารความเสี่ยงแบบบูรณาการ โดยผลักดันและติดตามผ่านคณะอนุกรรมการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

๓. มีกรอบการบริหารความเสี่ยงและมาตรฐานด้านความมั่นคงปลอดภัย IT ของธนาคารแห่งประเทศไทย ตามมาตรฐานสากลและแนวปฏิบัติที่ดี ครอบคลุมทุกมิติความเสี่ยงที่สำคัญเพื่อเป็นกรอบในการดำเนินงานด้าน IT ของทุกส่วนงาน โดยระบบและบริการด้าน IT ที่สำคัญหรือมีความเสี่ยงสูงอยู่ภายใต้การดูและของ ฝทส.

๔. มีโปรแกรมบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk Management Program) เพื่อรองรับการบริหารความเสี่ยงเชิงรุก สำหรับประเด็นความเสี่ยงที่สำคัญ

๕. มีการติดตามการปฏิบัติตามกฎหมายและหลักเกณฑ์ด้าน IT (IT Compliance โดย Digitize ข้อมูลความเสี่ยงสำคัญ เพื่อสนับสนุนการติดตามได้อย่างต่อเนื่องทันต่อเหตุการณ์ และมีประสิทธิภาพ

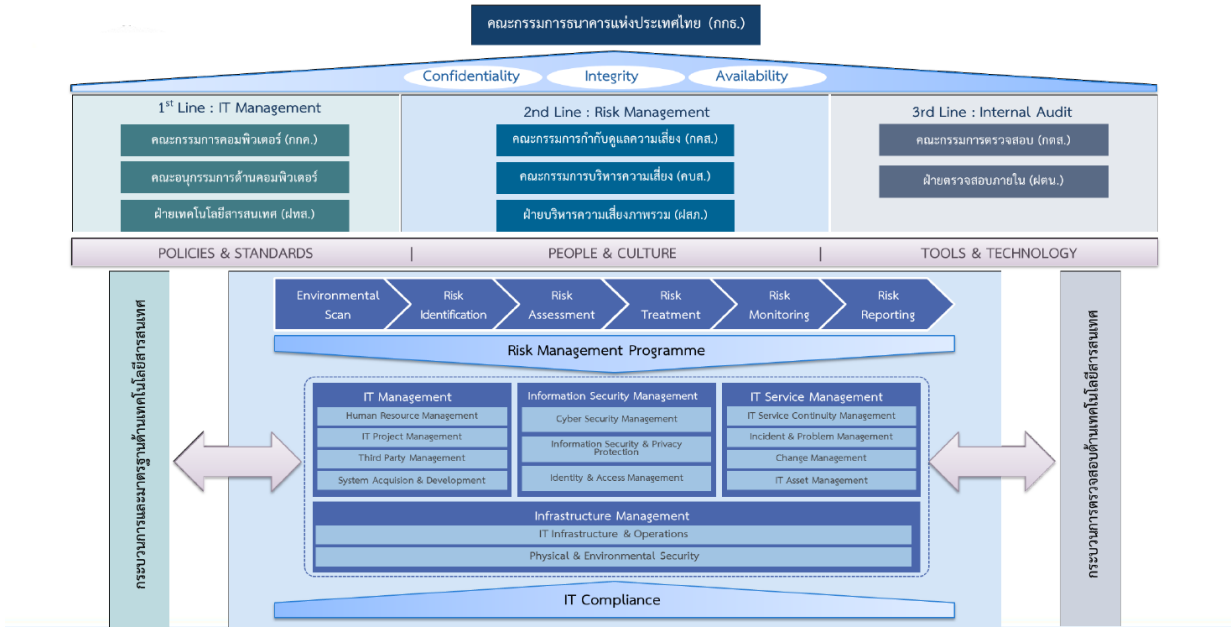
หลักการบริหารความเสี่ยงด้าน IT ของ ธปท.

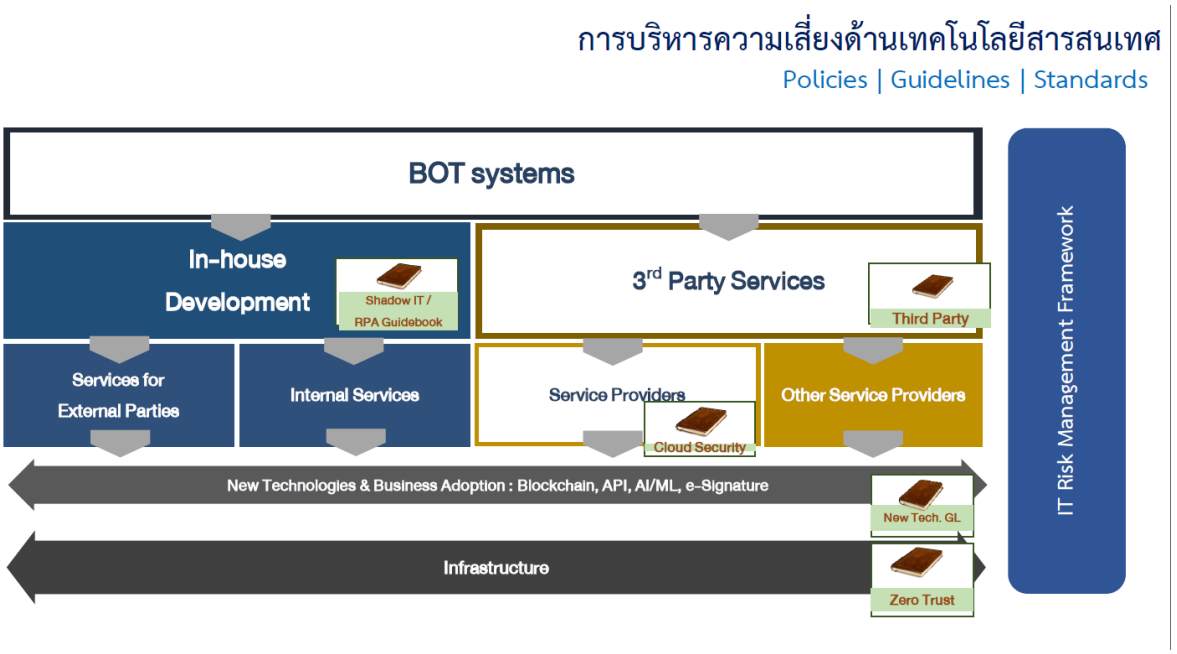


1. มีการกำกับดูแลโดยโครงสร้าง 3 Lines of Defense ที่เป็นอิสระและถ่วงดุลอำนาจอย่างเหมาะสม
2. มีกลไกสนับสนุนการกำกับดูแลและบริหารความเสี่ยงแบบบูรณาการ โดยผลักดันและติดตามผ่านคณะอนุกรรมการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ
3. มีกรอบการบริหารความเสี่ยงและมาตรฐานด้านความมั่นคงปลอดภัย IT ของ ธปท. ตามมาตรฐานสากลและแนวปฏิบัติที่ดี[1/] ครอบคลุมทุกมิติความเสี่ยงที่สำคัญ เพื่อเป็นกรอบในการดำเนินงานด้าน IT ของทุกส่วนงาน โดยระบบและบริการด้าน IT ที่สำคัญหรือมีความเสี่ยงสูงอยู่ภายใต้การดูแลของ ฝทส.
4. มีโปรแกรมการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk Management Programme) เพื่อรองรับการบริหารความเสี่ยงเชิงรุก สำหรับประเด็นความเสี่ยงที่สำคัญ
5. มีการติดตามการปฏิบัติตามกฎหมายและหลักเกณฑ์ด้าน IT (IT Compliance) โดย Digitize ข้อมูลความเสี่ยงสำคัญ เพื่อสนับสนุนการติดตามได้อย่างต่อเนื่อง ทันการณ์ และมีประสิทธิภาพ

1/ ได้แก่ กรอบการดำเนินงาน COBIT5, มาตรฐาน ISO/IEC 27001 เรื่อง Information Security Management, มาตรฐาน National Institute of Technology and Standards (NIST) SP 800-53 เรื่อง Recommended Security Controls for Federal information Systems and Organizations และประกาศ ธปท. ที่ สนส. 21/2562 เรื่อง หลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk) ของสถาบันการเงิน

กรอบการบริหารความเสี่ยงด้าน IT ของ ธปท.



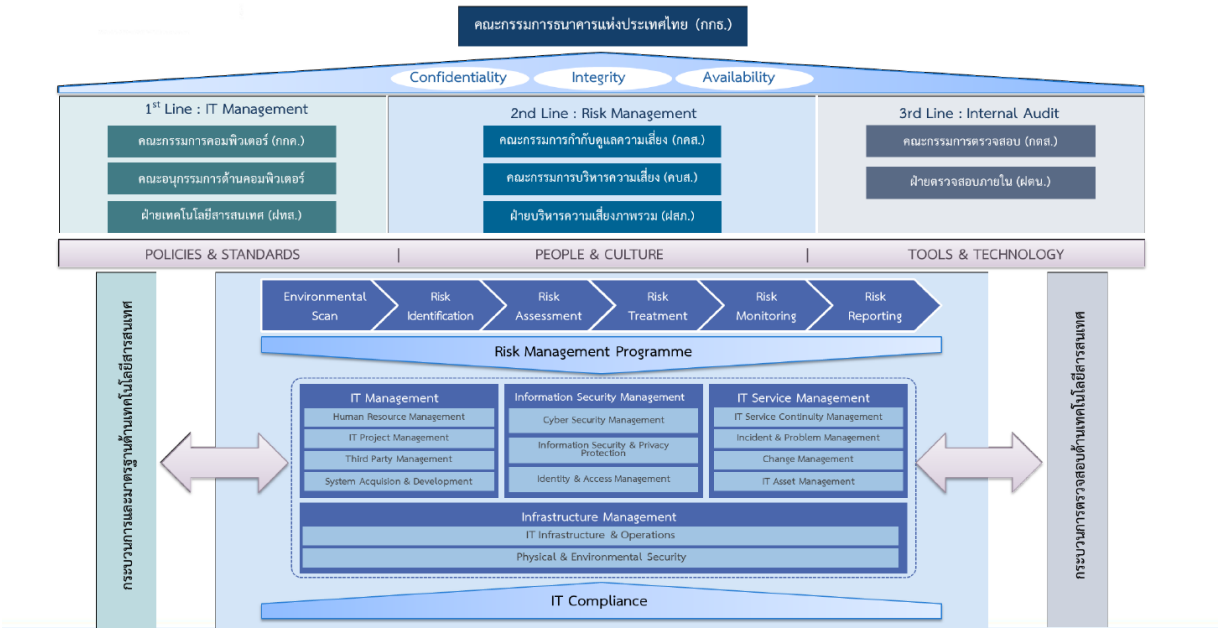


กรอบการบริหารความเสี่ยงด้านเทคโนโลยี IT

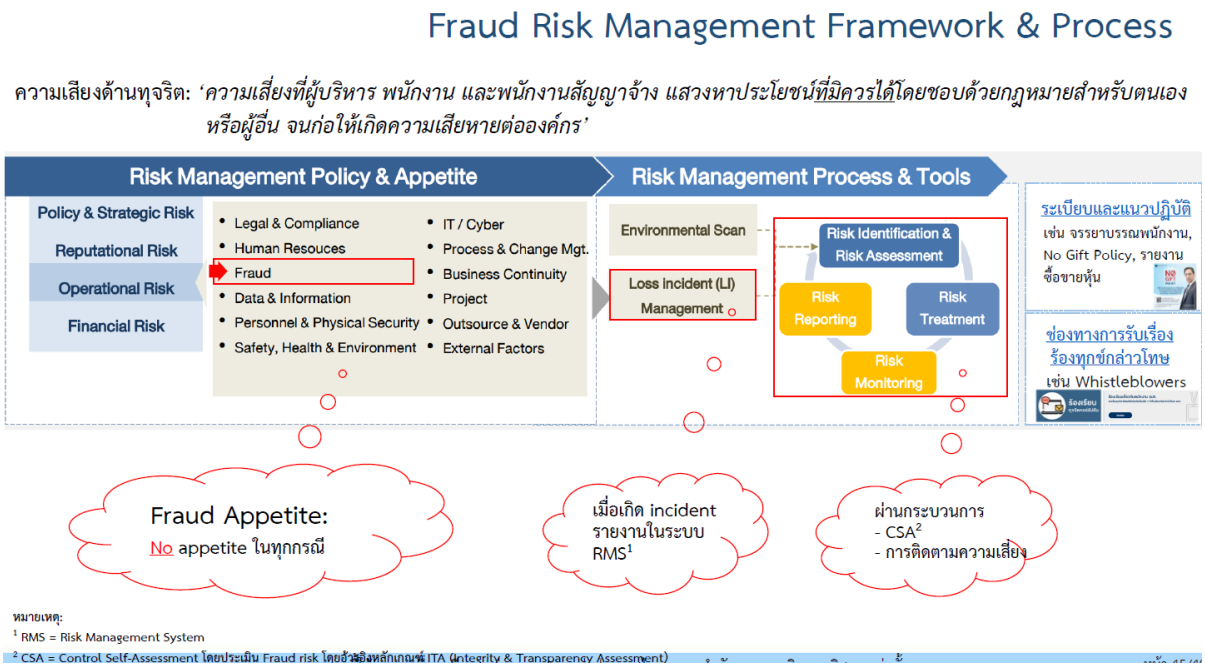
การพัฒนานโยบาย/แนวปฏิบัติการบริหารความเสี่ยง IT และมาตรฐานความมั่งคงปลอดภัยทางเทคโนโลยี

โดยธนาคารมีกรอบการบริหารความเสี่ยง นโยบาย/แนวปฏิบัติและมาตรฐานด้านความมั่นคงปลอดภัยIT ตามมาตรฐานสากลและแนวปฏิบัติที่ดี ครอบคลุมทุกมิติความเสี่ยงที่สำคัญเพื่อเป็นกรอบในการดำเนินงานของทุกส่วนงาน และกรณีพบความไม่สอดคล้อง เสนอคณะกรรมการบริหารความเสี่ยงด้าน IT พิจารณามาตรการควบคุมทดแทน

กรอบการบริหารความเสี่ยงด้าน IT ของ ธปท.



ด้าน Fraud Risk Management เป็นการบริหารความเสี่ยงด้านการทุจริตมีการป้องกันการทุจริตอย่างเป็นรูปธรรม เช่น ความเสี่ยงด้านการทุจริตของบุคลากรแสวงหาประโยชน์ที่มิควรได้โดยชอบด้วยกฎหมาย จนก่อให้เกิดความเสียหายแก่องค์กร ทั้งนี้ธนาคารจะมีช่องทางให้มีการรับเรื่องราวร้องทุกข์ และได้มีการประกาศแนวปฏิบัติให้บุคลากรของธนาคารมีจรรยาบรรณในการปฏิบัติงานจะไม่ยอมรับความเสี่ยงที่อาจก่อให้เกิดการทุจริต หรือก่อให้เกิดการขัดผลประโยชน์ส่วนตนกับผลประโยชน์ส่วนรวมในทุกกรณี (No Gift Policy)



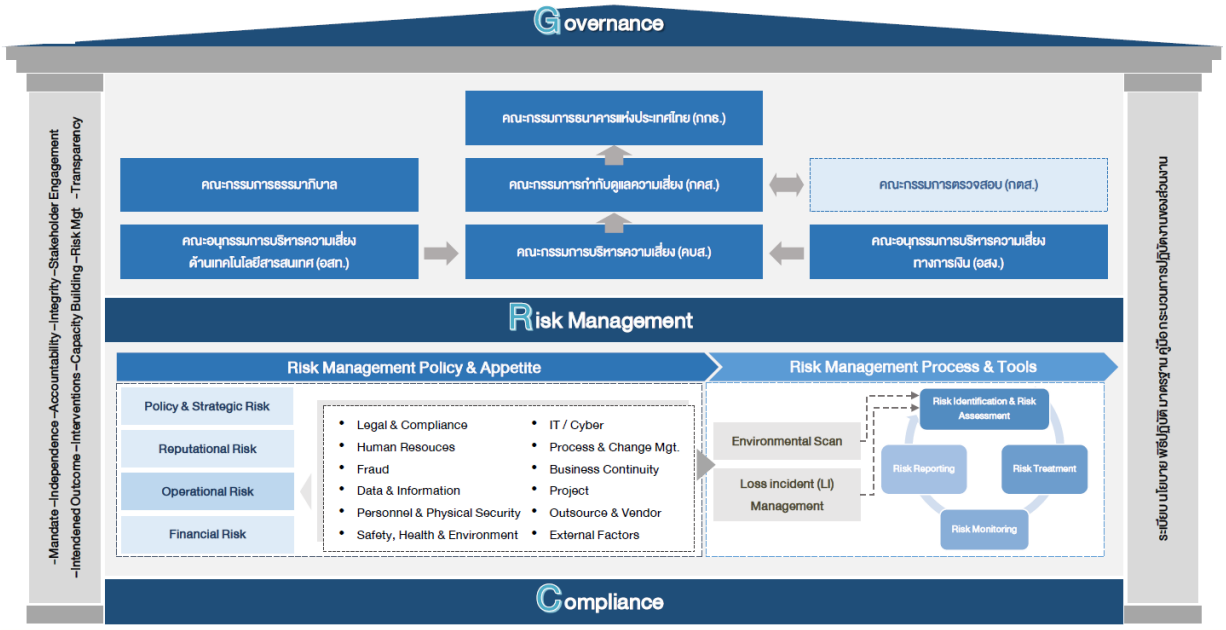
นโยบายการบริหารความเสี่ยงของธนาคารแห่งประเทศไทย

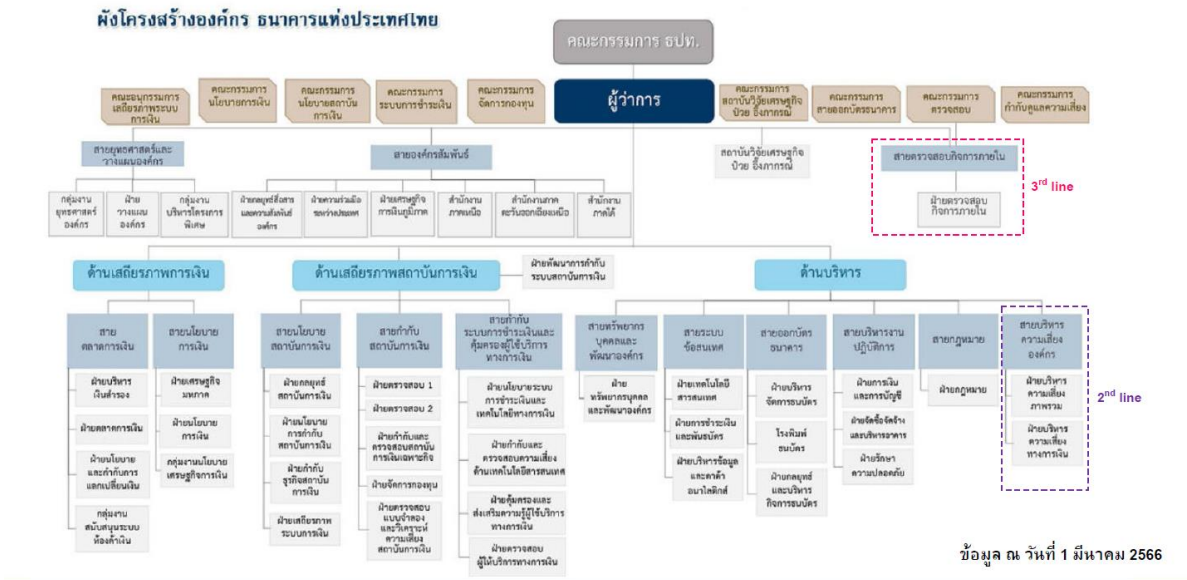
ธนาคารแห่งประเทศไทยมุ่งเน้นการบริหารความเสี่ยงในเชิงรุก และเป็นส่วนหนึ่งของการดำเนินงานเพื่อให้มั่นใจว่าสามารถบรรลุพันธกิจภายใต้ความเสี่ยงที่ยอมรับได้ โดยใช้หลักการบริหารความเสี่ยง ดังนี้

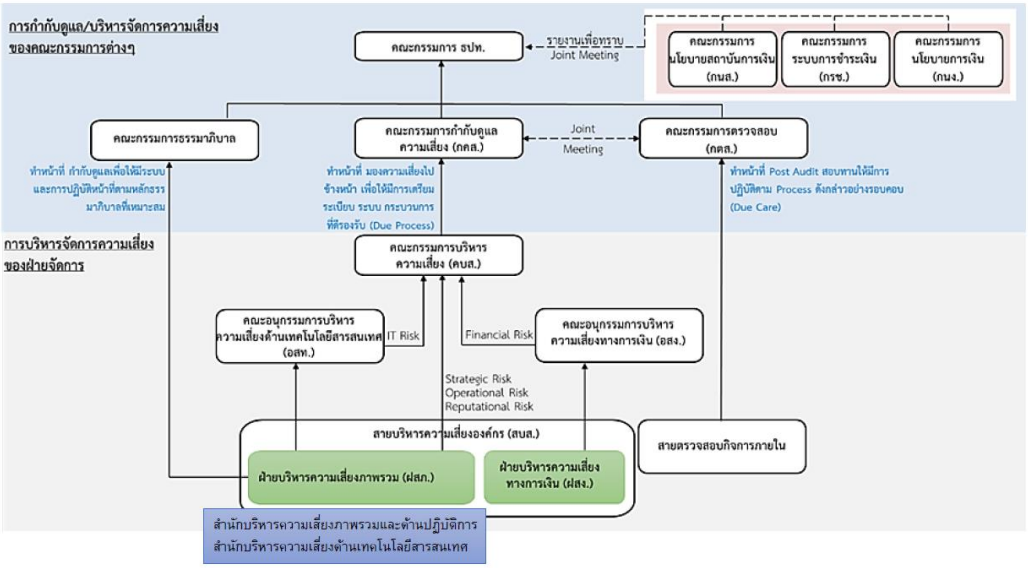
๑. การบริหารความเสี่ยงเป็นหน้าที่และความรับผิดชอบของพนักงานทุกคน โดยให้ถือว่าเป็นส่วนหนึ่งของการปฏิบัติงานปกติ

๒. หัวหน้าส่วนงานเป็นผู้รับผิดชอบหลักในการบริหารความเสี่ยงของส่วนงาน มีหน้าที่ส่งเสริมให้หัวหน้างานทุกระดับเข้าใจความเสี่ยงของส่วนงาน กำหนดแนวทางจัดการ สื่อสารให้พนักงานเข้าใจ และติดตามให้มีการปฏิบัติอย่างเคร่งครัด

๓. การวางแผนการตัดสินใจ และการดำเนินงานต้องมีการบริหารความเสี่ยงรอบด้านเปรียบเทียบกับประโยชน์ที่จะได้รับและระดับความเสี่ยงที่ยอมรับได้


Governance
-Mandate -Independence -Accountability -Integrity -Stakeholder Engagement
-Intendened Outcome -Interventions -Capacity Building -Risk Mgt -Transparency
คณะกรรมการธนาคารแห่งประเทศไทย (กกธ.)
คณะกรรมการธรรมาภิบาล
คณะกรรมการกำกับดูแลความเสี่ยง (กคส.)
คณะกรรมการตรวจสอบ (กตส.)
คณะอนุกรรมการบริหารความเสี่ยง ด้านเทคโนโลยีสารสนเทศ (อสท.)
คณะกรรมการบริหารความเสี่ยง (คบส.)
คณะอนุกรรมการบริหารความเสี่ยง ทางการเงิน (อสง.)
ระเบียบนโยบาย พิจิปฏิบัติเคร่งครัด คู่มือกระบวนการปฏิบัติงานอย่างต่อเนื่อง
Risk Management
Risk Management Policy & Appetite
Risk Management Process & Tools
Policy & Strategic Risk
Reputational Risk
Operational Risk
Financial Risk
Legal & Compliance
Human Resouces
Fraud
Data & Information
Personnel & Physical Security
Safety, Health & Environment
IT / Cyber
Process & Change Mgt.
Business Continuity
Project
Outsource & Vendor
External Factors
Environmental Scan
Loss incident (LI) Management
Risk Identification & Risk Assessment
Risk Reporting
Risk Treatment
Risk Monitoring
Compliance


ผังโครงสร้างองค์กร ธนาคารแห่งประเทศไทย
คณะกรรมการ ธปท.
ผู้ว่าการ
สายตรวจสอบกิจการภายใน
3rd line
ฝ่ายตรวจสอบกิจการภายใน
ด้านเสถียรภาพการเงิน
ด้านเสถียรภาพสถาบันการเงิน
ด้านบริหาร
2nd line
ข้อมูล ณ วันที่ 1 มีนาคม 2566



การประเมินผล Fraud risk โดยอ้างอิงหลักเกณฑ์ ITA (Integrity & Transparency Assessment)

R1. ความเสี่ยงการทุจริตในความโปร่งในของการใช้อำนาจและตำแหน่งหน้าที่

๑.๑ การให้ความช่วยเหลือหรือผ่อนผันให้แก่นิติบุคคลที่อยู่ภายใต้การกำกับดูแล เพื่อแสงหาผลประโยชน์ให้แก่ตนเอง

๑.๒ การนำข้อมูลลับหรือข้อมูลสำคัญของ ธปท. /นิติบุคคลที่อยู่ภายใต้การกำกับ ซึ่งได้รับมาตามอำนาจหน้าที่ไปแสวงหาประโยชน์แก่ตนเองหรือพวกพ้อง

๑.๓ การทำงานให้กับองค์กรอื่นที่อาจมีส่วนได้ส่วนเสียกับตำแหน่งหน้าที่เดิม ภายหลังการลาออก การเกษียณอายุ หรือการหมดวาระ

๑.๔ การทำงานให้กับองค์กรอื่นที่อาจมีส่วนได้ส่วนเสียกับการดำรงตำแหน่งหน้าที่ปัจจุบัน

๑.๕ การรับพนักงานใหม่ แต่งตั้ง โยกย้าย มีการเอื้อประโยชน์ให้พวกพ้อง หรือเครือญาติ

R2. ความเสี่ยงการทุจริตในความโปร่งใสของการใช้จ่ายงบประมาณ

๒.๑ การบริหารกิจการทั่วไป

(๑) การเบิกค่าใช้จ่าย / สวัสดิการตามสิทธิเป็นเท็จ เช่น ค่าใช้จ่ายเดินทาง ค่าอบรม ค่ารักษาพยาบาลฯ

(๒) การทำธุรกรรมการลงทุน หรือธุรกรรมในตลาดเงินโดยอาจเอื้อประโยชน์ให้คู่ค้า หรือไม่ได้พิจารณาอย่างรอบคอบเพียงพอ

(๓) ธนบัตรสูญหายระหว่างกระบวนการทำงาน

๒.๒ การจัดซื้อจัดจ้าง

(๑) การกำหนด TOR ในการจัดซื้อจัดจ้าง อาจมีการล็อคสเปคเข้ากับสินค้า ผู้รับจ้างรายใดรายหนึ่ง

(๒) การตรวจรับพัสดุ ไม่เป็นไปตามข้อกำหนดในสัญญา หรือ TOR ที่กำหนด

(๓) มีโอกาสที่เจ้าหน้าที่จะจัดซื้อจัดจ้าง จากผู้ค้าที่รู้จักคุ้นเคยซึ่งอาจเป็นการเอื้อประโยชน์ให้แก่พวกพ้องได้

R3. ความเสียงการทุจริตที่เกี่ยวข้องกับการพิจารณาอนุมัติ/อนุญาต ตาม พ.ร.บ. การอำนวยความสะดวก

๓.๑ การพิจารณาคำขอลักษณะใกล้เคียงกัน แต่มีโอกาสที่จะพิจารณาโดยใช้ดุลพินิจที่แตกต่างกันเพื่อแสวงหาผลประโยชน์จากผู้ยื่นคำขอ

๓.๒ การเรียกรับผลประโยชน์จากผู้ยื่นคำขอ เพื่อให้การดำเนินการรวดเร็วขึ้น

ผลการประเมิน Fraud risk โดยธนาคารแห่งประเทศไทยมีการควบคุมภายในตามกรอบมาตรฐานสากล COSO 2013 (Committee of Sponsoring Organization) ประกอบด้วย

๑. สภาพแวดล้อมการควบคุม (Control Environment)

๒. การประเมินความเสี่ยง (Risk Assessment)

๓. กิจกรรมควบคุม (Control Activities)

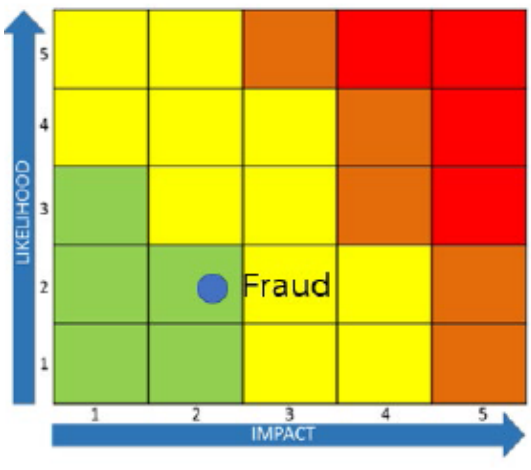
๔. สารสนเทศและการสื่อสาร (Information and Communication)

๕. กิจกรรมการติดตาม (Monitoring Activities)

ทั้งนี้ การประเมินความเสี่ยงและความควบคุมภายใน ธปท. ได้กำหนดระเบียบ เรื่องการประเมินความเสี่ยงและการควบคุมภายใน (ระเบียบ ธปท. ที่ ท ๓๑/๒๕๖๒) ซึ่งเป็นไปตามพระราชบัญญัติวินัยการเงินการคลังของรัฐ พ.ศ. ๒๕๖๑ และหลักเกณฑ์กระทรวงการคลังว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการควบคุมภายในสำหรับหน่วยงานของรัฐ พ.ศ. ๒๕๖๑ โดยกำหนดให้ทุกฝ่ายงานใน ธปท. วิเคราะห์ ประเมินความเสี่ยงและการควบคุมภายใน (Control self-assessment : CSA) เป็นประจำทุกปีซึ่งรวมถึงการประเมินความเสียงด่านการทุจริต โดยพิจารณาโอกาสที่จะเกิดความเสี่ยงจากบุคลากร กระบวนการทำงาน ระบบงานหรือการเปลี่ยนแปลงสภาพแวดล้อม เป็นต้น

ผลการประเมิน Fraud risk ที่เผยแพร่บน Website

ผลการประเมิน Fraud risk ที่เผยแพร่บน BOT Website



ประโยชน์ที่ได้รับ

๑) ทำให้สามารถนำความรู้ ข้อมูล ประสบการณ์และเทคนิคใหม่ ๆ ที่ได้รับการถ่ายทอดนำมาปรับใช้กับหน่วยงานของตนเอง

๒) เป็นการเชื่อมโยงเครือข่าย เปิดโอกาสในการสร้างพันธมิตร และสร้างความสัมพันธ์ที่ดีต่อกัน

๓) ทำให้เกิดความคิดริเริ่มสร้างสรรค์