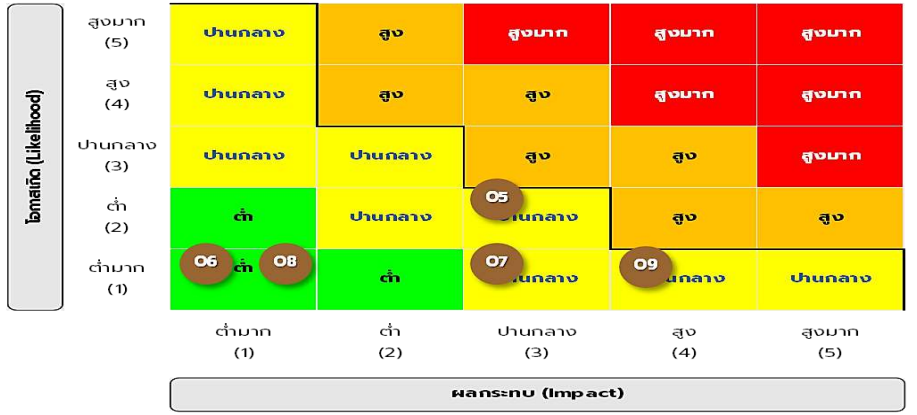
การดำเนินการเพื่อจัดการความเสี่ยงการทุจริต ประจำปี 2566

SAM : บริษัท บริหารสินทรัพย์สุขุมวิท จำกัด

- ✓ ระดับความเสี่ยงการทุจริตประจำปี 2566 ใน 5 ประเภทความเสี่ยง พบว่า บสส. มีระดับการควบคุมที่เพียงพอ โดยนำมาตรการควบคุมภายในที่มีอยู่มาพิจารณาประกอบร่วมด้วย
- ✓ ประเภทความเสี่ยงการทุจริตเรื่อง การยักยอกทรัพย์สิน, การแสวงหาประโยชน์จากทรัพย์สิน (O5) ยังมีระดับโอกาสที่จะเกิดขึ้น จึงมีแผนบริหารจัดการการควบคุมภายในเพื่อลดโอกาสการเกิดเหตุการณ์เพิ่มเติม
- ✓ จัดทำแผนเพิ่มประสิทธิภาพเพื่อพัฒนาปรับปรุงการบริหารจัดการความเสี่ยงด้านการทุจริตในปี 2566



ประเภทความเสี่ยงการทุจริต	มาตรการควบคุมที่มีอยู่	โอกาสเกิด	ผลกระทบ	ระดับความเสี่ยง	ความเสี่ยงที่เหลืออยู่	แผนจัดการ (Action Plan)
O5. FRAUD : การยักยอกทรัพย์สิน, การแสวงหาประโยชน์จากทรัพย์สิน	• วางกรอบอำนาจกำหนดอำนาจอนุมัติการใช้ทรัพย์สินภายในสำนักงาน • วางขั้นตอนการ Check & Balance ทั้งภายใน และภายนอกฝ่ายงาน • มีการจัดทำทะเบียนคุมทรัพย์สิน และใช้ระบบงานในการบันทึกทรัพย์สินทั้งหมดของสำนักงาน • Second Line ประเมินการควบคุมภายใน และ Third Line ตรวจสอบการทำงาน	2	3	ปานกลาง	- ปรับปรุงขั้นตอนตรวจสอบการยกเลิกงาน Outsource และ การโอนเงินคืนให้กับ บสส.	• หน่วยงานปฏิบัติการหลังอนุมัติ : ปรับปรุงขั้นตอนการตรวจสอบเอกสารใบสั่งงาน และการเคลียร์เงินทดรองจ่าย - เพิ่มข้อความในใบสั่งงาน Outsource เรื่องการกำหนดให้เคลียร์เงินสดภายในวันรุ่งขึ้น และการเคลียร์เงินสดคืน บสส. ให้โอนเข้าบัญชี บสส. เท่านั้น - เพิ่ม Field ข้อมูล "วันครบกำหนดเคลียร์เงินสด" ในทะเบียนคุมเบิก-จ่าย และมีการติดตามเอกสารการเคลียร์ในวันรุ่งขึ้น (ทุกวัน)
O6. FRAUD : การรายงานข้อมูลเท็จ	• กำหนดรูปแบบที่เป็นทางการในการนำเสนอข้อมูล • มีฐานข้อมูลกลางในการนำข้อมูลไปใช้งานร่วมกัน • มี Check & Balance ตรวจสอบความถูกต้องของข้อมูลก่อนนำเสนอ	1	1	ต่ำ	-	• แผนเพิ่มประสิทธิภาพเพื่อพัฒนาปรับปรุงการบริหารจัดการความเสี่ยงด้านการทุจริต - การจัดเก็บข้อมูลตัวชี้วัดความเสี่ยง (KRIs : Key Risk Indicators) เรื่องร้องเรียนการทุจริตภายในสำนักงานจากหน่วยงานที่เกี่ยวข้อง - ปรับปรุงช่องทางการร้องเรียนการทุจริตให้ชัดเจนขึ้น (แยกออกจากเรื่องร้องเรียนการให้บริการ) - ประสานงานกับทาง Audit เพื่อดำเนินงานตามหลักการ Three Lines of Defense - สื่อสารเรื่องการบริหารความเสี่ยงการทุจริตเพื่อสร้างความตระหนักให้กับพนักงานภายในองค์กร
O7. FRAUD : การแสวงหาประโยชน์จากข้อมูล	• มีระเบียบเรื่องการจัดการเอกสาร การจัดชั้นความลับ และการคุ้มครองข้อมูลส่วนบุคคล • มีการกำหนดสิทธิการเข้าถึงฐานข้อมูลต่างๆอย่างถูกต้อง และชัดเจน • ใช้ระบบงานป้องกันการเผยแพร่ข้อมูลออกข้างนอก	1	3	ปานกลาง	-	
O8. FRAUD : ผลประโยชน์ทับซ้อน	• มีระเบียบงานเรื่อง Conflict of Interest ที่พนักงานต้องปฏิบัติตาม • มีระบบตรวจสอบความสัมพันธ์ระหว่างคู่ค้ากับพนักงานในองค์กร • มีช่องทางการรับเรื่องร้องเรียน และการแจ้งเบาะแสภายในสำนักงาน	1	1	ต่ำ	-	
O9. FRAUD : เรียกรับผลประโยชน์ ติดสินบน	• มีการประกาศและเผยแพร่การไม่รับของขวัญใดใดให้บุคคลภายนอกรับทราบ • มีช่องทางการรับเรื่องร้องเรียน และการแจ้งเบาะแสภายในสำนักงาน • Second Line ประเมินการควบคุมภายใน และ Third Line ตรวจสอบการทำงาน	1	4	ปานกลาง	-	

แผนเพิ่มประสิทธิภาพเพื่อพัฒนาปรับปรุงการบริหารจัดการความเสี่ยงด้านการทุจริต ประจำปี 2566

กิจกรรม	หน่วยงานที่เกี่ยวข้อง	ปี 2566											
		Q1			Q2			Q3			Q4		
		ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	ต.ค.	พ.ย.	ธ.ค.
1. การจัดเก็บข้อมูลตัวชี้วัดความเสี่ยง (KRIs : Key Risk Indicators) เรื่องร้องเรียนการทุจริตภายในสำนักงานจากหน่วยงานที่เกี่ยวข้อง													
2. ปรับปรุงช่องทางการร้องเรียนการทุริตให้ชัดเจนขึ้น (แยกออกจากเรื่องร้องเรียนการให้บริการ)													
3. ประสานงานกับทาง Audit เพื่อดำเนินงานตามหลักการ Three Lines of Defense													
4. สื่อสารเรื่องการบริหารความเสี่ยงการทุจริตเพื่อสร้างความตระหนักให้กับพนักงานภายในองค์กร													

เอกสารแนบ : รายละเอียดที่เกี่ยวข้อง

SAM Risk Dashboard

Reputation Lower ← → Opportunity & Return Higher

Compliance Risk	Operational Risk	Information Technology Risk (CIA)	Financial Risk	Strategic Risk (High Risk High Return)

KRIs Monitoring ปี 66

Strategic

Project

- **SG1.** ความคืบหน้าการดำเนินงานโครงการ Acquisition
- **SG2.** ความคืบหน้าการดำเนินงานโครงการ NPL
- **SG3.** ความคืบหน้าการดำเนินงานโครงการ LED
- **SG4.** ความคืบหน้าการดำเนินงานโครงการ NPA

Human

- **SG5.** Tun Over Rate (Overall)

Performance

- **SG6.** NPL
- **SG7.** LED
- **SG8.** NPA
- **SG9.** ROA

Operational

Fraud

- **OP1.** การเฝ้าระวังการทุจริต และประพฤติมิชอบ (การแจ้งเบาะแส & การสอบทาน Conflict of Interest)
- **OP2.** ข่าวเชิงลบทาง Social Media & Offline Media

Data

- **OP3.** การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต
- **OP4.** การรั่วไหลของข้อมูลอย่าง ไม่เหมาะสม (ผ่านระบบ DLP)

Operational

- **OP5.** เรื่องร้องเรียน
- **OP6.** บสส. ถูกฟ้องร้องที่มีผลกระทบต่อชื่อเสียงภาพลักษณ์ขององค์กร หรือถูกเรียกค่าเสียหาย
- **OP7.** LET1 : ความเสียหายจากการทุจริตและ/หรือการฉ้อโกง โดยบุคคลภายใน (Internal Fraud)
- **OP8.** LET2 : ความเสียหายจากการทุจริตและ/หรือการฉ อ โกง โดยบุคคลภายนอก (External Fraud)
- **OP9.** LET3 : ความเสียหายจากแนวปฏิบัติเกี่ยวกับการจ้างงาน และความปลอดภัยของสถานที่ปฏิบัติงาน

Operational

- **OP10.** LET4 : ความเสียหายจากแนวปฏิบัติเกี่ยวกับลูกค้า ผลิตภัณฑ์ และการดำเนินธุรกิจ (Clients, Products and Business Practices)
- **OP11.** LET5 : ความเสียหายต่อทรัพยสิน (Damage to Physical Assets)
- **OP12.** LET6 : ความเสียหายจากการที่ธุรกิจหยุดชะงักและระบบงานขัดของ (System Failures)
- **OP13.** LET7 : ความเสียหายจากการปฏิบัติการ และการจัดการกระบวนการ (Execution, Delivery and Process Management)
- **OP14.** จำนวนครั้งที่เกิดความเสียหายจาก LET7
- **OP15.** ข้อมูลการสวมสิทธิทางคดี (SLA)

Financial

Liquidity

- **FI1.** ฐานะสภาพคล่องสุทธิสะสม (0-3 เดือน) รวมวงเงิน Committed facility
- **FI2.** IBD/E Ratio
- **FI3.**DSCR
- **FI4.**NOCF

Credit

- **FI5.** สัดส่วนของลูกหนี้ที่มีการปรับหนี้พอร์ตรวม
- **FI6.** สัดส่วนของลูกหนี้ที่มีการปรับหนี้Corporate
- **FI7.** สัดส่วนของลูกหนี้ที่มีการปรับหนี้ SME
- **FI8.** สัดส่วนของลูกหนี้ที่มีการปรับหนี้ Housing

Information Technology

Security

- **IT1.** การป้องกันความเสียหายระบบงานสำคัญจากภัยคุกคามทางเทคโนโลยีสารสนเทศ
- **IT2.** การทดสอบการเจาะระบบ (Penetration Test) ปี 65 ของระบบงานสำคัญ
- **IT3.** การทดสอบการเจาะระบบ (Penetration Test) ปี 66 ของระบบงานสำคัญ
- **IT4.** การการประเมินช่องโหว่ระบบ งานของ บสส. ปี 2565 (Vulnerability Assessment : VA)
- **IT5.** การการประเมินช่องโหว่ระบบงานของ บสส. ปี 2566 (Vulnerability Assessment : VA)
- **IT6.** การอัพเดต Critical Patch ของระบบงานสำคัญ
- **IT7.** การอัพเกรด Version ของระบบงานสำคัญ
- **IT8.** สิทธิการเข้าถึงระบบงานสำคัญ

Integrity

- **IT9.** ความคืบหน้าการพัฒนาระบบงานสำคัญเพื่อให้เกิดความถูกต้องสมบูรณ์ของข้อมูล
- **IT10.** Incident : ร้อยละของการแก้ไขข้อขัดข้องของระบบ งาน/ดำเนินการได้สำเร็จตาม SLA ที่ตกลงไว้

Availability

- **IT11.**ระบบ LRS สามารถใช้งานได้
- **IT12.**ระบบCDRP สามารถใช้งานได้
- **IT13.** ระบบD365 สามารถใช้งานได้
- **IT14.**ระบบOSLO สามารถใช้งานได้
- **IT15.** Backup Data (เวลา 22.00 – 10.00 น. Full Backup ทุกวัน)

Compliance

Law

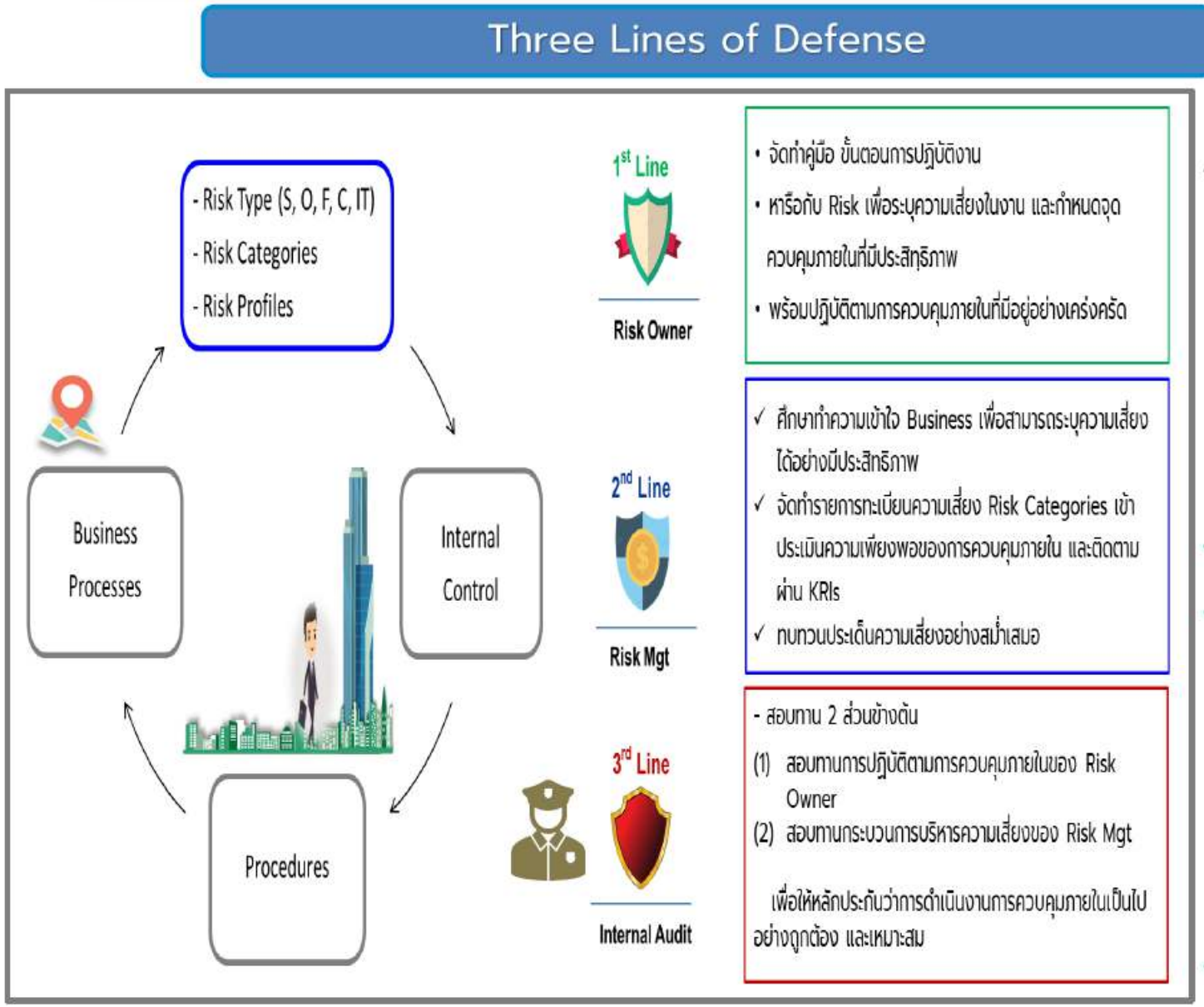
- **CO1.** การติดตามและการเตรียมการสำหรับการเปลี่ยนแปลงทางกฎหมายที่ซึ่งอาจส่งผลต่อการปฏิบัติงานของ บสส.
- **CO2.** การติดตามและการเตรียมการสำหรับการเปลี่ยนแปลงกฎหมายทั่วไป

Compliance

- **CO3.** การติดตามและการเตรียมการสำหรับการเปลี่ยนแปลงกฎเกณฑ์ของหน่วยงานกำกับ (Regulators)
- **CO4.** การไม่ปฏิบัติตามกฎหมายที่เกี่ยวข้องกับภาระกิจหลักของ บสส.
- **CO5.** การไม่ปฏิบัติตามกฎหมายทั่วไป เช่น PDPA ,กม. Digital, พรบ.จัดซื้อจัดจ้าง กม. ฟอกเงิน เป็นต้น
- **CO6.** การไม่ปฏิบัติตามกฎเกณฑ์ของ Regulators ที่เกี่ยวข้อง เช่น ธปท.

Previous | Current

ประสานงานกับทาง Audit เพื่อดำเนินงานตามหลักการ Three Lines of Defense



การปรับปรุงเพื่อให้เกิดความร่วมมือระหว่างกัน

- กรอบ หลักเกณฑ์มาตรฐานการจัดทำเรื่อง GRC
- แผนบริหารจัดการ Risk MGT ระยะเวลา 3 ปี
- ทบทวน จัดทำนโยบายการบริหารความเสี่ยงด้านต่างๆของ บสส.
- ทบทวน จัดทำเครื่องมือการบริหารความเสี่ยงด้านต่างๆของ บสส.
  - Risk Type (S, O, F, C, IT)
  - ระดับ Corporate : Risk Appetite, Risk Dashboard
  - ระดับ Department : Risk Metrix, Risk Categories, Risk Profiles
  - Regulator, กฎหมายที่เกี่ยวข้อง
- ทบทวน จัดทำการสื่อสารเพื่อสร้างความตะหนักเรื่อง GRC

การปรับปรุงเพื่อให้เกิดความร่วมมือระหว่างกัน

- การแลกเปลี่ยนข้อมูลระหว่างกันในเรื่อง Incident, Loss, Audit Issue เป็นต้น
- การพัฒนาโครงการ GRC เช่น การจัดอบรมเรื่อง 3 Lines of Defense
- การพัฒนาโครงการ ITA (ปปช.) ได้แก่ ช่องทางการแจ้งเบาะแสการทุจริต
- ร่วมกันชี้แจง ตอบประเด็นจากผู้ตรวจสอบ BOT
- เข้าประชุม และให้ความเห็นร่วมกันใน MM, IT Steering Committee, คณะทำงานอื่นๆ

สื่อสารเรื่องการบริหารความเสี่ยงการทุจริตเพื่อสร้างความตระหนักให้กับพนักงานภายในองค์กร

ภารกิจของ บสส.
บริหารจัดการสินทรัพย์ด้อยคุณภาพ

จึงต้องมีกระบวนการสร้างความโปร่งใส

เพื่อสร้างความมั่นใจในการดำเนินงานให้กับผู้มีส่วนได้เสีย

1.

[การป้องกันการทุจริต](#)

3.

Governance Structure มีโครงสร้างกรรมการ ผู้บริหาร และหน่วยงาน ทำหน้าที่กำกับดูแลการบริหารความเสี่ยงด้านการทุจริตภายในสานักงาน

มีระเบียบ นโยบาย ควบคุมดูแลการบริหารความเสี่ยงด้านการทุจริตภายในสำนักงาน

ใช้ระบบงาน ควบคุมการปฏิบัติงาน การอนุมัติงบประมาณ โครงการ และการเบิกจ่ายทรัพย์สิน

กระบวนการทำงาน มีคู่มือการปฏิบัติงาน Workflow และจุดควบคุมภายในที่ชัดเจน เช่น การสอบทานโดยหัวหน้างาน การ Check & Balance ภายใน และระหว่างหน่วยงาน

Three Lines of Defense มีผู้ประสานงานความเสี่ยงภายในฝ่ายงาน หน่วยงานกำกับดูแลการควบคุมภายใน และฝ่ายตรวจสอบการทำงาน

มีช่องทางการรับเรื่องร้องเรียน การแจ้งเบาะแสและระบบการรายงาน ติดตาม ข้อมูลต่างๆ ให้ผู้บริหารระดับสูงรับทราบอย่างต่อเนื่อง ข้อมูลต่างๆ ให้ผู้บริหารระดับสูงรับทราบอย่างต่อเนื่อง

[การมีส่วนร่วมของพนักงาน](#)

5.

- ปฏิบัติตามจรรยาบรรณพนักงาน
- ศึกษา ทำความเข้าใจ กฎ ระเบียบ ของสำนักงาน
- เคร่งครัดกับการปฏิบัติตามการควบคุมภายในที่มีอยู่
- ให้คำแนะนำเพื่อปิดช่องโหว่การกระทำทุจริต
- ช่วยกันสอดส่องดูแลสำนักงานให้ปลอดจากเรื่องทุจริต

4.

[การเฝ้าระวังการเกิดทุจริต](#)

- ✓ มีกล้อง CCTV และพนักงานรักษาความปลอดภัยเฝ้าระวังตามจุดต่างๆ
- ✓ มีระบบติดตามกระแสความเคลื่อนไหวบนโลก Social ที่กล่าวถึง บสส.
- ✓ มีการสื่อสารเพื่อแจ้งเตือนภัย และความเสี่ยงต่างๆ ให้พนักงานรับทราบ (Risk Monitor)
- ✓ มีระบบติดตาม รายงานสถานะความเสี่ยงให้ผู้บริหาร คณะกรรมการชุดย่อย และคณะกรรมการ บสส. รับทราบทุกเดือน
- ✓ มีระบบ IT Security ป้องกันภัยทาง Cyber
- ✓ มีการกำกับ และตรวจสอบการทำงานที่มีประสิทธิภาพ

2.

[ความหมายและประเภทของการทุจริต](#)

การกระทำโดยเจตนาเพื่อแสวงหาประโยชน์ที่มี
ควรได้โดยชอบด้วยกฎหมายสำหรับตนเองหรือผู้อื่น

THE END