การควบคุมภายในและการบริหารความเสี่ยง

โดย คณะทำงานบริหารความเสี่ยงและควบคุมภายในของสถาบันวิจัยสมุนไพร

ในการสัมมนาเชิงปฏิบัติการ เรื่อง

“การพัฒนาองค์การโดยบูรณาการเกณฑ์คุณภาพการบริหารจัดการภาครัฐกับระบบคุณภาพมาตรฐาน

ISO 9001:2015 ของสถาบันวิจัยสมุนไพร”

วันที่ 28 มกราคม 2559 ณ โรงแรม เดอะบลูม บาย ทีวีพูล อ.ปากช่อง จ.นครราชสีมา

ส่วนราชการต้องมีการบริหารจัดการความเสี่ยงเพื่อ ?

- สอดคล้องกับหลักการบริหารจัดการบ้านเมืองที่ดี (Good Governance)
- เป็นส่วนหนึ่งของการบริหารเชิงกลยุทธ์ ตามเกณฑ์คุณภาพการบริหารจัดการภาครัฐ (Public Sector Management Quality Award : PMQA)
- ISO 9001:2015 (ข้อกำหนด 6.1.1 และ 6.1.2)
- เพิ่มโอกาสในการบรรลุเป้าหมายและพันธกิจของส่วนราชการ
- พัฒนาผลงานขององค์กรให้มีประสิทธิภาพและประสิทธิผล

ความหมายและวัตถุประสงค์ของการควบคุมภายใน COSO : IC (Internal Control)

กระบวนการในการปฏิบัติงานที่ผู้กำกับดูแลฝ่ายบริหาร และบุคลากรของหน่วยงานจัดให้มีขึ้น เพื่อสร้างความมั่นใจอย่างสมเหตุสมผลว่าการดำเนินงานของหน่วยงานจะบรรลุวัตถุประสงค์ ดังต่อไปนี้

- เกิดประสิทธิผลและประสิทธิภาพของการดำเนินงาน (Operation : O)
- เกิดความน่าเชื่อถือของการรายงานทางการเงิน รวมถึงข้อมูลอื่น ๆ ในองค์กร (Financial : F)
- เกิดการปฏิบัติตามกฎหมาย ระเบียบและข้อบังคับที่เกี่ยวข้อง (Compliance : C)

แนวคิดพื้นฐานของการควบคุมภายใน

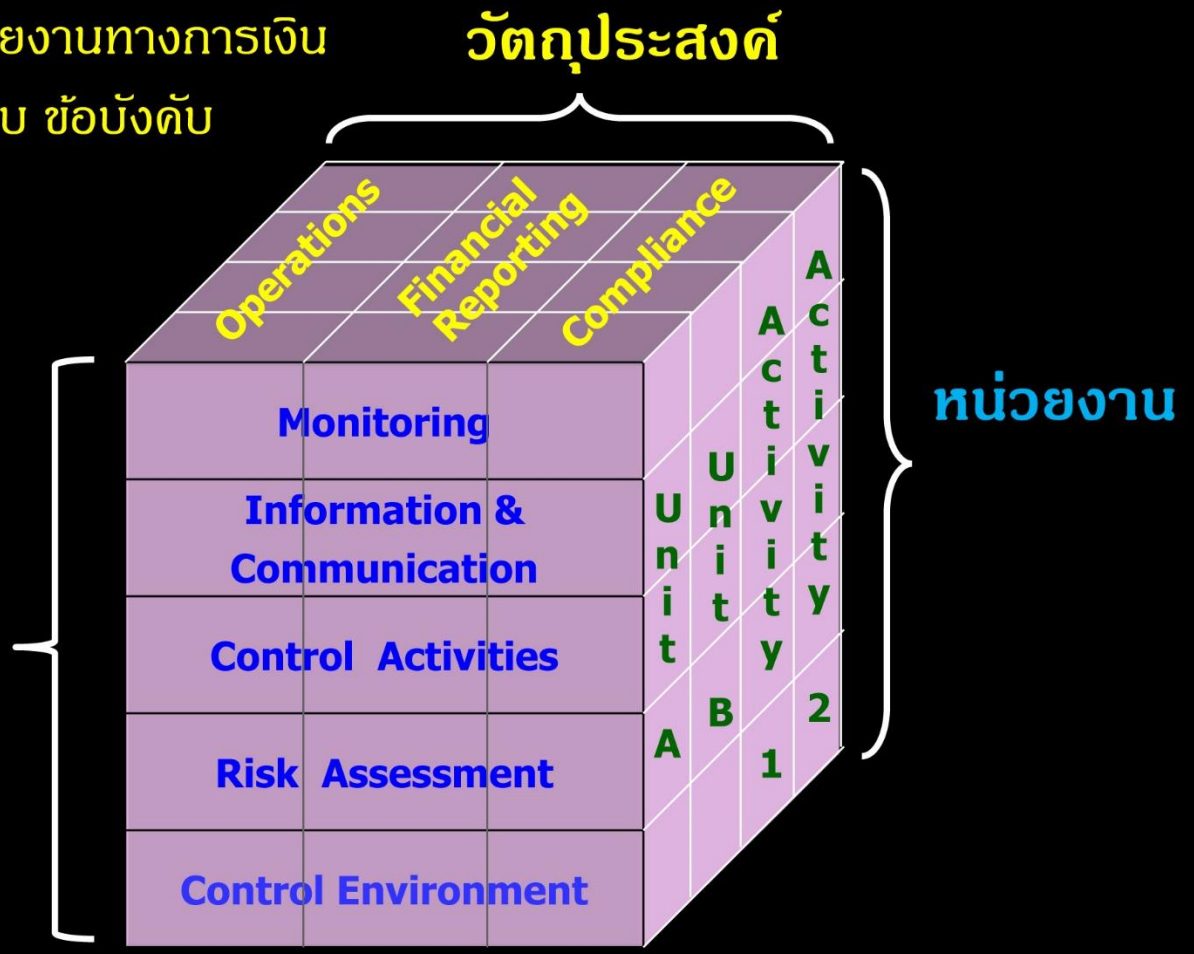
- เป็น “กระบวนการ” ที่รวมไว้หรือเป็นส่วนหนึ่งในการปฏิบัติงานตามปกติ
- เกิดขึ้นได้จาก “บุคลากรทุกระดับ” ในองค์กร
- ทำให้เกิด “ความมั่นใจอย่างสมเหตุสมผล” ว่า การดำเนินงานจะบรรลุผลสำเร็จตามวัตถุประสงค์

กรอบงานการควบคุมภายใน

1.ด้านความมีประประสิทธิภาพ
และประสิทธิผลของการดำเนินงาน
2.ด้านความเชื่อถือได้ของข้อมูลและรายงานทางการเงิน
3.ด้านการปฏิบัติตามกฎหมาย ระเบียบ ข้อบังคับ

5 องค์ประกอบ

1.สภาพแวดล้อมการควบคุมภายใน
2.การประเมินความเสี่ยง
3.กิจกรรมการควบคุม
4.สารสนเทศและการสื่อสาร
5.การติดตามและประเมินผล



การควบคุมภายในตามแนวคิดของ COSO

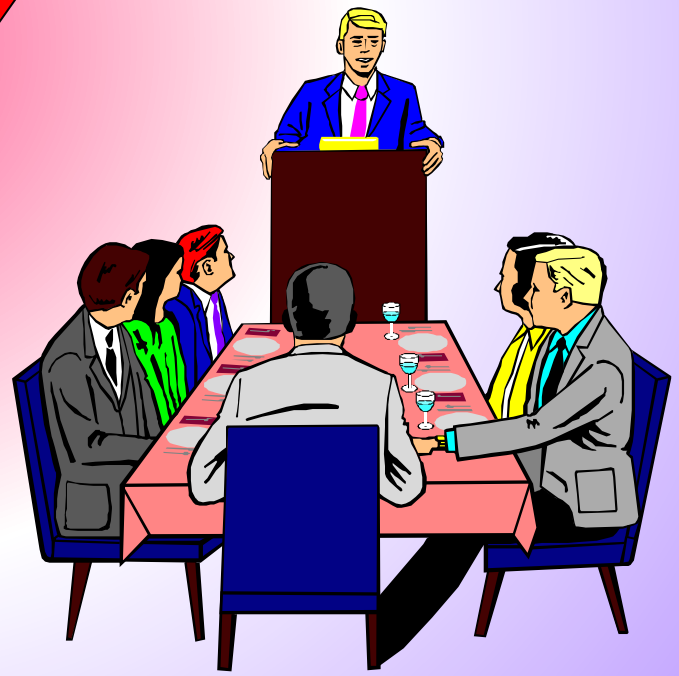
The Committee of Sponsoring Organizations of the Treadway Commission (COSO)

- องค์กรพิเศษที่ประกอบด้วยคณะกรรมการจากสมาคมต่างๆ ที่มาร่วมประชุมเป็นคณะทำงานเกี่ยวกับการพัฒนาระบบการควบคุมภายในของประเทศสหรัฐอเมริกา
- มาตรฐานเดิมของ COSO มีขึ้นเมื่อปี 2528 ปรับปรุงในปี 2547 โดยเปลี่ยนชื่อเป็น Enterprise Risk Management (ERM) Framework

การบริหารความเสี่ยงองค์กร
(Enterprise Risk Management)

COSO

การควบคุมภายใน
(Internal Control)



COSO : Enterprise Risk Management (ERM)

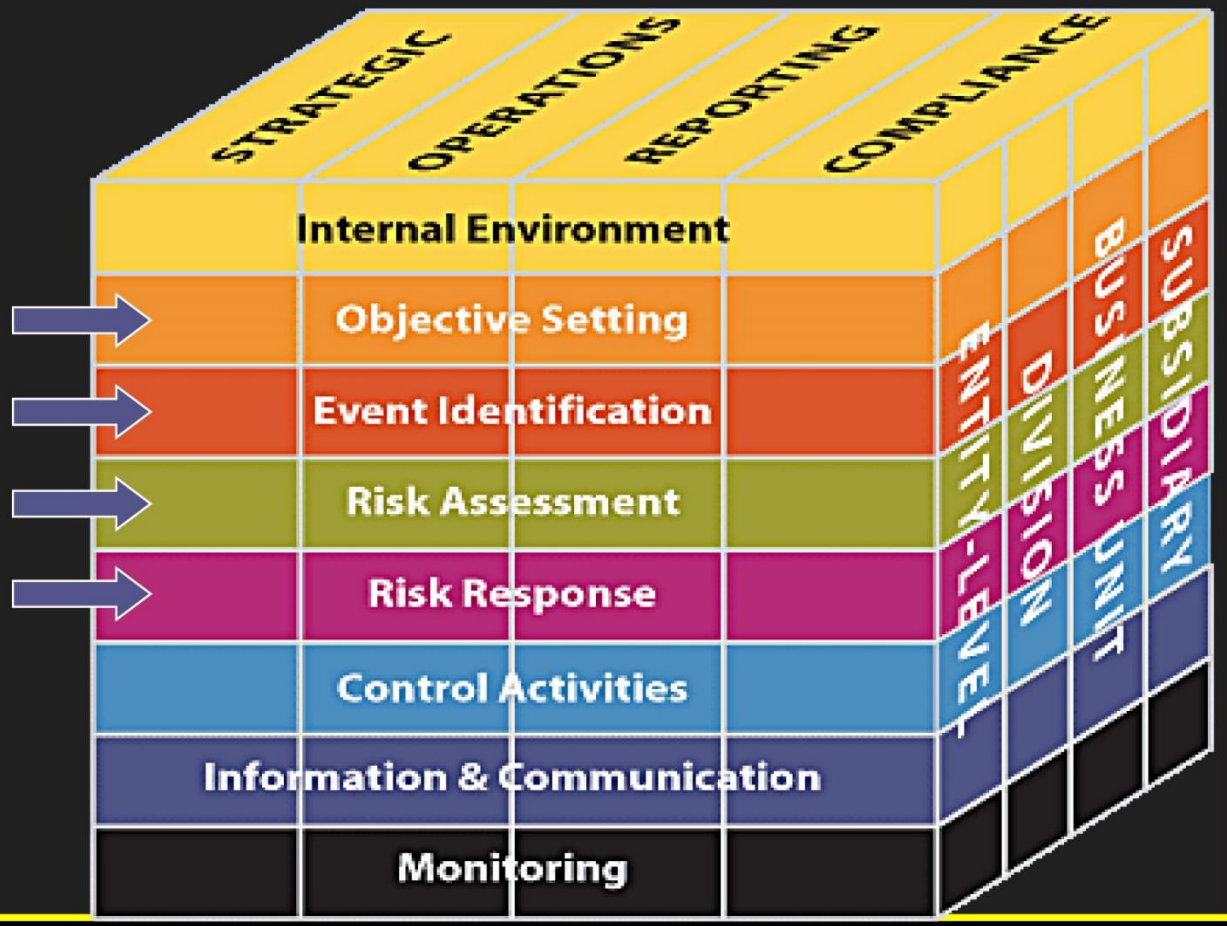
ให้แนวทางในการแจกแจงปัญหาและความเสี่ยงออกเป็นองค์ประกอบย่อย ๆ เพื่อความสะดวกในการวิเคราะห์และหาแนวทางในการบริหารจัดการ โดยแยกการบริหารความเสี่ยงออกเป็น 3 มิติ

มิติที่ 1 ด้านกระบวนการในการบริหารความเสี่ยง (ระบบการบริหารความเสียง)
ประกอบด้วย 8 องค์ประกอบ

องค์ประกอบของกรอบงานการบริหารความเสี่ยง
(COSO : Committee of Sponsoring Organization of The Treadway Commission)

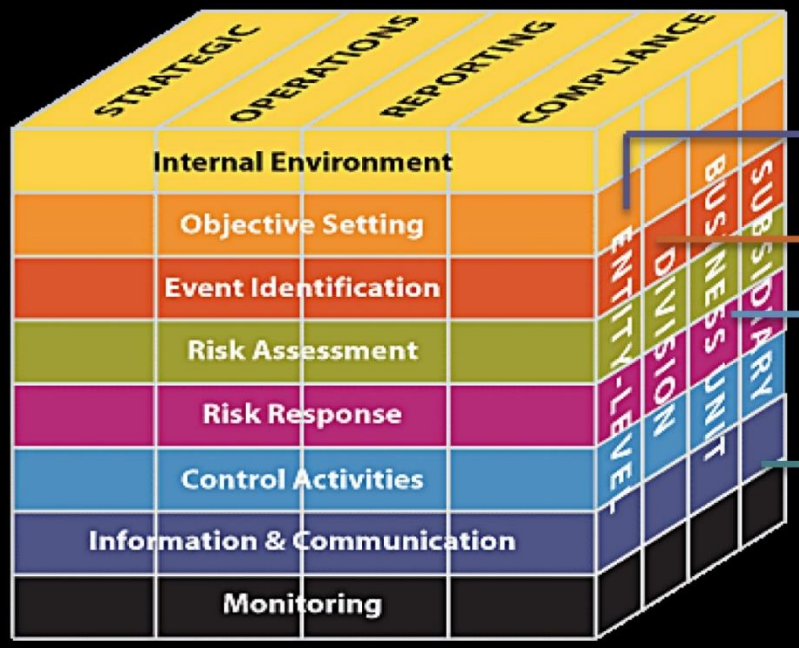
8 องค์ประกอบ

1. สภาพแวดล้อมภายในองค์กร
2. การกำหนดวัตถุประสงค์
3. การบ่งชี้เหตุการณ์
4. การประเมินความเสี่ยง
5. การตอบสนองความเสี่ยง
6. กิจกรรมเพื่อการควบคุม
7. สารสนเทศและการสื่อสาร
8. การติดตามและประเมินผล



มิติที่ 2 ด้านการบริหารจัดการความเสี่ยงระดับต่าง ๆ ในองค์กร

ระดับของหน่วยงานองค์กร

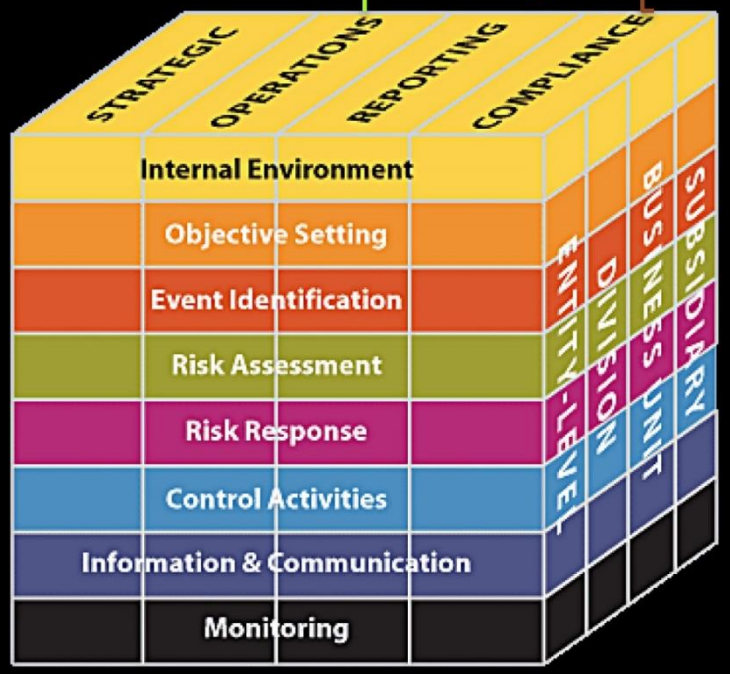


หน่วยงานองค์กร แบ่งออกได้เป็น 4 ระดับ คือ

1. ระดับทั่วทั้งองค์กร (Entity-level : EL)
2. ระดับส่วนงาน (Division : D)
3. ระดับหน่วยงาน (Business units : BU)
4. ระดับหน่วยงายย่อย (Subsidiary : S)

มิติที่ 3 ด้านการบรรลุวัตถุประสงค์ขององค์กร

วัตถุประสงค์การบริหารความเสี่ยง



1 ด้านกลยุทธ์ (Strategic) เป้าหมายระดับสูงต้องสอดคล้องและสนับสนุนพันธกิจขององค์กร

2 ด้านการปฏิบัติการ (Operation) การใช้ทรัพยากรอย่างมีประสิทธิผลและประสิทธิภาพ

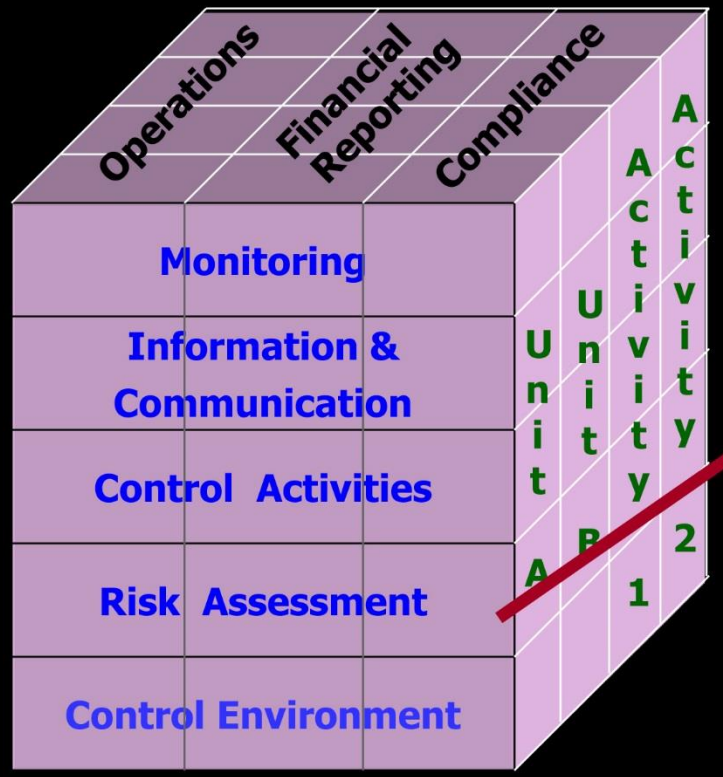
3 ด้านการรายงาน (Reporting) การรายงานมีความน่าเชื่อถือ

4 ด้านการปฏิบัติตามกฎระเบียบ (Compliance) การปฏิบัติให้ถูกต้องตามกฎระเบียบที่เกี่ยวข้อง

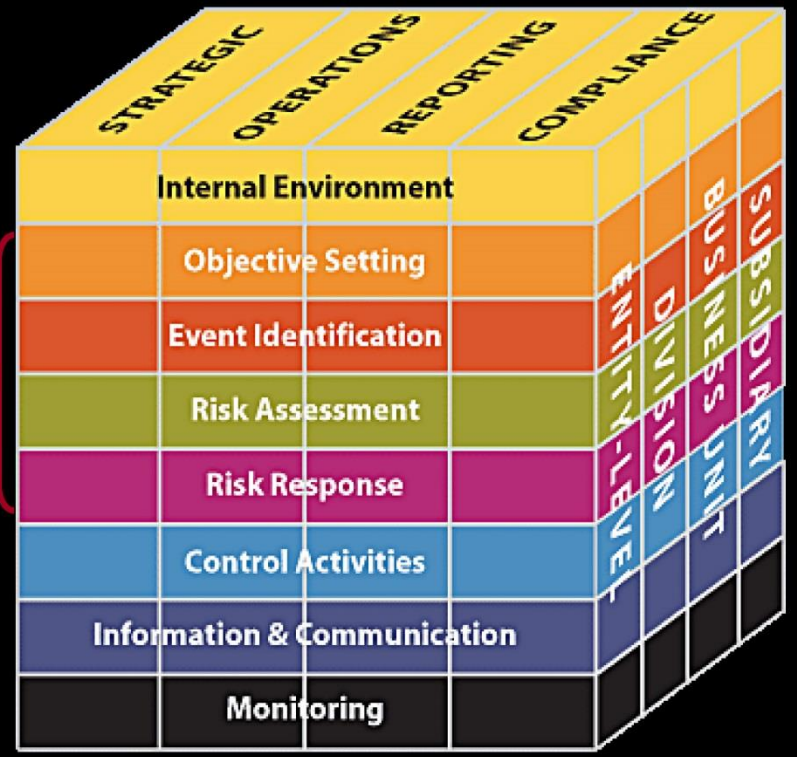
กรอบงานการบริหารความเสี่ยงและการควบคุมภายใน ตามแนวคิดของ COSO

(Committee of Sponsoring Organization of The Treadway Commission)

Control



ERM



ใครมีหน้าที่รับผิดชอบการควบคุมภายใน

- ☑ ผู้บริหารระดับสูง
- ☑ ผู้บริหารระดับรองลงมาทุกระดับ
- ☑ ผู้ปฏิบัติงานของหน่วยงาน
- ☑ ผู้ตรวจสอบภายใน

สภาพแวดล้อมการควบคุม (Control Environment)

หมายถึง สภาวการณ์หรือปัจจัยต่าง ๆ ที่ส่งผลให้เกิดระบบการควบคุมภายใน

- ความซื้อสัตย์และจริยธรรม
- ปรัชญาและรูปแบบการบริหาร
- โครงสร้างการจัดการองค์กร
- การมอบอำนาจและความรับผิดชอบ
- นโยบายด้านทรัพยากรมนุษย์
- ความรู้ ทักษะ และความสามารถ
- ผู้บริหารหรือคณะกรรมการตรวจสอบ

การประเมินความเสี่ยง (Risk Assessment)

กระบวนการระบุปัจจัยเสี่ยงและวิเคราะห์ความเสี่ยงอย่างเป็นระบบในการตัดสินใจรวมถึงการจัดลำดับความสำคัญว่าเหตุการณ์ใดหรือเงื่อนไขอย่างใดที่จะมีผลกระทบต่อการไม่บรรลุวัตถุประสงค์ของหน่วยงาน

กิจกรรมการควบคุม (Control Activities)

หมายถึง นโยบาย มาตรการ และวิธีการต่างๆ ที่ฝ่ายบริหารกำหนดหรือนำมาใช้ เพื่อลดความเสี่ยงที่จะเกิดขึ้น และช่วยเพิ่มความมั่นใจในความสำเร็จตามวัตถุประสงค์

ตัวอย่างกิจกรรมการควบคุม

1. การกำหนดระเบียบ ข้อบังคับ วิธีปฏิบัติ
2. การสอบทานการปฏิบัติ
3. การควบคุมการประมวลผลข้อมูล
4. การจัดทำบัญชี ทะเบียน รายงาน
5. การกำหนดขอบเขต อำนาจหน้าที่ความรับผิดชอบ
6. การแบ่งแยกหน้าที่ความรับผิดชอบ
7. การกำหนดดัชนีวัดผลการดำเนินงาน

ข้อมูลสารสนเทศและการสื่อสาร
(Information & Communication)

สารสนเทศ หมายถึง ข้อมูลข่าวสารที่ใช้ในการบริหารซึ่งเป็นข้อมูลเกี่ยวกับการเงินและไม่ใช่การเงินรวมทั้งข้อมูลข่าวสารอื่น ๆ ทั้งจากแหล่งภายในและภายนอก

การสื่อสาร หมายถึง การรับและส่งข้อมูลระหว่างกันเพื่อให้เกิดความเข้าใจอันดีระหว่างบุคคล ซึ่งมีหน้าที่ความรับผิดชอบในงานที่สัมพันธ์กัน การสื่อสารจะเกิดได้ทั้งภายในและภายนอกหน่วยงาน

การติดตามผลและประเมินผล (Monitoring)

การติดตามผล หมายถึง การสอดส่องดูแลกิจกรรมที่อยู่ระหว่างการดำเนินงาน เพื่อให้เกิดความมั่นใจว่าการดำเนินงานเป็นไปตามระบบการควบคุมภายในที่กำหนด

การประเมินผล หมายถึง การเปรียบเทียบผล การปฏิบัติงานกับระบบการควบคุมภายในที่กำหนดไว้ว่ามีความสอดคล้องหรือไม่ เพียงใด และสอบทานระบบการควบคุมภายในที่กำหนดไว้ว่ายังเหมาะสมกับสภาพแวดล้อมในปัจจุบันหรือไม่

ระบบการควบคุมภายในที่ดี

- มีความเหมาะสม เพียงพอ และรัดกุม
- มีความคุ้มค่า
- สามารถป้องกันความเสียหาย ความสูญเสีย สิ้นเปลือง สูญเปล่า
- ปฏิบัติงานได้สะดวก และปลอดภัย
- เสริมสร้างความพอใจ

ประโยชน์ของการควบคุมภายใน

- ทำให้การดำเนินงานของกิจการมีประสิทธิภาพ
- สินทรัพย์ของกิจการปลอดภัยจากการทุจริตทั้งปวง
- รายงานทางการเงินของกิจการมีความถูกต้องและน่าเชื่อถือ
- บุคลากรในหน่วยงานมีการปฏิบัติงานตามกฎระเบียบข้อบังคับ

การบริหารความเสี่ยงองค์กร

(Enterprise Risk Management : ERM)

กระบวนการที่ปฏิบัติโดยคณะกรรมการ ผู้บริหาร และบุคลากรทุกคนในองค์กร เพื่อช่วยในการกำหนดกลยุทธ์และการดำเนินงาน ซึ่งกระบวนการบริหารความเสี่ยงได้รับการออกแบบไว้ให้สามารถบ่งชี้เหตุการณ์ที่อาจเกิดขึ้น เพื่อให้ได้รับความมั่นใจอย่างสมเหตุสมผลในการบรรลุวัตถุประสงค์ที่องค์กรกำหนดไว้

ความเสี่ยง (Risk) คืออะไร

ความเป็นไปได้ที่จะเกิดเหตุการณ์ที่เป็นอุปสรรคต่อการบรรลุเป้าหมายขององค์กร ความเสี่ยงวัดได้จากผลกระทบที่ได้จากเหตุการณ์และโอกาสที่จะเกิดเหตุการณ์นั้น

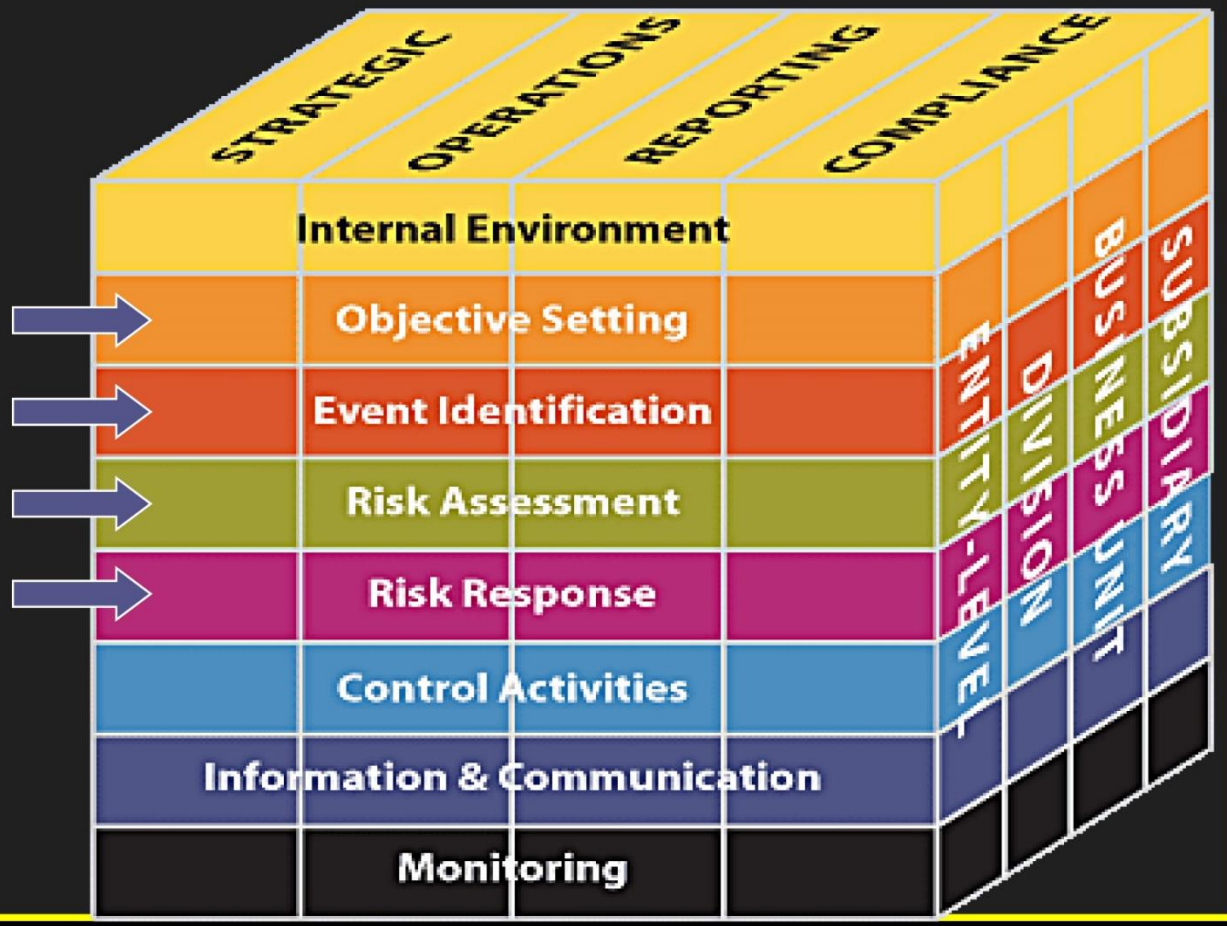
องค์ประกอบความเสี่ยง

ความเสี่ยง จะมีองค์ประกอบสองประการร่วมอยู่เสมอ คือ โอกาส (Opportunity) หรือความเป็นไปได้ (Possibility Likelihood) และผลกระทบ (Impact)

องค์ประกอบของกรอบงานการบริหารความเสี่ยง
(COSO : Committee of Sponsoring Organization of The Treadway Commission)

8 องค์ประกอบ

1. สภาพแวดล้อมภายในองค์กร
2. การกำหนดวัตถุประสงค์
3. การบ่งชี้เหตุการณ์
4. การประเมินความเสี่ยง
5. การตอบสนองความเสี่ยง
6. กิจกรรมเพื่อการควบคุม
7. สารสนเทศและการสื่อสาร
8. การติดตามและประเมินผล



แนวคิดพื้นฐาน

- เป็นกระบวนการ
- เกิดจากบุคลากร
- กำหนดกลยุทธ์องค์กร
- นำไปใช้ทั่วทั้งองค์กร
- จัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้
- สร้างความมั่นใจอย่างสมเหตุสมผล
- บรรลุวัตถุประสงค์

การบริหารความเสี่ยงขององค์กร

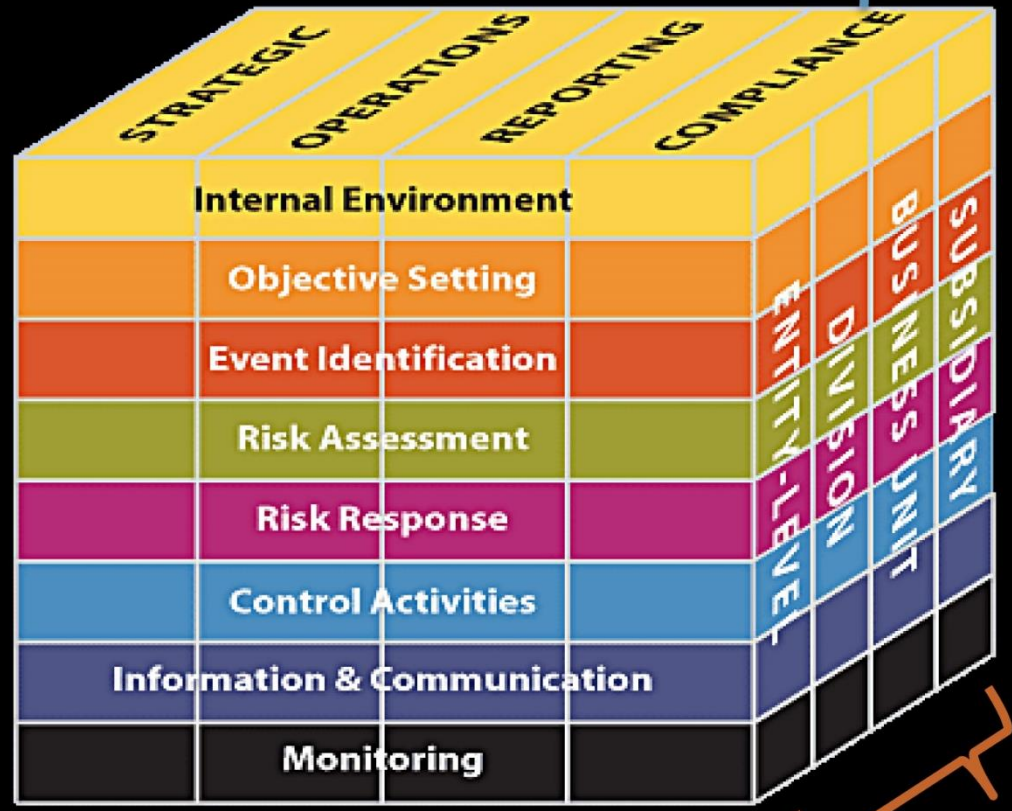
เป็นเครื่องมือนำไปสู่การบรรลุวัตถุประสงค์องค์กร

1. ด้านกลยุทธ์ (Strategic : S)
2. ด้านการดำเนินงาน (Operation : O)
3. ด้านการรายงาน (Reporting : R/Financial : F)
4. ด้านการปฏิบัติตามกฎ/ระเบียบ/ข้อบังคับ (Compliance : C)

กรอบงานการบริหารความเสี่ยง

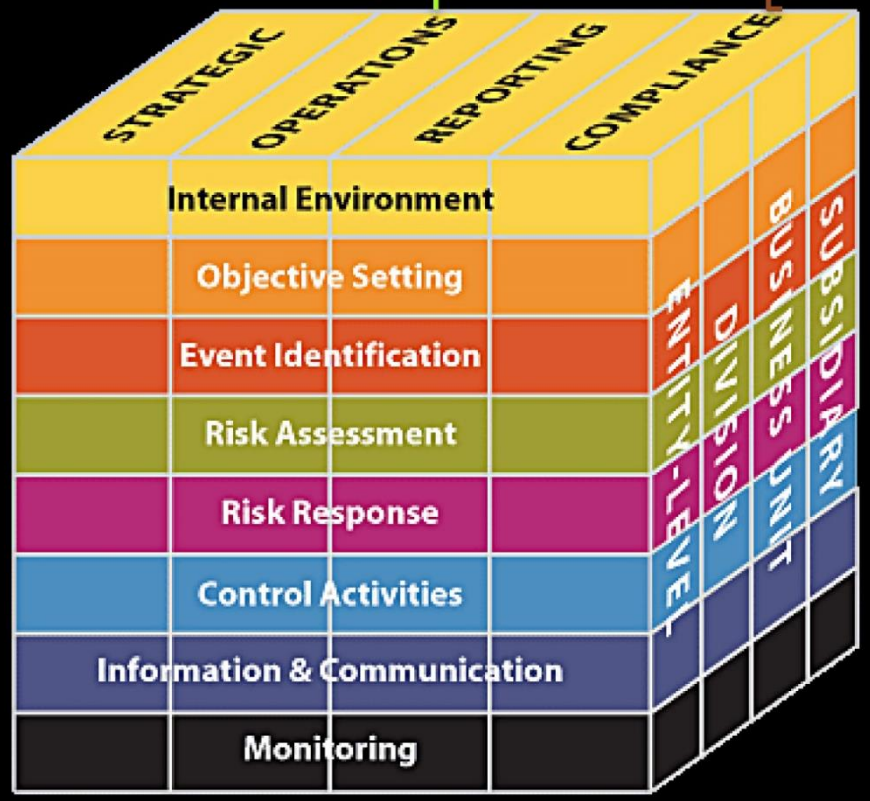
4 วัตถุประสงค์

8 องค์ประกอบ



ระดับของหน่วยงาน

วัตถุประสงค์การบริหารความเสี่ยง



1 ด้านกลยุทธ์ (Strategic) เป้าหมายระดับสูงต้องสอดคล้องและสนับสนุนพันธกิจขององค์กร

2 ด้านการปฏิบัติการ (Operation) การใช้ทรัพยากรอย่างมีประสิทธิผลและประสิทธิภาพ

3 ด้านการรายงาน (Reporting) การรายงานมีความน่าเชื่อถือ

4 ด้านการปฏิบัติตามกฎระเบียบ (Compliance) การปฏิบัติให้ถูกต้องตามกฎระเบียบที่เกี่ยวข้อง

ประเภทของความเสี่ยง

- ความเสี่ยงทางนโยบาย/กลยุทธ์ (Policy/Strategic Risk)
- ความเสี่ยงทางเศรษฐกิจ/การเมือง (Economic/Political Risk)
- ความเสี่ยงทางการเงิน (Financial Risk)
- ความเสี่ยงทางกฎ/ระเบียบ/ข้อบังคับ (Regulatory Risk)
- ความเสี่ยงทางธรรมชาติ (Natural Risk)

กระบวนการบริหารความสี่ยง

1. กำหนดวัตถุประสงค์และเป้าหมาย
2. การระบุความเสี่ยง
3. การประเมินความเสี่ยงและการกำหนดกลยุทธ์ในการจัดการความเสี่ยง
4. การเลือกวิธีการจัดการความเสี่ยง/กิจกรรมการบริหารความเสี่ยง
5. ข้อมูลและการสื่อสารด้านการบริหารความเสี่ยง
6. การติดตามและประเมินผล

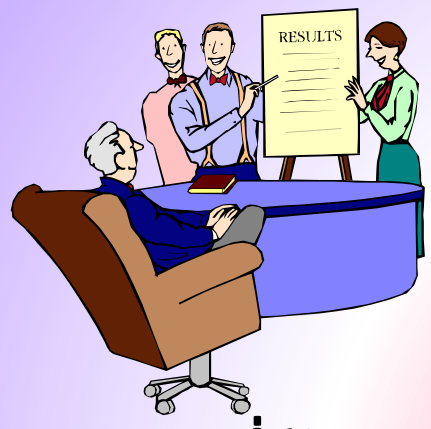
การจัดการความเสี่ยง

1. การหลีกเลี่ยง (Avoid)
2. การยอมรับ (Accept)
3. การลด (Reduce)
4. การโอน/กระจาย (Share)

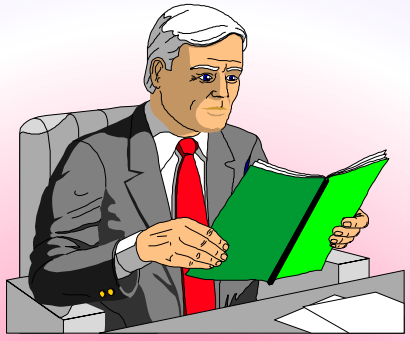
ประโยชน์ของการจัดระบบบริหารความเสี่ยงที่มีประสิทธิภาพ

- ☞ องค์กรสามารถบริหารความเสี่ยง หรือเตรียมแผนจัดการกับเหตุการณ์ที่อาจจะเกิดขึ้นได้อย่างมีประสิทธิภาพ
- ☞ สามารถกำหนดแผนกลยุทธ์และวัตถุประสงค์ที่สอดคล้องกับระดับความเสี่ยงที่ยอมรับได้
- ☞ สามารถตัดสินใจ และเลือกกลยุทธ์ในการบริหารความเสี่ยงที่ดีขึ้น
- ☞ เกิดการบริหารความเสี่ยงในภาพรวม และทั่วทั้งองค์กร
- ☞ การดำเนินงานเป็นไปตามกฎระเบียบ และกฎหมาย
- ☞ มีระบบข้อมูลเพื่อการตัดสินใจที่เชื่อมโยง และเหมาะสมยิ่งขึ้น
- ☞ เพิ่มประสิทธิภาพในการวางแผนการตรวจสอบภายใน

การสนับสนุนจากผู้บริหาร



เป้าหมายที่ชัดเจน



ความรับผิดชอบ

ปัจจัยสู่ความสำเร็จ

การดำเนินการต่อเนื่อง

การวัดและติดตามผล

การสื่อสารมีประสิทธิผล

ผลการจัดทำแผนบริหารความเสี่ยง

- ISO 9001:2015 ข้อกำหนดที่ 6.1.1 และ 6.1.2
- ISO 17025:2005 ข้อกำหนดที่ 4.10 (Improvement) และ ข้อกำหนดที่ 4.12 (Preventive action)
- การประเมินผลการควบคุมภายใน (แบบ ปย.1 และ ปย.2)
- PMQA (58) หมวด 2 ข้อ 2.1 ก (3)

เอกสารเพื่อการศึกษาและเรียนรู้เพิ่มเติม