



**แนวทางการวิเคราะห์
และจัดทำแผนบริหารความเสี่ยง (SP 7)
ตามเกณฑ์คุณภาพการบริหารจัดการภาครัฐ
ระดับพื้นฐาน**



ประเด็นการดำเนินการตาม SP 7

“ส่วนราชการต้องมีการวิเคราะห์และจัดทำแผนบริหารความเสี่ยงเพื่อเตรียมการรองรับสภาวะการเปลี่ยนแปลงที่จะเกิดขึ้น ซึ่งต้องครอบคลุมถึงความเสี่ยงเชิงยุทธศาสตร์ ความเสี่ยงด้านธรรมาภิบาล ด้านเทคโนโลยีสารสนเทศ และด้านกระบวนการ”

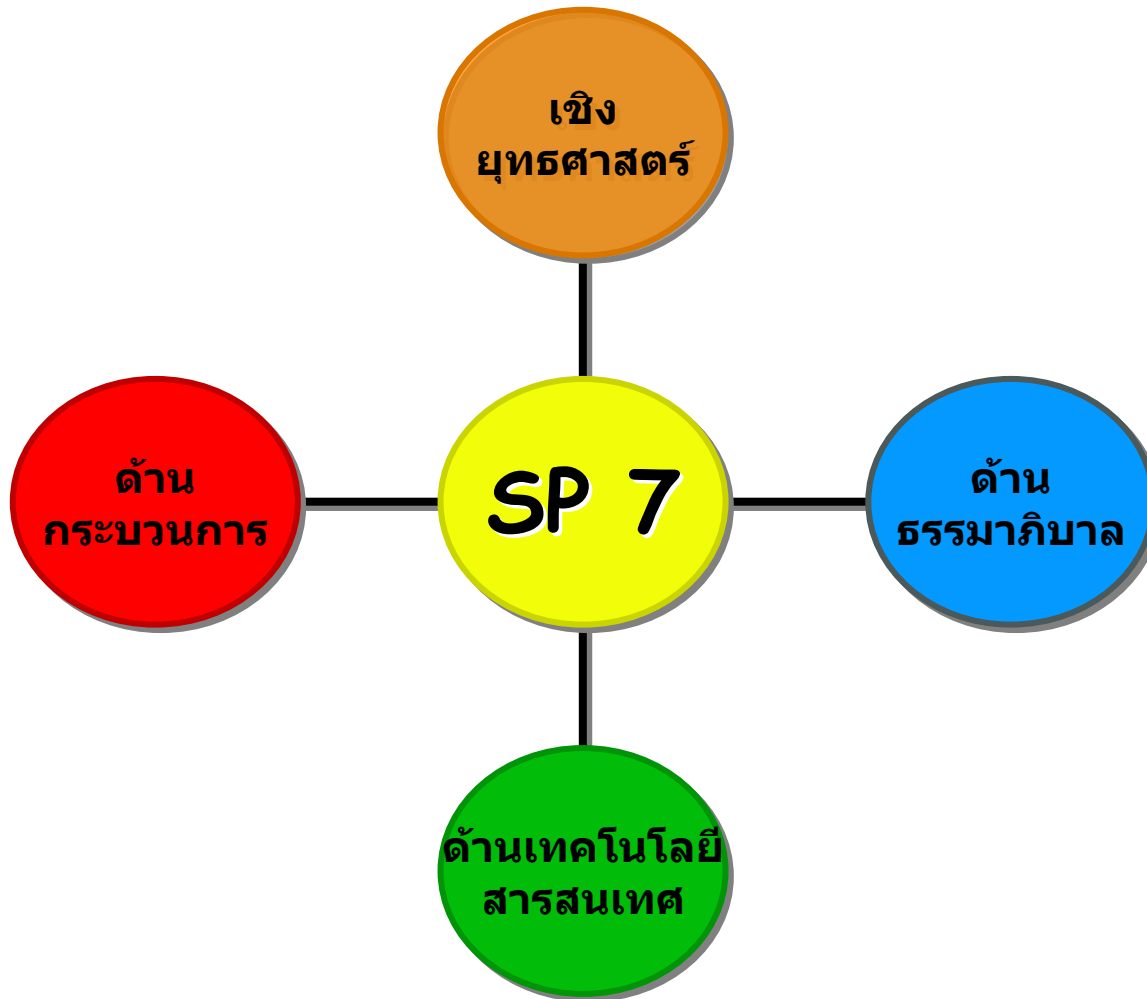
คำอธิบาย

การบริหารความเสี่ยง (Risk Management) หมายถึง กระบวนการที่ใช้ในการระบุ ความเสี่ยง การวิเคราะห์ความเสี่ยง และการกำหนดแนวทางการหรือมาตรการควบคุมเพื่อ ป้องกันหรือลดความเสี่ยง เพื่อมุ่งหวังให้ส่วนราชการบรรลุผลตามเป้าประสงค์ขององค์กร

การบริหารความเสี่ยงอย่างมีประสิทธิภาพ ส่วนราชการต้องมีขั้นตอนการดำเนินการ หลักเกณฑ์ในการวิเคราะห์อย่างเหมาะสม โดยครอบคลุม 5 ขั้นตอน คือ

1. การระบุความเสี่ยงหรือปัจจัยเสี่ยง
2. การวิเคราะห์ความเสี่ยง
3. การกำหนดมาตรการจัดการความเสี่ยงอย่างรัดกุม
4. การติดตาม รายงาน และประเมินผลการดำเนินการตามมาตรการจัดการความเสี่ยง ที่ได้กำหนดไว้
5. การทบทวนการบริหารความเสี่ยง โดยระบุกรอบเวลาในการทบทวนอย่างชัดเจน


มุมมองการจัดการความเสี่ยง





- **ความเสี่ยงเชิงยุทธศาสตร์** ส่วนราชการต้องมีการวิเคราะห์ความเสี่ยงในด้านต่าง ๆ ที่อาจก่อให้เกิดการเปลี่ยนแปลงหรือการไม่บรรลุผลตามเป้าหมายในแต่ละประเด็นยุทธศาสตร์ของส่วนราชการ และดำเนินการวางมาตรการบริหารความเสี่ยง

- **ความเสี่ยงด้านธรรมาภิบาล** ส่วนราชการต้องมีการวิเคราะห์ความเสี่ยงด้านธรรมาภิบาลที่จะเกิดขึ้นในกระบวนการหลักขององค์กร เพื่อให้มั่นใจว่าการดำเนินการเป็นไปตามหลักธรรมาภิบาล เช่น ความมีประสิทธิภาพ ความคุ้มค่า ความโปร่งใสตรวจสอบได้ เป็นต้น รวมถึง ส่วนราชการต้องมีการวิเคราะห์ความเสี่ยงในการกำกับดูแลตนเองที่ดีด้วย โดยต้องมีการจัดทำแผนธรรมาภิบาล และ/หรือแผนบริหารความเสี่ยงในเรื่องการกำกับดูแลตนเองที่ดี


- 
- **ความเสี่ยงด้านเทคโนโลยีสารสนเทศ** ส่วนราชการต้องมีการวางระบบบริหารความเสี่ยงของระบบฐานข้อมูลและสารสนเทศ โดยต้องดำเนินการดังต่อไปนี้

1. มีการบริหารความเสี่ยงเพื่อกำจัด ป้องกันหรือลดการเกิดความเสียหายในรูปแบบต่าง ๆ โดยสามารถฟื้นฟูระบบสารสนเทศ และการสำรองและกู้คืนข้อมูลจากความเสียหาย (Back up and Recovery)

2. มีการจัดทำแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจเกิดกับระบบสารสนเทศ (IT Contingency Plan)

3. มีระบบรักษาความมั่นคงและปลอดภัย (Security) ของระบบฐานข้อมูล เช่น ระบบ Anti-Virus ระบบไฟฟ้าสำรอง เป็นต้น

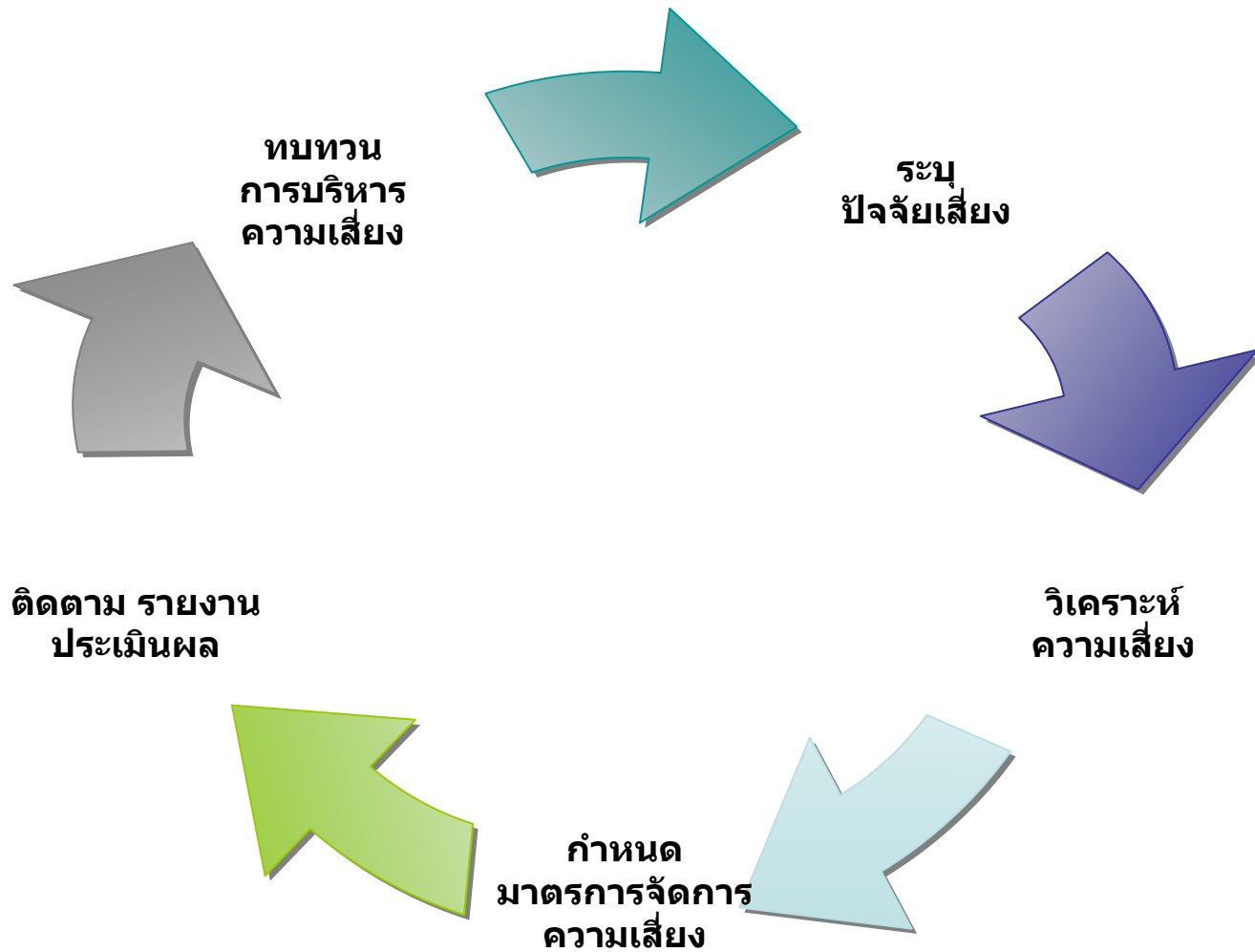
4. มีการกำหนดสิทธิให้ผู้ใช้ในแต่ละระดับ (Access rights)

- 
- **ความเสี่ยงด้านกระบวนการ** ส่วนราชการต้องมีการวางระบบบริหารความเสี่ยงของกระบวนการที่สร้างคุณค่าเพื่อให้เป็นไปตามมาตรฐานการปฏิบัติงานที่กำหนด

การบริหารความเสี่ยงของกระบวนการ อาจนำแนวคิดในการออกแบบระบบควบคุมมาใช้ได้ ซึ่งระบบการควบคุมกระบวนการมีปัจจัยสำคัญดังต่อไปนี้

- วัตถุประสงค์ของการควบคุม
- ความคุ้มค่าของการควบคุม
- ความทันการณ์ของการติดตามและบอกเหตุ
- ความสม่ำเสมอของกลไกการควบคุม
- การจูงใจผู้ปฏิบัติงาน

ขั้นตอนในการบริหารความเสี่ยงขององค์กร





หลักการและแนวทางการวิเคราะห์

ความเสี่ยง



การประเมินความเสี่ยง

โอกาสที่จะเกิด (L: Likelihood เป็นระดับของโอกาสหรือความบ่อยครั้งที่จะเกิดความเสี่ยง)

ผลกระทบ (I: Impact) คือ ระดับความรุนแรงของความเสี่ยงที่เกิดขึ้น

- 1 = โอกาสเกิดน้อยที่สุด / รุนแรงน้อยที่สุด
- 2 = โอกาสเกิดน้อย / รุนแรงน้อย
- 3 = โอกาสเกิดปานกลาง / รุนแรงปานกลาง
- 4 = โอกาสเกิดมาก / รุนแรงมาก
- 5 = โอกาสเกิดมากที่สุด / รุนแรงมากที่สุด

$$\text{ระดับความเสี่ยง} = L \times I$$



ผลกระทบต่อองค์กร (ด้านเวลา)

ผลกระทบ ต่อองค์กร	ความเสียหาย	ระดับ คะแนน
สูงมาก	ทำให้เกิดความล่าช้าของโครงการ มากกว่า 6 เดือน	5
สูง	ทำให้เกิดความล่าช้าของโครงการ มากกว่า 4.5 เดือน ถึง 6 เดือน	4
ปานกลาง	ทำให้เกิดความล่าช้าของโครงการ มากกว่า 3 เดือน ถึง 4.5 เดือน	3
น้อย	ทำให้เกิดความล่าช้าของโครงการ มากกว่า 1.5 เดือน ถึง 3 เดือน	2
น้อยมาก	ทำให้เกิดความล่าช้าของโครงการ ไม่เกิน 1.5 เดือน	1



ผลกระทบต่อองค์กร (ด้านชื่อเสียง)

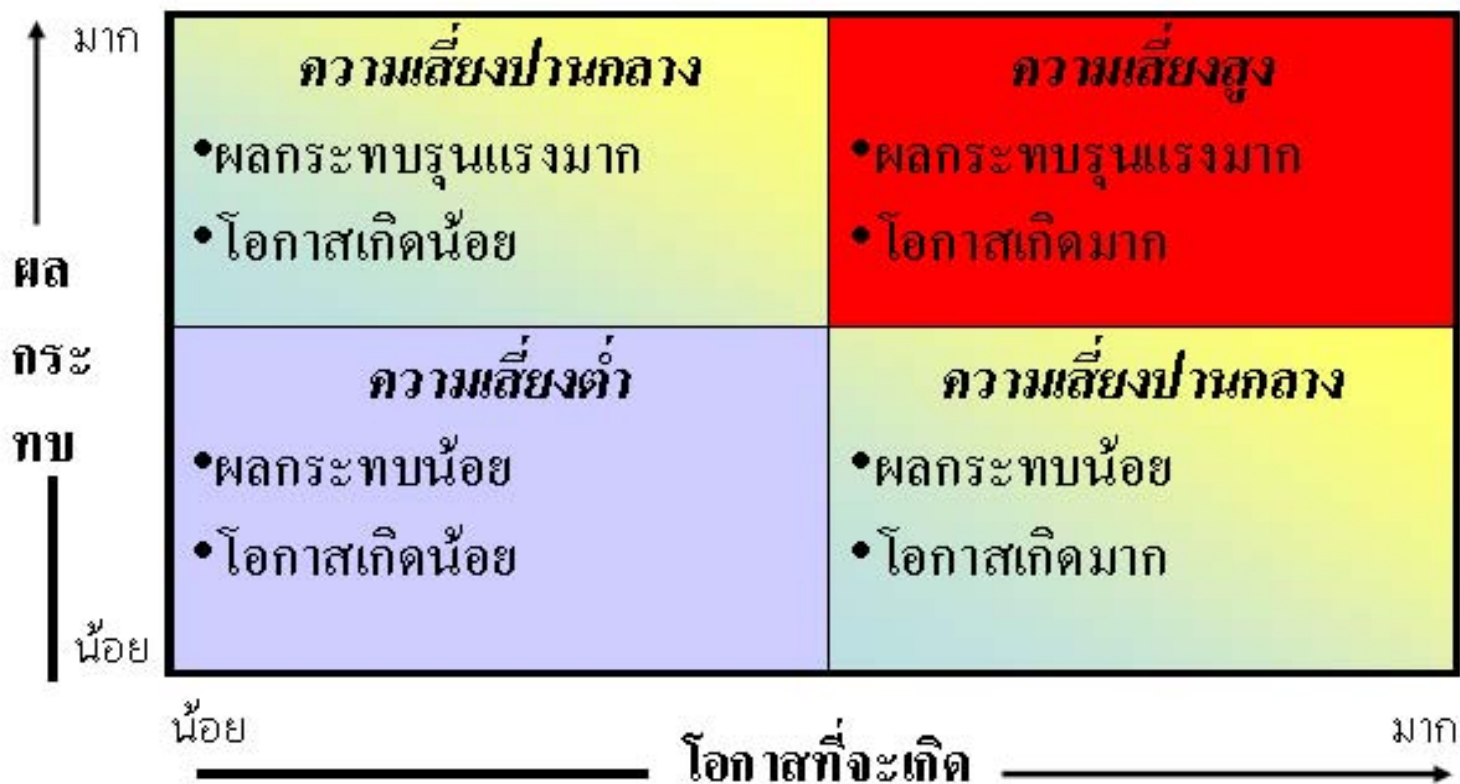
ผลกระทบ ต่อองค์กร	ความเสียหาย	ระดับ คะแนน
สูงมาก	มีการเผยแพร่ข่าวทั้งจากสื่อภายในและต่างประเทศเป็นวงกว้าง	5
สูง	มีการเผยแพร่ข่าวเป็นวงกว้างในประเทศและมีการเผยแพร่ข่าวอยู่ วงจำกัดในต่างประเทศ	4
ปานกลาง	มีการลงข่าวในหนังสือพิมพ์ในประเทศหลายฉบับ 2-3 วัน	3
น้อย	มีการลงข่าวในหนังสือพิมพ์ในประเทศบางฉบับ 1 วัน	2
น้อยมาก	ไม่มีการเผยแพร่ข่าว	1

การจัดลำดับความเสี่ยง

รวมคะแนนระหว่างโอกาสที่จะเกิดกับความเสียหาย/
ผลกระทบ เพื่อจัดลำดับความสำคัญ และใช้ในการ
ตัดสินใจว่าความเสี่ยงใดควรเร่งจัดการก่อน

จัดทำแผนภูมิความเสี่ยงเพื่อให้ผู้บริหารและคนใน
องค์กร ได้เห็นภาพรวมว่าความเสี่ยงมีการกระจายตัว
อย่างไร

แผนภูมิความเสี่ยง (Risk Map)



แผนภูมิความเสี่ยง (Risk Map)

ผลกระทบ

5					
4				สูง	มาก
3			สูง		
2		ปาน	กลาง		
1	ต่ำ				
	1	2	3	4	5

โอกาสที่จะเกิด

การจัดการความเสี่ยง

การจัดการความเสี่ยง : การวิเคราะห์ถึงต้นทุนและประโยชน์ที่จะ
ได้รับภายใต้ทางเลือก



การหลีกเลี่ยงความเสี่ยง



การถ่ายโอนความเสี่ยง



การยอมรับความเสี่ยง



การควบคุมความเสี่ยง



ขอบเขตการวิเคราะห์

ในแต่ละด้าน





ความเสี่ยงเชิงยุทธศาสตร์

- ความเสี่ยงเชิงยุทธศาสตร์ ส่วนราชการต้องมีการวิเคราะห์ความเสี่ยงในด้านต่าง ๆ ที่อาจก่อให้เกิดการเปลี่ยนแปลงหรือการไม่บรรลุผลตามเป้าหมายในแต่ละประเด็นยุทธศาสตร์ของส่วนราชการ และดำเนินการวางมาตรการบริหารความเสี่ยง

ตามแนวทางดำเนินการและแบบฟอร์มการวิเคราะห์
เช่นเดียวกันกับปีงบประมาณ พ.ศ. 2551

ด้านธรรมาภิบาล

- **ความเสี่ยงด้านธรรมาภิบาล** หมายถึง โอกาสหรือแนวโน้มที่จะประพฤติดีดหลักธรรมาภิบาลซึ่งส่งผลกระทบต่อรัฐ สังคม และสิ่งแวดล้อม ผู้รับบริการ และผู้มีส่วนได้ส่วนเสีย องค์กร และผู้ปฏิบัติงาน

สามารถศึกษารายละเอียดเพิ่มเติมได้ที่

คู่มือนโยบายการกำกับดูแลองค์กรที่ดี ภาคผนวก 5 หน้า 44

**และแนวทางดำเนินการตามตัวชี้วัด “ระดับความสำเร็จของการดำเนินการตาม
มาตรการป้องกันและปราบปรามการทุจริต”**

ตัวชี้วัดที่ 6 มิติที่ 2 มิติด้านคุณภาพการให้บริการ

ตามคำรับรองการปฏิบัติราชการ

การระบุปัจจัยเสี่ยงด้านธรรมาภิบาล

หลักธรรมาภิบาล	ความหมาย	ความเสี่ยงที่อาจเกิดขึ้น
ความซื่อสัตย์	การปฏิบัติหน้าที่อย่างตรงไปตรงมาตาม กฎหมาย กฎระเบียบ รักษาവാจาสัตย์ เปิดใจ กว้าง ไม่หลอกลวง ไม่ปิดความรับผิดชอบ ไม่ใช้ผู้อื่นเป็นเครื่องมือเพื่อแสวงหาผลประโยชน์ส่วนตัว	<ul style="list-style-type: none"> ใช้อำนาจหน้าที่เพื่อเอื้อประโยชน์ต่อพวกพ้อง ใช้ช่องโหว่ทางกฎหมายเพื่อแสวงหาประโยชน์ส่วนตัว
ความโปร่งใส	การเปิดเผยข้อมูล วิธีการและขั้นตอนการดำเนินงาน รวมทั้งเปิดโอกาสให้มีส่วนร่วมรับรู้ มีส่วนเกี่ยวข้องของกับ กระบวนการตัดสินใจ กระบวนการดำเนินการ และตรวจสอบการทำงาน	<ul style="list-style-type: none"> ไม่เปิดเผยข้อมูลและขั้นตอนการดำเนินการ เปิดเผยข้อมูลไม่ครบถ้วน บิดเบือนข้อมูล ไม่เปิดเผยข้อมูลเพื่อการตรวจสอบการทำงาน
ความยุติธรรม	การปฏิบัติต่อผู้อื่นด้วยความเป็นธรรมและเท่าเทียมกัน โดยยึดหลักด้านสิทธิผลประโยชน์ ข้อดี ความพยายามของแต่ละคน หรือการช่วยเหลือสังคมเป็นพื้นฐานในการตัดสินใจ	<ul style="list-style-type: none"> ปฏิบัติต่อผู้รับบริการอย่างไม่เป็นธรรม เสมอภาค เอื้อประโยชน์ให้กับกลุ่มใด กลุ่มหนึ่งเป็นพิเศษ
ความสามัคคี	การช่วยเหลือ ให้ความเคารพซึ่งกันและกัน ทำงานร่วมกันอย่างมีประสิทธิภาพเพื่อบรรลุเป้าหมายเดียวกัน	<ul style="list-style-type: none"> แบ่งพรรคแบ่งพวกในการทำงาน ไม่ให้ความร่วมมือในการทำงาน

การระบุปัจจัยเสี่ยงด้านธรรมาภิบาล

หลักธรรมาภิบาล	ความหมาย	ความเสี่ยงที่อาจเกิดขึ้น
ความมีประสิทธิภาพ	การทำงานอย่างรวดเร็วและใช้ทรัพยากรที่มีอยู่อย่างจำกัดให้ได้ผลคุ้มค่าและก่อให้เกิดประโยชน์สูงสุด	<ul style="list-style-type: none"> • ปฏิบัติงานล่าช้ากว่ากำหนด • ขาดระบบและขั้นตอนการดำเนินการที่มีประสิทธิภาพ
ความรับผิดชอบ	การรับผิดชอบต่อการตัดสินใจปฏิบัติงานและผลที่เกิดขึ้น	<ul style="list-style-type: none"> • โยนความผิดให้กับผู้อื่น • ไม่ยินดีให้มีการตรวจสอบ • ไม่รับผิดชอบต่อผลที่เกิดขึ้น
การมุ่งเน้นผลงาน	การปฏิบัติงานให้สำเร็จตามเป้าหมาย สามารถวัดหรือประเมินผลได้อย่างเป็นรูปธรรม	<ul style="list-style-type: none"> • ขาดเป้าหมายและแผนงานที่ชัดเจนในการดำเนินการ • งานไม่สำเร็จตามเป้าหมาย
ความคล่องตัว	การเรียนรู้และปรับตัวให้ทันกับเศรษฐกิจ สังคม และสิ่งแวดล้อมที่เปลี่ยนแปลงไป	<ul style="list-style-type: none"> • ไม่ปรับตัวต่อการเปลี่ยนแปลงที่เกิดขึ้น
การทุจริตคอรัปชั่น	การประพฤติปฏิบัติโดยใช้อำนาจหน้าที่ทำผิดกฎหมาย หรือระเบียบ มีการฉ้อโกงทรัพย์สินของทางราชการ	<ul style="list-style-type: none"> • เจ้าหน้าที่รับสินบนในการทำงาน



ตาราง การวิเคราะห์ความเป็นไปได้และระดับความเสี่ยง

	ระดับ				
		ต่ำ	กลาง	สูง	รุนแรงมาก
ความเป็นไปได้	ต่ำ	C	C	B	A
	กลาง	C	B	A	A
	สูง	B	A	A	A

แนวทางลดและบรรเทาความเสี่ยง

เกรด A หมายถึง ต้องดำเนินการลดความเสี่ยงทันที

เกรด B หมายถึง จะกำหนดแนวทางลดความเสี่ยงในระยะกลางและระยะยาวต่อไป

เกรด C หมายถึง รับทราบ แต่ไม่ต้องดำเนินการใดๆ ยกเว้นระดับความเสี่ยงจะสูงขึ้นเมื่อเวลาผ่านไป



ตารางที่ ตัวอย่างการจัดลำดับความเสี่ยง

หลักธรรมาภิบาล	ความเสี่ยงที่อาจเกิดขึ้น	เกรดที่ได้รับ
ความซื่อสัตย์	▪ ใช้อำนาจหน้าที่เพื่อเอื้อประโยชน์ต่อพวกพ้อง	A
	▪ ใช้ช่องโหว่ทางกฎหมายเพื่อแสวงหาประโยชน์ส่วนตัว	A
ความโปร่งใส	▪ ไม่เปิดเผยข้อมูลและขั้นตอนการดำเนินการ	B
	▪ เปิดเผยข้อมูลไม่ครบถ้วน บิดเบือนข้อมูล	A
	▪ ไม่เปิดเผยข้อมูลเพื่อการตรวจสอบการทำงาน	A
ความยุติธรรม	▪ ปฏิบัติต่อผู้รับบริการอย่างไม่เป็นธรรม เสมอภาค	A
	▪ เอื้อประโยชน์ให้กับกลุ่มใด กลุ่มหนึ่งเป็นพิเศษ	A
ความสามัคคี	▪ แบ่งพรรคแบ่งพวกในการทำงาน	B
	▪ ไม่ให้ความร่วมมือในการทำงาน	B
ความมีประสิทธิภาพ	▪ ปฏิบัติงานล่าช้ากว่ากำหนด	A
	▪ ขาดระบบและขั้นตอนการดำเนินการที่มีประสิทธิภาพ	B
ความรับผิดชอบ	▪ โยนความผิดให้กับผู้อื่น	B
	▪ ไม่ยินดีให้มีการตรวจสอบ	A
	▪ ไม่รับผิดชอบต่อผลที่เกิดขึ้น	A

ด้านเทคโนโลยีสารสนเทศ

- โครงสร้างด้าน IT
- นโยบายและระเบียบปฏิบัติด้าน IT
- การตรวจสอบและการควบคุมการปฏิบัติงาน

- Network Security
- การกำหนดสิทธิและการควบคุมผู้ใช้งาน
- การจัดการและตรวจสอบระบบเครือข่าย
- การป้องกันไวรัส

- มีขั้นตอนการปฏิบัติงานของเจ้าหน้าที่เป็นลายลักษณ์อักษร
- มีการติดตามการทำงานและประสิทธิภาพของระบบคอมพิวเตอร์
- มีการบันทึกเหตุการณ์ผิดปกติของระบบคอมพิวเตอร์เป็นประจำ
- มีสัญญาบำรุงรักษาอุปกรณ์คอมพิวเตอร์

- มีแผนฉุกเฉินเป็นลายลักษณ์อักษร และมีการสื่อสารผู้ที่เกี่ยวข้อง
- มีศูนย์สำรอง
- มีการทดสอบแผนฉุกเฉิน

ระบบปฏิบัติงานประจำด้านคอมพิวเตอร์

แผนฉุกเฉิน

โครงสร้างและระบบการจัดการ

มุมมองการบริหารความเสี่ยงด้าน IT

การสำรองข้อมูลและโปรแกรม

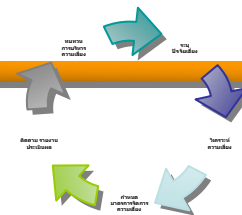
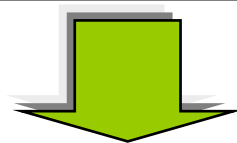
การรักษาความปลอดภัยข้อมูลและเครือข่าย

การรักษาความปลอดภัยศูนย์คอมพิวเตอร์

- มีระบบสำรองข้อมูลทั้ง front และ back office
- มีความถี่ในการจัดเก็บและการตรวจสอบ

- การควบคุมการเข้าออกศูนย์
- การป้องกันความเสียหายภายในศูนย์

นำขอบเขตแต่ละด้านมาวิเคราะห์ 5 ขั้นตอนหลัก



- **สิ่งที่ต้องดำเนินการ ในปีงบประมาณ พ.ศ. 2552**

ต้องมีการกำหนดมาตรการจัดการความเสี่ยงอย่างน้อยใน 4 ประเด็น ดังต่อไปนี้

1. มีการบริหารความเสี่ยงเพื่อกำจัด ป้องกันหรือลดการเกิดความเสียหายในรูปแบบต่าง ๆ โดยสามารถฟื้นฟูระบบสารสนเทศ และการสำรองและกู้คืนข้อมูลจากความเสียหาย (Back up and Recovery)

2. มีการจัดทำแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจจะเกิดกับระบบสารสนเทศ (IT Contingency Plan)

3. มีระบบรักษาความมั่นคงและปลอดภัย (Security) ของระบบฐานข้อมูล เช่น ระบบ Anti-Virus ระบบไฟฟ้าสำรอง เป็นต้น

4. มีการกำหนดสิทธิให้ผู้ใช้ในแต่ละระดับ (Access rights)

โดยในแต่ละประเด็น ต้องมีรายละเอียดในการดำเนินการเพื่อนำมาจัดทำแผนบริหารความเสี่ยงต่อไป

ด้านกระบวนการ

- ✓ นำกระบวนการที่สร้างคุณค่า (ตามที่ระบุในหมวด 6) มาวิเคราะห์ตาม 5 ขั้นตอนหลัก ภายใต้ขอบเขตการวิเคราะห์ดังนี้
 - ❖ วัตถุประสงค์ของการควบคุม เช่น ตัวชี้วัดกระบวนการ มาตรฐานงาน
 - ❖ ความคุ้มค่าของการควบคุม เช่น ความสามารถในการลดค่าใช้จ่าย
 - ❖ ความทันการณ์ของการติดตามและบอกเหตุ เช่น ระบบเตือนภัยของกระบวนการ
 - ❖ ความสม่ำเสมอของกลไกการควบคุม เช่น ระบบรายงานและติดตามผล
 - ❖ การจูงใจผู้ปฏิบัติงาน เช่น การเชื่อมโยงกับระบบประเมินผล
- ✓ จัดลำดับความสำคัญของการดำเนินการ
- ✓ เลือกนำมาจัดทำแผนบริหารความเสี่ยง



**สำหรับแบบฟอร์มในการจัดทำของแต่ละด้าน
สามารถใช้ตามแนวทางดำเนินการเดิม
(การบริหารความเสี่ยงเชิงยุทธศาสตร์)
มาประยุกต์ใช้ได้**