

บทที่ ๓

กระบวนการบริหารความเสี่ยง

๓.๑ ขั้นตอนการบริหารความเสี่ยง

ในการพัฒนาและทบทวนกระบวนการบริหารความเสี่ยงและควบคุมภายในขององค์การบริหารส่วนตำบลหินดาดจะนำหลักการของมาตรฐาน COSO ซึ่งมีการดำเนินงานที่สำคัญประกอบไปด้วย ๘ ขั้นตอน

๑. ทบทวนการดำเนินงานขององค์การบริหารส่วนตำบลหินดาด(Establishing the Context) เป็นการทบทวนทิศทาง และสภาพแวดล้อมภายในขององค์กร (Internal Environment) ภารกิจ และกิจกรรมภายใน ทบทวนนโยบาย (Policy) และเป้าหมาย (Objective) ในการบริหารความเสี่ยงของ องค์กร

๒. การระบุประเด็นความเสี่ยง (Risk Identification) เป็นการกำหนดประเด็นความเสี่ยงที่มีความสัมพันธ์สอดคล้องกับยุทธศาสตร์ และกลยุทธ์ขององค์การบริหารส่วนตำบลหินดาดโดยแบ่งออกเป็น ๔ ด้าน คือ ความเสี่ยงด้านนโยบาย (Strategic Risk) ความเสี่ยงด้านการดำเนินงาน (Operational Risk) ความเสี่ยงด้านการเงิน (Financial Risk) และความเสี่ยงด้านการกฎระเบียบ (Compliance Risk) พร้อมกำหนดเจ้าภาพในการบริหารความเสี่ยง (Risk Owner) ระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) และระดับความเบี่ยงเบนที่ยอมรับได้ (Risk Tolerance) ของแต่ละประเด็นความเสี่ยง

๓. การวิเคราะห์ปัจจัยเสี่ยง (Risk Analysis) เป็นการวิเคราะห์ปัจจัยเสี่ยงที่มี (Risk Factor) และการค้นหาสาเหตุของความเสี่ยง (Risk Cause / Root Cause) ที่มีความสัมพันธ์กับแต่ละปัจจัยเสี่ยง รวมถึงการกำหนดเกณฑ์ในการประเมินโอกาสในการเกิดความเสี่ยง (Likelihood) และผลกระทบของความเสี่ยง (Impact) พร้อมกำหนดระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite)

๔. การประเมินระดับความรุนแรงของความเสี่ยง (Risk Evaluation) เป็นการระบุระดับของโอกาสที่จะเกิด (Likelihood) และผลกระทบ (Impact) ในแต่ละสาเหตุความเสี่ยง (Risk Cause/ Root Cause) ทั้งระดับในปัจจุบัน และระดับที่ต้องการ

๕. การกำหนดมาตรการในการตอบสนองความเสี่ยง (Risk Response) เป็นการกำหนดค่าระดับความรุนแรงของความเสี่ยง (Likelihood x Impact : LI) ที่จำเป็นต้องดำเนินการวางแผนในการตอบสนอง ความเสี่ยง โดยจะกำหนดมาตรการในการรองรับความเสี่ยงสำหรับปัจจัยเสี่ยงที่มีค่าระดับความรุนแรงของความเสี่ยงในระดับสูงมาก (Very High) และระดับสูง (High) ซึ่งจะประเมินทางเลือกที่เหมาะสมในการตอบสนองความเสี่ยง ได้แก่ การยอมรับความเสี่ยง (Take) การลดโอกาสในการเกิดและผลกระทบของแต่ละความเสี่ยง (Treat) การหลีกเลี่ยงความเสี่ยง (Terminate) และการถ่ายโอนความเสี่ยง (Transfer)

๖. การจัดทำแผนที่ความเสี่ยง (Risk Map) เป็นการเชื่อมโยงสาเหตุและปัจจัยความเสี่ยง เข้ากับยุทธศาสตร์ และกลยุทธ์ขององค์กร

๗. การทบทวนและสอบทานตัวชี้วัดความเสี่ยง (Key Risk Indicator : KRI) เป็นการกำหนด ดัชนีชี้วัดของความเสี่ยงหลัก เพื่อเป็นปัจจัยในการพิจารณาทิศทางของความเสี่ยงว่ามีแนวโน้มเพิ่มขึ้น หรือลดลง และเป็นสัญญาณเตือนให้องค์กรสามารถรับรู้ และสามารถบริหารจัดการความเสี่ยงได้ทัน ต่อเหตุการณ์รวมทั้งช่วยสนับสนุนกิจกรรมควบคุมภายใน

๘. การจัดทำคู่มือและแผนในการบริหารความเสี่ยง (Risk Management Plan and Manual) แบ่งออกเป็น ๒ ส่วน คือ (๑) คู่มือการบริหารความเสี่ยง ประกอบไปด้วยหลักการและแนวทาง ในการบริหารความเสี่ยง

ในการบริหารความเสี่ยง ประเด็นความเสี่ยงหลัก ปัจจัยเสี่ยง สาเหตุหลักของความเสี่ยงเกณฑ์ต่างๆ ที่ใช้ในการประเมินระดับของโอกาสในการเกิดความเสี่ยง และระดับผลกระทบที่เกิดจากความเสี่ยง การจัดทำแผนที่ความเสี่ยง การทบทวนและสอบทานตัวชี้วัดความเสี่ยง และ (๒) แผนการบริหารความเสี่ยง ประกอบไปด้วยมาตรการที่จะตอบสนองต่อความเสี่ยงในแต่ละปัจจัยเสี่ยง แผนในการดำเนินการตามมาตรการและแผนการติดตามควบคุมความเสี่ยง

๓.๒ กระบวนการบริหารจัดการความเสี่ยง

กระบวนการบริหารจัดการความเสี่ยง เป็นกระบวนการที่ใช้ในการระบุ วิเคราะห์ ประเมินและจัดลำดับความเสี่ยงที่มีผลกระทบต่อการบรรลุวัตถุประสงค์ในการดำเนินงานขององค์กร รวมทั้งการจัดทำแผนบริหารจัดการความเสี่ยง โดยกำหนดแนวทางการควบคุมเพื่อป้องกันหรือลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ ซึ่ง องค์การบริหารส่วนตำบลหินดาดมีขั้นตอนหรือกระบวนการบริหารจัดการความเสี่ยง ๖ ขั้นตอนหลักดังนี้

๑. ระบุความเสี่ยง เป็นการระบุเหตุการณ์ใดๆ ทั้งที่มีผลดีและผลเสียต่อการบรรลุวัตถุประสงค์ โดยต้องระบุได้ด้วยว่าเหตุการณ์นั้นจะเกิดที่ไหน เมื่อใด และเกิดขึ้นได้อย่างไร

๒. ประเมินความเสี่ยง เป็นการวิเคราะห์ความเสี่ยง และจัดลำดับความเสี่ยง โดยพิจารณาจากการประเมินโอกาสที่จะเกิดความเสี่ยง และความรุนแรงของผลกระทบจากเหตุการณ์ความเสี่ยง โดยอาศัยเกณฑ์มาตรฐานที่ได้กำหนดไว้ ทำให้การตัดสินใจจัดการกับความเสี่ยงเป็นไปอย่างเหมาะสม

๓. จัดการความเสี่ยง เป็นการกำหนดมาตรการ หรือแผนปฏิบัติการในการจัดการ และควบคุมความเสี่ยงที่สูง (High) และสูงมาก (Extreme) นั้นให้ลดลง ให้อยู่ในระดับที่ยอมรับได้ สามารถปฏิบัติได้จริง และควรต้องพิจารณาถึงความคุ้มค่าในด้านค่าใช้จ่ายและต้นทุนที่ต้องใช้ลงทุนในการกำหนดมาตรการหรือแผนปฏิบัติการนั้นกับประโยชน์ที่จะได้รับด้วย

๔. รายงานและติดตามผล เป็นการรายงานและติดตามผลการดำเนินงานตามแผนบริหารความเสี่ยงที่ได้ดำเนินการทั้งหมดตามลำดับให้ฝ่ายบริหารรับทราบและให้ความเห็นชอบดำเนินการตามแผนบริหารจัดการความเสี่ยง

๕. ประเมินผลการบริหารจัดการความเสี่ยง เป็นการประเมินการบริหารความเสี่ยงประจำปีเพื่อให้มั่นใจว่าองค์กรมีการบริหารความเสี่ยงเป็นไปอย่างเหมาะสม เพียงพอ ถูกต้อง และมีประสิทธิผลมาตรการหรือกลไกการควบคุมความเสี่ยง (Control Activity) ที่ดำเนินการสามารถลดและควบคุมความเสี่ยงที่เกิดขึ้นได้จริงและอยู่ในระดับที่ยอมรับได้ หรือต้องจัดทำมาตรการหรือตัวควบคุมอื่นเพิ่มเติม เพื่อให้ความเสี่ยงที่ยังเหลืออยู่หลังมีการจัดการ (Residual Risk) อยู่ในระดับที่ยอมรับได้ และให้องค์กรมีการบริหารความเสี่ยงอย่างต่อเนื่อง

๖. ทบทวนการบริหารจัดการความเสี่ยง เป็นการทบทวนประสิทธิภาพของแนวการบริหารความเสี่ยงในทุกขั้นตอน เพื่อพัฒนาระบบให้ดียิ่งขึ้น

๓.๓ ประเภทความเสี่ยง แบ่งเป็น ๔ ประเภท ได้แก่

๑) ความเสี่ยงเชิงยุทธศาสตร์ (Strategic Risk) หมายถึง ความเสี่ยงที่เกี่ยวข้องกับกลยุทธ์ เป้าหมาย พันธกิจ ในภาพรวมขององค์กร ที่อาจก่อให้เกิดการเปลี่ยนแปลงหรือการไม่บรรลุผลตามเป้าหมาย ในแต่ละประเด็นยุทธศาสตร์ขององค์กร

๒) ความเสี่ยงด้านการปฏิบัติงาน (Operational Risk) เป็นความเสี่ยงที่เกี่ยวข้องกับประเด็น ปัญหาการปฏิบัติงานประจำวัน หรือการดำเนินงานปกติที่องค์กรต้องเผชิญเพื่อให้บรรลุวัตถุประสงค์เชิงกลยุทธ์ ความเสี่ยงด้านนี้ อาทิ การปฏิบัติงานไม่เป็นไปตามแผนปฏิบัติงานโดยไม่มีผังการปฏิบัติงานที่ชัดเจน หรือไม่มีการมอบหมายอำนาจหน้าที่ความรับผิดชอบ บุคลากรขาดแรงจูงใจในการปฏิบัติงาน

๓) ความเสี่ยงด้านการเงิน (Financial Risk) เป็นความเสี่ยงที่เกี่ยวข้องกับการบริหารและควบคุมทางการเงินและการงบประมาณขององค์กรให้เป็นไปอย่างมีประสิทธิภาพ ผลกระทบการเงินที่เกิดจากปัจจัยภายนอก อาทิ ข้อบังคับเกี่ยวกับรายงานทางการเงินของหน่วยงานที่เกี่ยวข้อง ได้แก่ กรมบัญชีกลาง สำนักงานตรวจเงินแผ่นดิน สำนักงานประมาณ รวมทั้ง การจัดสรรงบประมาณไม่เหมาะสม

๔) ความเสี่ยงด้านการปฏิบัติตามกฎหมาย ระเบียบ ข้อบังคับ (Compliance Risk) เป็นความเสี่ยง ที่เกี่ยวข้องกับประเด็นข้อกฎหมาย ระเบียบ การปกป้องคุ้มครองผู้รับบริการหรือผู้มีส่วนได้เสียการ ป้องกันข้อมูลรวมถึงประเด็นทางด้านกฎระเบียบอื่นๆ

๓.๔ การประเมินความเสี่ยง

ในการประเมินระดับความรุนแรงของความเสี่ยง เป็นการวิเคราะห์เพื่อวัดระดับโอกาสหรือความถี่ที่จะเกิดความเสี่ยงและวัดระดับผลกระทบของความเสี่ยงนั้นๆ โดยนำเหตุการณ์ความเสี่ยง และปัจจัยเสี่ยงที่มีการค้นพบหรือระบุได้มาทำการวัดหรือประเมินระดับความรุนแรง กับความถี่หรือโอกาสที่จะเป็นไปได้ เพื่อระบุระดับความสำคัญของความเสี่ยง ซึ่งมีองค์ประกอบหลักในการพิจารณาอยู่ ๒ ประการคือโอกาส (Likelihood) ที่จะเกิดและผลกระทบ (Impact) ที่เกิดขึ้น โดยโอกาสที่จะเกิด คือความเป็นไปได้ที่จะเกิดเหตุการณ์นั้น ๆ ในช่วงเวลาหนึ่งและผลกระทบที่เกิดขึ้นคือความเสียหายที่เกิดขึ้น และมีผลกระทบต่อองค์กร หากเกิดเหตุการณ์ความเสี่ยง ทั้งนี้ จะต้องมีการกำหนดระดับของโอกาสที่จะเกิด และระดับของผลกระทบที่จะเกิด เพื่อให้สามารถกำหนดหรือจัดลำดับความสำคัญของความเสี่ยงได้

พิจารณาโอกาสในการเกิดความเสี่ยง จากสถิติการเกิดเหตุการณ์ในอดีต ปัจจุบัน หรือ การคาดการณ์ล่วงหน้าของโอกาสที่จะเกิดในอนาคต โดยจัดระดับของการเกิดความเสี่ยงเป็น ๕ ระดับ คือ สูงมาก สูง ปานกลาง น้อย และน้อยมาก แทนด้วยตัวเลข ๕ ๔ ๓ ๒ และ ๑ ตามลำดับ ใช้หลักเกณฑ์การวิเคราะห์โอกาสที่จะเกิดซึ่ง กำหนดเกณฑ์ไว้ ๕ ระดับ

หลักเกณฑ์การให้คะแนนโอกาสที่จะเกิดความเสี่ยงและความรุนแรงของผลกระทบ

๑. โอกาสที่จะเกิด (Likelihood : L) หมายถึง ความถี่หรือโอกาสที่จะเกิดเหตุการณ์ความเสี่ยงซึ่งจำแนก เป็น ๕ ระดับ คือ

การวิเคราะห์โอกาสที่จะเกิดปัจจัยเสี่ยงหรือสาเหตุของความเสี่ยง

| ระดับ | โอกาสที่จะเกิด | คำอธิบาย | |
|-------|----------------|--|---|
| | | โอกาสเกิดเชิงคุณภาพ | โอกาสเกิดเชิงปริมาณ (ความถี่ที่เกิดขึ้น) |
| ๕ | สูงมาก | มีโอกาสในการเกิดเกือบ ทุกครั้ง | มากกว่า ๘๐% หรือ มากกว่า ๑ ครั้ง/เดือน |
| ๔ | สูง | มีโอกาสในการเกิด ค่อนข้างสูงหรือบ่อยๆ | ๖๑-๘๐% หรือ ๑-๖ เดือน/ ครั้ง |
| ๓ | ปานกลาง | มีโอกาสเกิดบางครั้ง | ๔๑-๖๐% หรือ ๖-๑๒ เดือน/ ครั้ง |
| ๒ | ต่ำ | อาจมีโอกาสดังกล่าว ครั้ง | ๒๑-๔๐ % หรือ ๑ ปี / ครั้ง |
| ๑ | ต่ำมาก | มีโอกาสเกิดในกรณียกเว้น | น้อยกว่า ๒๐% หรือ มากกว่า ๕ ปี/ครั้ง |

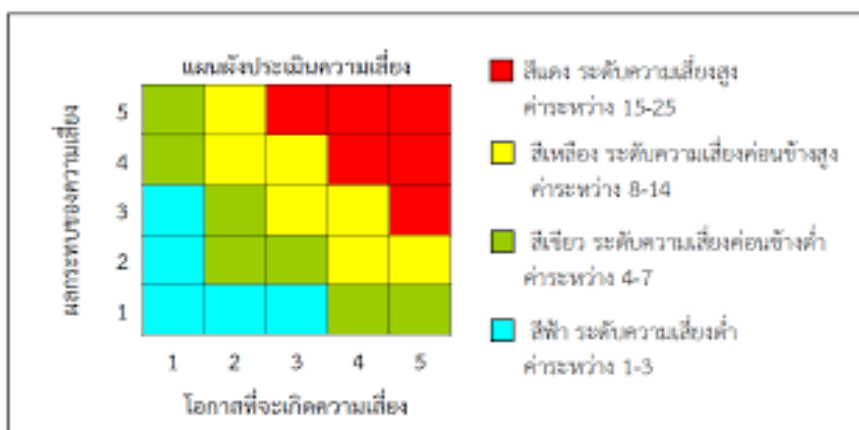
๒. ผลกระทบ (Impact : I) หมายถึง ขนาดความรุนแรงของความเสียหายที่จะเกิดขึ้นหากเกิดเหตุการณ์ความเสี่ยง จำแนก เป็น ๕ ระดับ คือ

พิจารณาความรุนแรงของผลกระทบที่เกิดจากความเสียหายหรือมูลค่าความเสียหายจากความเสียหายที่คาดว่าจะได้รับหากเกิดเหตุการณ์ความเสี่ยง การจัดระดับความรุนแรงของผลกระทบที่เกิดจากความเสียหาย เป็น ๕ ระดับ คือ สูงมาก สูง ปานกลาง ต่ำ และต่ำมาก แทนด้วยตัวเลข ๕ ๔ ๓ ๒ ๑ ตามลำดับ ซึ่งการกำหนดระดับของผลกระทบนั้น จะต้องพิจารณาถึงความเสียหาย หากความเสี่ยงนั้น เกิดขึ้นโดยอาจแบ่งผลกระทบออกเป็นผลกระทบด้านการเงิน/ทรัพย์สินการดำเนินงาน ชื่อเสียง/ภาพลักษณ์บุคลากร ฯลฯ เป็นต้นการวิเคราะห์ผลกระทบ ซึ่งกำหนดเกณฑ์ไว้ ๕ ระดับ

การวิเคราะห์ผลกระทบของปัจจัยเสี่ยงหรือสาเหตุของความเสี่ยง

| ระดับ | ผลกระทบ | คำอธิบาย |
|-------|---------|---|
| ๕ | สูงมาก | ส่งผลกระทบต่อประชาชน |
| ๔ | สูง | ส่งผลกระทบต่อองค์กรอื่นที่ ปฏิบัติงานร่วมกัน |
| ๓ | ปานกลาง | ส่งผลกระทบต่อ องค์กร. |
| ๒ | ต่ำ | ส่งผลกระทบต่อสำนัก/กอง |
| ๑ | ต่ำมาก | ส่งผลกระทบต่องานตนเอง |

๓. ระดับของความเสี่ยง (Degree of Risk) หมายถึงสถานะของความเสี่ยงที่ได้จากการประเมินโอกาสที่จะเกิดและผลกระทบของแต่ละปัจจัยเสี่ยงแบ่งเป็น ๕ ระดับ คือสูงมาก สูงปานกลาง ต่ำ และต่ำมาก ในรูปแบบของ แผนภูมิความเสี่ยง (Risk profile)



การประเมินโอกาสและผลกระทบของความเสี่ยง

เป็นการนำความเสี่ยงและปัจจัยเสี่ยงแต่ละปัจจัยที่ระบุไว้มาประเมินโอกาส (Likelihood) ที่จะเกิดเหตุการณ์ ความเสี่ยงต่างๆ และประเมินระดับความรุนแรงของผลกระทบหรือมูลค่าความเสียหาย (Impact) จาก ความเสี่ยง เพื่อให้เห็นถึงระดับของความเสี่ยงที่แตกต่างกัน ทำให้สามารถกำหนดการควบคุมความเสี่ยงได้อย่าง เหมาะสม ซึ่งจะช่วยให้สามารถวางแผนและจัดสรรทรัพยากรได้อย่างถูกต้องภายใต้งบประมาณ กำลังคนหรือ เวลาที่มีจำกัด โดยอาศัยเกณฑ์มาตรฐานที่กำหนดไว้ข้างต้น ซึ่งมีขั้นตอนดำเนินการ ดังนี้

๑) พิจารณาโอกาส ความถี่ ในการเกิดเหตุการณ์ต่างๆ (Likelihood) ว่ามีโอกาส ความถี่ที่จะเกิดขึ้น มากน้อยเพียงใด ตามเกณฑ์มาตรฐานที่กำหนด

๒) พิจารณาความรุนแรงของผลกระทบของความเสี่ยง (Impact) ที่มีผลต่อหน่วยงานว่ามีระดับความ รุนแรง หรือมีความเสียหายเพียงใด ตามเกณฑ์มาตรฐานที่กำหนด

การวิเคราะห์ความเสี่ยง
องค์การบริหารส่วนตำบลหินดาดได้พิจารณาโอกาสที่จะเกิดเหตุการณ์ (Likelihood) และระดับ ผลกระทบ (Impact) ของแต่ละปัจจัยแล้วนำผลที่ได้มาพิจารณา ความสัมพันธ์ระหว่างโอกาสที่จะเกิด ความเสี่ยงและผลกระทบว่าจะเกิดความเสี่ยงในระดับใด (ระดับความเสี่ยง = โอกาสที่จะเกิดเหตุการณ์ x ผลกระทบ ที่จะเกิดความเสียหาย) ซึ่งจัดแบ่งเป็น ๔ ระดับความเสี่ยง คือ

๑) ระดับความเสี่ยงต่ำ (Low) คะแนนระดับความเสี่ยง ๑-๒ คะแนน หมายถึง ระดับความเสี่ยง ที่ยอมรับได้ไม่ต้องควบคุมความเสี่ยง

๒) ระดับความเสี่ยงปานกลาง (Medium) คะแนนระดับความเสี่ยง ๓-๙ คะแนน หมายถึง ระดับ ความเสี่ยงที่ยอมรับได้ แต่ต้องมีการควบคุมเพื่อป้องกันมิให้ความเสี่ยงเพิ่ม มากขึ้นไปอยู่ในระดับ ที่ไม่สามารถ ยอมรับ

๓) ระดับความเสี่ยงสูง (high) คะแนนระดับความเสี่ยงเท่ากับ ๑๐-๑๕ คะแนน หมายถึง ระดับความ เสี่ยงที่ไม่สามารถยอมรับได้ โดยต้องจัดการความเสี่ยงเพื่อให้อยู่ในระดับที่ยอมรับได้

๔) ระดับความเสี่ยงสูงมาก (Extreme) คะแนนระดับความเสี่ยง ๑๖-๒๕ คะแนน หมายถึง ระดับความเสี่ยงที่ไม่สามารถยอมรับได้ จำเป็นต้องเร่งจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ทันที



ประเภทความเสี่ยง

Strategic Risk : S = ด้านกลยุทธ์

Operational Risk : O = ด้านการดำเนินงาน

Financial Risk : F = ด้านการเงิน

Compliance Risk : C = ด้านกฎหมาย/กฎระเบียบ

การควบคุม (Control) หมายถึง นโยบายแนวทาง หรือขั้นตอนปฏิบัติต่างๆ ซึ่งกระทำเพื่อลดความเสี่ยง และทำให้การดำเนินงานบรรลุวัตถุประสงค์ มีดังนี้

๑. การควบคุมเพื่อการป้องกัน (Preventive Control) เป็นวิธีการควบคุมที่กำหนดขึ้นเพื่อป้องกันไม่ให้เกิดความเสี่ยงและข้อผิดพลาดตั้งแต่แรก เช่น การอนุมัติ การจัดโครงสร้างองค์กร การแบ่งแยกหน้าที่ การควบคุมการเข้าถึงเอกสาร ข้อมูล ทรัพย์สิน เป็นต้น

๒. การควบคุมเพื่อให้ตรวจพบ (Detective Control) เป็นวิธีการควบคุมที่กำหนดขึ้นเพื่อค้นพบข้อผิดพลาดที่เกิดขึ้นแล้ว เช่น การสอบทาน การวิเคราะห์ การยืนยันยอดการตรวจนับ การรายงานข้อบกพร่อง เป็นต้น

๓. การควบคุมโดยการชี้แนะ (Directive Control) เป็นวิธีการควบคุมที่ส่งเสริมหรือกระตุ้นให้เกิดความสำเร็จตามวัตถุประสงค์ที่ต้องการ เช่น การให้รางวัล แก่ผู้มีผลงานดี การประกาศเกียรติคุณ เป็นต้น

๔. การควบคุมเพื่อการแก้ไข (Corrective Control) เป็นวิธีการควบคุมที่กำหนดขึ้นเพื่อแก้ไขข้อผิดพลาดที่เกิดขึ้นให้ถูกต้อง หรือเพื่อหาวิธีการแก้ไขไม่ให้เกิดข้อผิดพลาดซ้ำอีกในอนาคต

การจัดการความเสี่ยง

แนวทางการบริหารจัดการความเสี่ยงมีหลายวิธี และสามารถปรับเปลี่ยนให้เหมาะสมกับสถานการณ์ขึ้นอยู่กับดุลยพินิจของคณะกรรมการจัดทำแผนบริหารความเสี่ยง แต่อย่างไรก็ตามแนวทาง การบริหารจัดการความเสี่ยงนั้น ต้องคำนึงถึงการลดระดับผลกระทบของความเสี่ยงทางเลือกหรือยุทธศาสตร์

ในการจัดการความเสี่ยง โดยองค์การบริหารส่วนตำบลหินดาด มีวิธีการบริหาร/จัดการเสี่ยง ๔ แนวคิดหลัก (๔T's) ซึ่งมีรายละเอียด ดังต่อไปนี้

| วิธีการบริหาร/จัดการความเสี่ยง | ศัพท์ที่นิยมใช้ทั่วไป (กรมบัญชีกลาง) | แนวคิด ๔T |
|---|--------------------------------------|-----------|
| ๑.การยอมรับความเสี่ยง หมายถึง การตกลงกันที่จะยอมรับ เนื่องจากไม่คุ้มค่าในการจัดการหรือป้องกันแต่การเลือกบริหารความเสี่ยงด้วยวิธีนี้ ต้องมีการติดตามเฝ้าระวังอย่างสม่ำเสมอ | Risk Acceptance (Accept) | Take |
| ๒.การลด/การควบคุมความเสี่ยง หมายถึง การปรับปรุงระบบการทำงาน หรือออกแบบวิธีการทำงานใหม่ เพื่อลดโอกาสที่จะเกิดความเสียหาย หรือลดผลกระทบที่อาจจะเกิดขึ้นจากความเสี่ยง ให้อยู่ในระดับที่ยอมรับได้ เช่น การจัดอบรมพนักงาน การจัดทำคู่มือ การปฏิบัติงาน | Risk Reduction (Control) | Treat |
| ๓. กระจายความเสี่ยง หรือโอนความเสี่ยง หมายถึง กระจายหรือถ่ายโอนความเสี่ยงให้หน่วยงานอื่นช่วยแบ่งความรับผิดชอบไป เช่น การทำประกันภัยกับบริษัทภายนอก หรือการจ้างบุคคลภายนอก ดำเนินการแทน (Outsource) | Risk Sharing (Transfer) | Transfer |
| ๔.การหลีกเลี่ยงความเสี่ยง หมายถึง การจัดการกับความเสี่ยงที่อยู่ในระดับสูงมาก และไม่อาจยอมรับได้ จึงตัดสินใจยกเลิกโครงการ/กิจกรรมที่จะก่อให้เกิดความเสี่ยงนั้นไป | Risk Ad voidance (Ad void) | Terminate |

การรายงานและติดตามผล

หลังจากจัดทำแผนบริหารความเสี่ยงและมีการดำเนินงานตามแผนแล้ว จะต้องมีการรายงานและติดตามผลเป็นระยะ เพื่อให้เกิดความมั่นใจว่าได้มีการดำเนินงานไปอย่างถูกต้องและเหมาะสม โดยมีเป้าหมายในการติดตามผล คือ เป็นการประเมินคุณภาพและความเหมาะสมของวิธีการจัดการความเสี่ยง รวมทั้งติดตามผลการจัดการความเสี่ยงที่ได้มีการดำเนินการไปแล้วว่าบรรลุผลตามวัตถุประสงค์ของการบริหารความเสี่ยงหรือไม่ โดยหน่วยงานต้องสอบถามดูว่า วิธีการบริหารจัดการความเสี่ยงได้มีประสิทธิภาพดีก็ให้ดำเนินการต่อไป หรือวิธีการบริหารจัดการความเสี่ยงใดควรปรับเปลี่ยน และนำผลการติดตามไปรายงานให้ฝ่ายบริหารทราบตามแบบรายงานที่ได้กล่าวไว้ข้างต้น ทั้งนี้กระบวนการสอบถามอาจกำหนดข้อมูลที่ต้องติดตาม หรืออาจทำ Check List การติดตาม พร้อมทั้งกำหนดความถี่ในการติดตามผล โดยสามารถติดตามผลได้ใน ๒ ลักษณะ คือ

- ๑) การติดตามผลเป็นรายครั้ง (Separate Monitoring) เป็นการติดตาม ตามรอบระยะเวลาที่กำหนด เช่น ทุก ๓ เดือน ๖ เดือน ๙ เดือน หรือทุกสิ้นปี เป็นต้น
- ๒) การติดตามผลในระหว่างการปฏิบัติงาน (Ongoing Monitoring) เป็นการติดตามที่ รวมอยู่ในการดำเนินงานต่างๆ ตามปกติของหน่วยงาน

การประเมินผลการบริหารความเสี่ยง

คณะทำงานบริหารความเสี่ยง จะต้องทำสรุปรายงานผลและประเมินผลการบริหารความเสี่ยงประจำปีต่อผู้บริหารท้องถิ่น เพื่อให้มั่นใจว่าองค์กรบริหารส่วนตำบลห็นาดามีการบริหารความเสี่ยงเป็นไปอย่างเหมาะสมเพียงพอ ถูกต้อง และมีประสิทธิผล มาตรการหรือกลไกควบคุมความเสี่ยงที่ดำเนินการ สามารถลดและควบคุมความเสี่ยงที่เกิดขึ้นได้จริงและอยู่ในระดับที่ยอมรับได้ หรือต้องจัดทำมาตรการหรือตัวควบคุมอื่นเพิ่มเติม เพื่อให้ความเสี่ยงที่ยังเหลืออยู่หลังมีการจัดการอยู่ในระดับที่ยอมรับได้ และให้องค์กรมีการบริหารความเสี่ยงอย่างต่อเนื่องจนเป็นวัฒนธรรมในการดำเนินงาน

การทบทวนการบริหารความเสี่ยง

การทบทวนแผนบริหารความเสี่ยง เป็นการทบทวนประสิทธิภาพของแนวการบริหาร ความเสี่ยงในทุกชั้นตอน เพื่อการปรับปรุงและพัฒนาแผนงานในการบริหารความเสี่ยงให้ทันสมัยและเหมาะสมกับการปฏิบัติงานจริงเป็นประจำทุกปี