บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)
National Telecom Public Company Limited

ประกาศ บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)

เรื่อง นโยบายการกำกับดูแลกิจการที่ดี การบริหารความเสี่ยงและการควบคุมภายใน และการปฏิบัติตามกฎระเบียบของบริษัท โทรคมนาคม แห่งชาติ จำกัด (มหาชน) (Governance Risk and Control Management and Compliance Policy : GRC Policy) บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)

คณะกรรมการบริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) ตระหนักถึงความสำคัญของการบูรณาการด้านการกำกับดูแลกิจการที่ดี การบริหารความเสี่ยงและการควบคุมภายใน และการปฏิบัติตามกฎระเบียบ (Governance Risk and Compliance : GRC) จึงอาศัยอำนาจตามความในข้อ 13 ของข้อบังคับบริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) ยกเลิกประกาศ นโยบายการบริหารความเสี่ยงและการควบคุมภายใน ฉบับลงวันที่ 28 เมษายน 2565 และนโยบายการกำกับดูแลกิจการที่ดี การบริหารความเสี่ยงและการควบคุมภายใน และการปฏิบัติตามกฎระเบียบ (Governance Risk and Control Management and Compliance Policy : GRC Policy) ฉบับลงวันที่ 13 ธันวาคม 2565 และให้ใช้ประกาศฉบับนี้แทน

เพื่อสร้างสรรค์คุณค่าให้บริษัท (Value Creation) จากความสมดุลระหว่าง การมุ่งสู่องค์กรแห่งความเป็นเลิศ (Business Excellence) กับการดำเนินธุรกิจอย่างมีจริยธรรม (Business Ethics) ภายใต้ระบบบูรณาการ (Integrity) การกำกับดูแลกิจการที่ดี การบริหารความเสี่ยงและการควบคุมภายใน และการกำกับการปฏิบัติตามกฎเกณฑ์ (GRC System) สอดคล้องตามแนวทางของ Open Compliance and Ethics Group (OCEG) บนพื้นฐานการดำเนินการที่เกี่ยวข้องกับบุคลากร (People) กระบวนการ (Process) เทคโนโลยี (Technology) และข้อมูลสารสนเทศ (Information) ซึ่งมีการแบ่งปัน (Resource Sharing) และแลกเปลี่ยนความรู้ (Knowledge Exchange) สนับสนุนการดำเนินงาน ข้ามสายงาน (Cross Functional) อย่างเป็นระบบ โดยคำนึงถึงการมีความเสี่ยงอยู่ในระดับที่ยอมรับได้ (Risk Appetite) ให้การกำกับดูแลกิจการที่ดี การบริหารความเสี่ยงและการควบคุมภายใน และการปฏิบัติตามกฎระเบียบของบริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) เป็นไปตามกรอบและแนวทางปฏิบัติ ดังนี้

1. วัตถุประสงค์

1.1 เพื่อสนับสนุนการดำเนินงานให้บรรลุวัตถุประสงค์เชิงยุทธศาสตร์ (Strategic Objectives : SO) ด้วยความรับผิดชอบต่อผู้มีส่วนได้ส่วนเสีย ตามหลักการกำกับดูแลกิจการที่ดี ปฏิบัติตามกฎหมาย ระเบียบ ข้อบังคับ จริยธรรม และจรรยาบรรณ มุ่งมั่นในการต่อต้านการทุจริตคอร์รัปชันทุกรูปแบบ มีระบบการตรวจสอบ การบริหารความเสี่ยงและการควบคุมภายใน ที่มีการแจ้งเตือนภัยล่วงหน้าอย่างเป็นระบบ (Early Warning System) เปิดเผย

ข้อมูลสารสนเทศด้านการเงินและไม่ใช่การเงิน อย่างโปร่งใส ถูกต้อง ทันกาล และตรวจสอบได้ โดยมีคณะกรรมการบริษัทและผู้บริหารเป็นแบบอย่างที่ดี (Role Model) แก่พนักงาน

1.2 กำหนดกรอบการปฏิบัติงานในกระบวนการบริหารความเสี่ยงและการควบคุมภายในที่ชัดเจน เป็นลายลักษณ์อักษร และให้นำไปปฏิบัติทั่วทั้งบริษัท (รายละเอียดตามเอกสารแนบ 1 และเอกสารแนบ 2)

1.3 เพื่อให้การดำเนินการในการบริหารความเสี่ยงและการควบคุมภายในเป็นไปตามหลักเกณฑ์กระทรวงการคลัง ว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ พ.ศ. 2562 และมาตรฐานและหลักเกณฑ์ปฏิบัติการควบคุมภายในสำหรับหน่วยงานของรัฐ พ.ศ. 2561 และมีการทบทวนเพื่อปรับปรุงอย่างต่อเนื่องตามระบบการประเมินผลการดำเนินงานรัฐวิสาหกิจ ตามระบบประเมินผลรัฐวิสาหกิจ State Enterprise Assessment Model : SE-AM

1.4 กำหนดโครงสร้าง และบทบาทหน้าที่ความรับผิดชอบในการกำกับดูแล บริหารจัดการความเสี่ยงและควบคุมภายในอย่างชัดเจนและเหมาะสม พร้อมทั้งการกำกับ ติดตาม ประเมิน และรายงานผลตามเวลาที่กำหนด

2. โครงสร้างและบทบาทหน้าที่

2.1 คณะกรรมการ บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)

2.1.1 ทำหน้าที่ในการอนุมัติ GRC Policy และในฐานะผู้นำที่สร้างคุณค่าให้แก่บริษัทอย่างยั่งยืน โดยกำกับดูแลการนำกลยุทธ์ไปสู่การปฏิบัติ พร้อมมอบข้อสังเกตและข้อเสนอแนะเพื่อให้มั่นใจได้ว่าบริษัทจะสามารถดำเนินงานให้บรรลุผลสำเร็จตามกลยุทธ์ที่กำหนดไว้ รวมทั้งสามารถเชื่อมโยงและประสานงานที่เกี่ยวข้องกับการกำกับดูแลกิจการ (Governance) การบริหารความเสี่ยง (Risk Management) และการปฏิบัติตามกฎระเบียบ (Compliance) ให้ร้อยเรียงเป็น "ภาพเดียวกัน" ภายใต้วัฒนธรรมบริษัทที่มีจริยธรรม โปร่งใส และซื่อสัตย์ ซึ่งรวมเรียกว่าการบูรณาการ Governance, Risk and Compliance หรือ GRC

2.1.2 รับทราบแผนการบริหารความเสี่ยงและการควบคุมภายใน กำกับดูแลให้มีการบริหารความเสี่ยงและควบคุมภายในอย่างเหมาะสมและสม่ำเสมอทั่วทั้งบริษัท ผ่านคณะกรรมการบริหารความเสี่ยงและควบคุมภายใน

2.1.3 สร้างบรรยากาศและวัฒนธรรมที่สนับสนุนการบริหารความเสี่ยงและการควบคุมภายใน ให้ได้รับการปฏิบัติทั่วทั้งองค์กร

2.1.4 ส่งเสริมให้พนักงานทุกระดับชั้นตระหนักถึงความเสี่ยงที่มีในการปฏิบัติงานของหน่วยงานตนและบริษัทให้มีการบริหารจัดการความเสี่ยงและการควบคุมภายในอย่างเป็นระบบในระดับที่เพียงพอและเหมาะสม

2.2 คณะกรรมการบริหารความเสี่ยงและควบคุมภายใน

2.2.1 ทำหน้าที่เสนอ (ร่าง) GRC Policy ต่อคณะกรรมการบริษัท เพื่อพิจารณาอนุมัติ และกำกับดูแล ติดตามผลการดำเนินงานตาม GRC Policy ทุกไตรมาส ผลักดันการบูรณาการระหว่างแผนแม่บทสำคัญต่าง ๆ กับแผนบริหารความเสี่ยง ด้วยการสนับสนุนการติดตาม เฝ้าระวัง (Watchlist) ภัยคุกคามและอุบัติภัยใหม่ ๆ จากการใช้ข้อมูลความเสี่ยงด้านกำกับดูแลกิจการ การดำเนินธุรกิจ และการกำกับกฎหมาย กฎระเบียบ (GRC Risk) อย่างมีประสิทธิภาพและประสิทธิผล รวมถึง สื่อสารและประชาสัมพันธ์ GRC Policy ผ่านช่องทางต่าง ๆ ทั้งภายในและภายนอกบริษัท เพื่อสร้างความมั่นใจแก่ผู้มีส่วนได้ส่วนเสีย (Stakeholders)

2.2.2 อนุมัติแผนการจัดการบริหารความเสี่ยงและแผนการควบคุมภายในของบริษัท และนำเสนอคณะกรรมการ บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) เพื่อทราบ

2.2.3 กำกับดูแลการบริหารความเสี่ยงและการควบคุมภายในของ บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)

2.2.4 พิจารณาให้การสนับสนุนการดำเนินการแก่หน่วยงานที่รับผิดชอบเพื่อประสิทธิภาพและประสิทธิผลในการบริหารความเสี่ยงและการควบคุมภายใน

2.2.5 ติดตามและรายงานผลการดำเนินการบริหารความเสี่ยงและการควบคุมภายใน ต่อคณะกรรมการบริษัทเป็นรายไตรมาส หรือเมื่อมีกรณีสำคัญที่เห็นควรรายงานต่อคณะกรรมการบริษัท

2.3 คณะกรรมการกำกับดูแลกิจการที่ดีและพัฒนาองค์กรอย่างยั่งยืน

ทำหน้าที่กำหนดหลักการกำกับดูแลกิจการที่ดีของบริษัท ให้มีนโยบายเป้าหมายด้านการกำกับดูแลกิจการที่ดีที่ชัดเจน กำกับดูแลการดำเนินกิจการของบริษัท และการปฏิบัติงานของคณะกรรมการบริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) คณะกรรมการเฉพาะเรื่องชุดต่าง ๆ รวมถึงผู้บริหารและพนักงานให้เป็นไปตามหลักการกำกับดูแลกิจการที่ดี กำหนดแนวทางและวางนโยบายการดำเนินธุรกิจของบริษัท ให้มีความรับผิดชอบต่อสังคมและเหมาะสมกับธุรกิจของบริษัท สอดคล้องกับหลักการกำกับดูแลกิจการที่เป็นมาตรฐานสากล และรายงานผลการดำเนินการต่อคณะกรรมการบริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) เป็นรายไตรมาส หรือเมื่อมีกรณีสำคัญที่เห็นควรรายงาน

2.4 คณะกรรมการตรวจสอบ

2.4.1 ทำหน้าที่สนับสนุนต่อการดำเนินงานของคณะกรรมการบริษัทโทรคมนาคมแห่งชาติ จำกัด (มหาชน) โดยเสนอผลสอบทานและข้อเสนอแนะต่อการดำเนินงานด้านการกำกับดูแลกิจการที่ดี การบริหารความเสี่ยงและการควบคุมภายใน และการปฏิบัติตามกฎ ระเบียบ ของหน่วยงานต่าง ๆ โดยอิสระ เพื่อให้มั่นใจว่าการบริหารจัดการในงานที่สำคัญขององค์กรมีความเหมาะสมและมีประสิทธิผล

2.4.2 ทำหน้าที่สนับสนุนคณะกรรมการบริษัท ด้านการบริหารความเสี่ยงและการควบคุมภายใน โดยสอบทานประสิทธิภาพและประสิทธิผลของกระบวนการควบคุมภายใน และกระบวนการบริหารความเสี่ยง

2.5 ผู้บริหารระดับสูง (กรรมการผู้จัดการใหญ่/รองกรรมการผู้จัดการใหญ่/ผู้ช่วยกรรมการผู้จัดการใหญ่)

2.5.1 ทำหน้าที่ในการนำนโยบายการบูรณาการ GRC ไปปฏิบัติและกำกับดูแล ติดตามและรายงานผลการนำไปใช้อย่างต่อเนื่อง โดยได้รับการสนับสนุนจากคณะกรรมการบริหารความเสี่ยงและควบคุมภายในตลอดจนสร้างวัฒนธรรมที่สนับสนุนการกำกับดูแลกิจการที่ดี การบริหารความเสี่ยงและการควบคุมภายใน และการปฏิบัติตามกฎระเบียบ

2.5.2 พิจารณาให้ความเห็นชอบแผนการจัดการบริหารความเสี่ยงและแผนการควบคุมภายในประจำปีก่อนนำเสนอคณะกรรมการบริหารความเสี่ยงและควบคุมภายในอนุมัติ

2.5.3 เป็นเจ้าของความเสี่ยงระดับองค์กรซึ่งมีหน้าที่รับผิดชอบในการระบุ และประเมินความเสี่ยงองค์กร รวมทั้งกำหนดมาตรการที่เหมาะสม เพื่อจัดการความเสี่ยง และถ่ายทอดความเสี่ยงที่เหลืออยู่ลงในระดับสายงานและระดับหน่วยงาน เพื่อให้หน่วยงานภายใต้นำไปพิจารณาปรับปรุงการควบคุมภายในให้สอดคล้องกับหน้าที่ความรับผิดชอบ

2.5.4 จัดให้มีบรรยากาศและวัฒนธรรมที่สนับสนุนการบริหารความเสี่ยงและการควบคุมภายใน เช่น จรรยาบรรณ การสื่อสารสองทางที่มีประสิทธิภาพ ความรับผิดชอบ และการรับฟังการท้วงติงถึงความเสี่ยง

2.6 ผู้บริหารและพนักงานทุกคน

2.6.1 มีหน้าที่ในการปฏิบัติตาม GRC Policy อย่างเคร่งครัด และร่วมสร้างวัฒนธรรมในการทำงาน ที่สอดคล้องกับค่านิยมองค์กร และเป็นไปตาม GRC Policy

2.6.2 รับผิดชอบในการปฏิบัติตามคู่มือบริหารความเสี่ยงและการควบคุมภายใน

2.6.3 เป็นเจ้าของความเสี่ยง ซึ่งมีหน้าที่รับผิดชอบในการระบุ และประเมินความเสี่ยงของหน่วยงานที่ตนเองรับผิดชอบ รวมทั้งกำหนดมาตรการที่เหมาะสม เพื่อจัดการความเสี่ยง/ปรับปรุงการควบคุมภายใน

2.7 หน่วยงานที่ทำหน้าที่สนับสนุนให้เกิดการบูรณาการ GRC ได้อย่างเป็นรูปธรรมและมีแนวทางในการปฏิบัติที่ชัดเจน ได้แก่ หน่วยงานด้านการกำกับดูแลที่ดี กลยุทธ์ การบริหารความเสี่ยง การตรวจสอบภายใน การกำกับกฎหมายและกฎระเบียบขององค์กร จริยธรรมและวัฒนธรรม เทคโนโลยีสารสนเทศและความปลอดภัย โดยนำเทคโนโลยีสารสนเทศมาใช้ในการบูรณาการข้อมูลของกระบวนการ ด้วยการคำนึงถึงความเสี่ยงด้านเทคโนโลยีสารสนเทศ และความคุ้มค่าของการใช้เทคโนโลยีในกระบวนการปฏิบัติงานอย่างเหมาะสม

2.8 คณะกรรมการบริหาร ช่วยสนับสนุนคณะกรรมการบริษัท ด้านการบริหารความเสี่ยง โดยเสนอแนะแนวทางกำกับดูแลการดำเนินธุรกิจของ บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) ให้เป็นไปตามนโยบายด้านยุทธศาสตร์ แผนแม่บท และแผนงานต่าง ๆ ที่เกี่ยวข้อง

2.9 คณะกรรมการประเมินผลการควบคุมภายใน มีหน้าที่ อำนวยการในการประเมินผลการควบคุมภายในกำหนดแนวทางการประเมินผลการควบคุมภายใน รวบรวม พิจารณากลั่นกรอง และสรุปผลการประเมินการควบคุมภายในในภาพรวม ประสานงานการประเมินผลการควบคุมภายในกับหน่วยงานในสังกัดที่เกี่ยวข้อง จัดทำรายงานการประเมินผลการควบคุมภายในระดับองค์กร

2.10 คณะกรรมการและคณะทำงานการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management) มีหน้าที่ กำหนดนโยบายการบริหารความต่อเนื่องทางธุรกิจ กำกับดูแลและบัญชาการให้ปฏิบัติตามแผนบริหารความต่อเนื่องทางธุรกิจของ บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) เมื่อเกิดสถานการณ์ฉุกเฉิน และภัยคุกคามต่าง ๆ รวมทั้งรายงานผลเป็นกรณีพิเศษ โดยเร็ว ต่อคณะกรรมการบริหารความเสี่ยงและควบคุมภายในก่อนนำเสนอคณะกรรมการบริษัท เพื่อทราบต่อไป

2.11 คณะทำงานบริหารความเสี่ยงและควบคุมภายในประจำสายงาน มีหน้าที่ ผลักดัน และประสานงานให้มีการประเมินความเสี่ยง กำหนดแนวทางในการบริหารความเสี่ยงและการควบคุมภายในของสายงาน และส่วนงานภายใต้สังกัด รวมถึงการจัดทำแผนจัดการความเสี่ยงระดับสายงาน การประเมินและทบทวนการควบคุมภายในรวมทั้งการรายงานผลการจัดการความเสี่ยง เป็นประจำทุกเดือน และรายงานผลตามแผนการควบคุมภายใน เป็นประจำทุกไตรมาส

3. การบูรณาการ

บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) นำหลักการและแนวคิด GRC ช่วยขับเคลื่อนองค์กร ดังนี้

3.1 กำหนดวัตถุประสงค์ทางธุรกิจ เพื่อให้สอดคล้องกับมูลค่าและความเสี่ยงที่เกี่ยวข้อง

3.2 บรรลุวัตถุประสงค์ตามเป้าหมายที่กำหนด และสามารถเพิ่มประสิทธิภาพในการเฝ้าระวัง ความเสี่ยง (Risk Profile) และปกป้องคุณค่าขององค์กร (Value)

3.3 ดำเนินการภายใต้ขอบเขตของกฎหมาย สัญญา ระบบภายในสังคม และจริยธรรม

3.4 ให้ข้อมูลที่เกี่ยวข้อง เชื่อถือได้ และทันเวลา ต่อผู้มีส่วนได้เสีย

3.5 ส่งเสริมการวัดผลของระบบการดำเนินงานและการมีประสิทธิผล

(รายละเอียดตามเอกสารแนบ 3)

4. การทบทวน GRC Policy

สายงานกลยุทธ์ติดตามการปฏิบัติตามนโยบาย รวบรวมข้อมูลป้อนกลับ ปัญหา/อุปสรรค ข้อมูลบริบทองค์กรมาใช้ในการวิเคราะห์ประสิทธิผล เพื่อทบทวนและปรับปรุงนโยบายให้เหมาะสมกับสภาพแวดล้อมการดำเนินการขององค์กรที่อาจเปลี่ยนแปลงไป หรืออย่างน้อยปีละ 1 ครั้ง

ประกาศ ณ วันที่ 17 พฤศจิกายน 2566

(นายอำนวย ปรีมนวงศ์)
รองประธานกรรมการ บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)

แนวทางการบริหารความเสี่ยงและการควบคุมภายใน (Risk Management and Internal Control Policy)

1. จัดวางระบบและกระบวนการบริหารความเสี่ยงตามกรอบการบริหารความเสี่ยงตามแนวทาง COSO – ERM 2017 (Enterprise Risk Management-Integrating with Strategy and Performance) สอดคล้องกับระบบการประเมินผลการดำเนินงานรัฐวิสาหกิจ ตามระบบประเมินผลรัฐวิสาหกิจ State Enterprise Assessment Model : SE-AM และหลักเกณฑ์กระทรวงการคลัง ว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ พ.ศ. 2562

2. จัดวางระบบการควบคุมภายในอย่างเพียงพอ เหมาะสม และเป็นส่วนหนึ่งของการปฏิบัติงานอย่างเป็นขั้นตอนและต่อเนื่อง ตามแนวทาง COSO 2013 (Internal Control – Integrated Framework) สอดคล้องกับระบบการประเมินผลการดำเนินงานรัฐวิสาหกิจ ตามระบบประเมินผลรัฐวิสาหกิจ State Enterprise Assessment Model : SE-AM และหลักเกณฑ์กระทรวงการคลัง ว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการควบคุมภายในสำหรับหน่วยงานของรัฐ พ.ศ. 2561

3. การบริหารความเสี่ยงและการควบคุมภายใน เป็นองค์ประกอบสำคัญของทุกกระบวนการดำเนินงาน จึงถือเป็นหน้าที่ของผู้บริหารและพนักงานทุกคน ในการบริหารจัดการความเสี่ยงของหน่วยงานตนเองและดำเนินการตามกิจกรรมการควบคุมภายในที่เพียงพอ เหมาะสม และบริหารจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้

4. ความเสี่ยงที่กระทบต่อเป้าหมายขององค์กร GRC Policy และตัวชี้วัดองค์กร รวมถึงความเสี่ยงที่เกี่ยวข้องกับการตัดสินใจทางธุรกิจที่สำคัญ แผนธุรกิจ แผนปฏิบัติงานต่าง ๆ จะต้องมีการจัดการ ดังนี้

(1) ระบุความเสี่ยงให้ครอบคลุมทั้งปัจจัยภายใน และภายนอก รวมทั้งภาวะวิกฤตต่าง ๆ ที่อาจเกิดขึ้น

(2) ประเมินระดับความเสี่ยงที่อาจจะเกิดขึ้น โดยพิจารณาจากผลกระทบของความเสี่ยง และโอกาสที่จะเกิดความเสี่ยงนั้น ๆ

(3) เลือกวิธีการตอบสนองต่อความเสี่ยง ให้สอดคล้องตามหลักเกณฑ์การบริหารความเสี่ยงที่กำหนด * และระดับความเสี่ยงที่ยอมรับได้ เพื่อกำหนดการจัดการที่พิจารณาจากต้นทุนและผลประโยชน์ที่ได้รับอย่างเหมาะสม

(4) กำหนดระดับความเสี่ยงที่ยอมรับได้ โดยคำนึงถึงตัวชี้วัดที่ สคร. กำหนด เป้าหมายตามยุทธศาสตร์กำหนดที่ผ่านความเห็นชอบจากคณะกรรมการ บมจ. โทรคมนาคมแห่งชาติ โดยแยกตามวัตถุประสงค์ของการบริหารความเสี่ยง ดังนี้

- ด้านกลยุทธ์
  - ตัวชี้วัดที่ สคร. กำหนด ต้องได้ ตามเป้าหมายที่ตกลงกับ สคร.
  - ตัวชี้วัดค่าเป้าหมายตามที่กำหนดในแผนวิสาหกิจ ต้องได้ตามที่กำหนดในแผนวิสาหกิจ
- ด้านการปฏิบัติงาน
  - ตัวชี้วัดที่นอกเหนือจากแผนวิสาหกิจ ยอมรับค่าเบี่ยงเบนจากเป้าหมายได้ไม่เกิน 10%
- ด้านการรายงานผล และการเงิน
  - ตัวชี้วัดที่นอกเหนือจากแผนวิสาหกิจ ยอมรับค่าเบี่ยงเบนจากเป้าหมายได้ไม่เกิน 10%
- ด้านการปฏิบัติตามกฎระเบียบ
  - ต้องไม่เกิดรายการทุจริต
- ด้านภาพลักษณ์ชื่อเสียง
  - ยอมรับความเสี่ยงจากการเสนอข่าวเรื่องเดียวกันผ่านสื่อต่าง ๆ ติดต่อกันไม่เกิน 3 วัน

• ด้านเทคโนโลยีดิจิทัล

- ยอมรับความเสี่ยงในเรื่องความมั่นคงปลอดภัยของสารสนเทศและระบบงานภายใต้มาตรการการรักษาความลับของข้อมูล (Confidentiality) ความถูกต้องสมบูรณ์ (integrity) และความพร้อมใช้งาน (Availability)

• ด้านความต่อเนื่องในการดำเนินธุรกิจ

- ยอมรับให้เกิดความล่าช้า/ความต่อเนื่องในการดำเนินธุรกิจ ในระดับที่ไม่หยุดชะงักเป็นเวลานาน (ตามมาตรฐานคุณภาพบริการ) จนก่อให้เกิดความเสียหายที่เป็นผลกระทบต่อชื่อเสียง และความเชื่อมั่นต่อการให้บริการที่เป็นสาระสำคัญ

(5) กำกับดูแล ติดตาม ประเมินผล และปรับปรุงกระบวนการบริหารความเสี่ยงและการควบคุมภายในอย่างต่อเนื่อง

5. การบริหารความเสี่ยงและการรายงานผลในภาวะปกติและภาวะพิเศษ

(1) การบริหารความเสี่ยงในภาวะปกติ มุ่งเน้นการดำเนินการตาม GRC Policy เพิ่มประสิทธิภาพ และประสิทธิผลในการบริหารจัดการความเสี่ยงให้บรรลุเป้าหมายและวัตถุประสงค์ขององค์กร โดยการระบุและค้นหาสาเหตุของปัจจัยเสี่ยง ประเมิน และจัดลำดับความสำคัญ เลือกวิธีการ พร้อมกำหนดแผนจัดการความเสี่ยง มีการติดตาม ประเมินผลพร้อมทั้งรายงานผลการดำเนินงานต่อผู้บริหารระดับสูง คณะกรรมการบริหารความเสี่ยงและควบคุมภายใน และคณะกรรมการบริษัท เป็นระยะ ๆ อย่างน้อยเป็นรายไตรมาส เพื่อรับฟังข้อพิจารณา และนำไปปรับปรุงแก้ไขได้ทันเวลา และต้องรายงานการดำเนินการตามมติ หากเป็นกรณีที่มีระดับความเสี่ยงที่สูงมาก

(2) การบริหารความเสี่ยงในภาวะพิเศษ

- การกำหนดกระบวนการบริหารความต่อเนื่องทางธุรกิจอย่างเป็นระบบ ที่เชื่อมโยงเป้าหมายและยุทธศาสตร์องค์กร โดยให้มีการจัดทำแผนบริหารความต่อเนื่องทางธุรกิจ เพื่อรองรับภาวะวิกฤติต่าง ๆ ที่อาจก่อให้เกิดการหยุดชะงักของกระบวนการสำคัญในการดำเนินธุรกิจโดยเฉพาะด้านดิจิทัล รวมทั้งแสวงหาโอกาสทางธุรกิจในภาวะพิเศษ (หากมี) และให้รายงานเป็นกรณีพิเศษโดยเร็ว ซึ่งการบริหารจัดการความเสี่ยงในภาวะพิเศษสามารถดำเนินการผ่านคณะกรรมการและคณะทำงานการบริหารความต่อเนื่องทางธุรกิจ และรายงานต่อคณะกรรมการบริหารความเสี่ยงและควบคุมภายในก่อนนำเสนอคณะกรรมการบริษัท เพื่อทราบต่อไป

- การกำหนดแผนการประชุมในภาวะปกติจะมีอย่างน้อย 4 ครั้งต่อปี หากมีวาระเร่งด่วนจะจัดให้มีการประชุมนอกเหนือจากแผนประชุมที่กำหนดไว้เป็นวาระพิเศษ

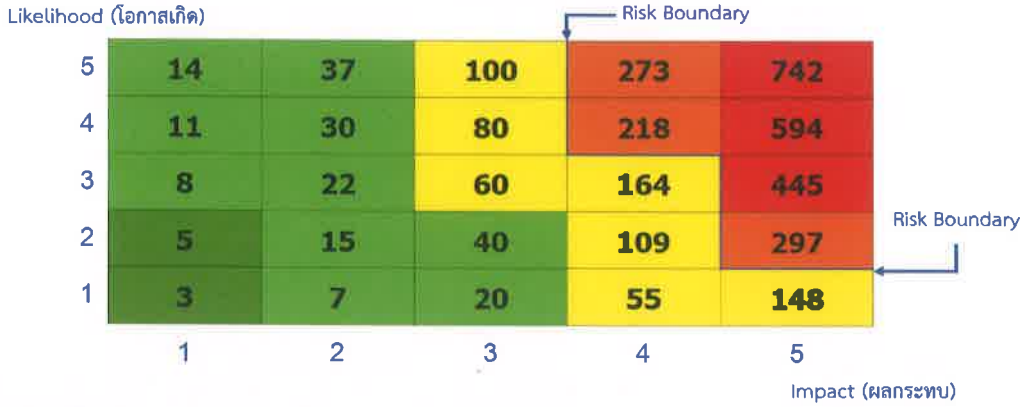
* หลักเกณฑ์การบริหารความเสี่ยงของ บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)

NT Risk Matrix

การคำนวณระดับความรุนแรงของความเสี่ยง Risk Severity

$$\text{Risk Severity} = \text{Likelihood} \times e^{\text{Impact}}$$

$$E \approx 2.71828182845904$$

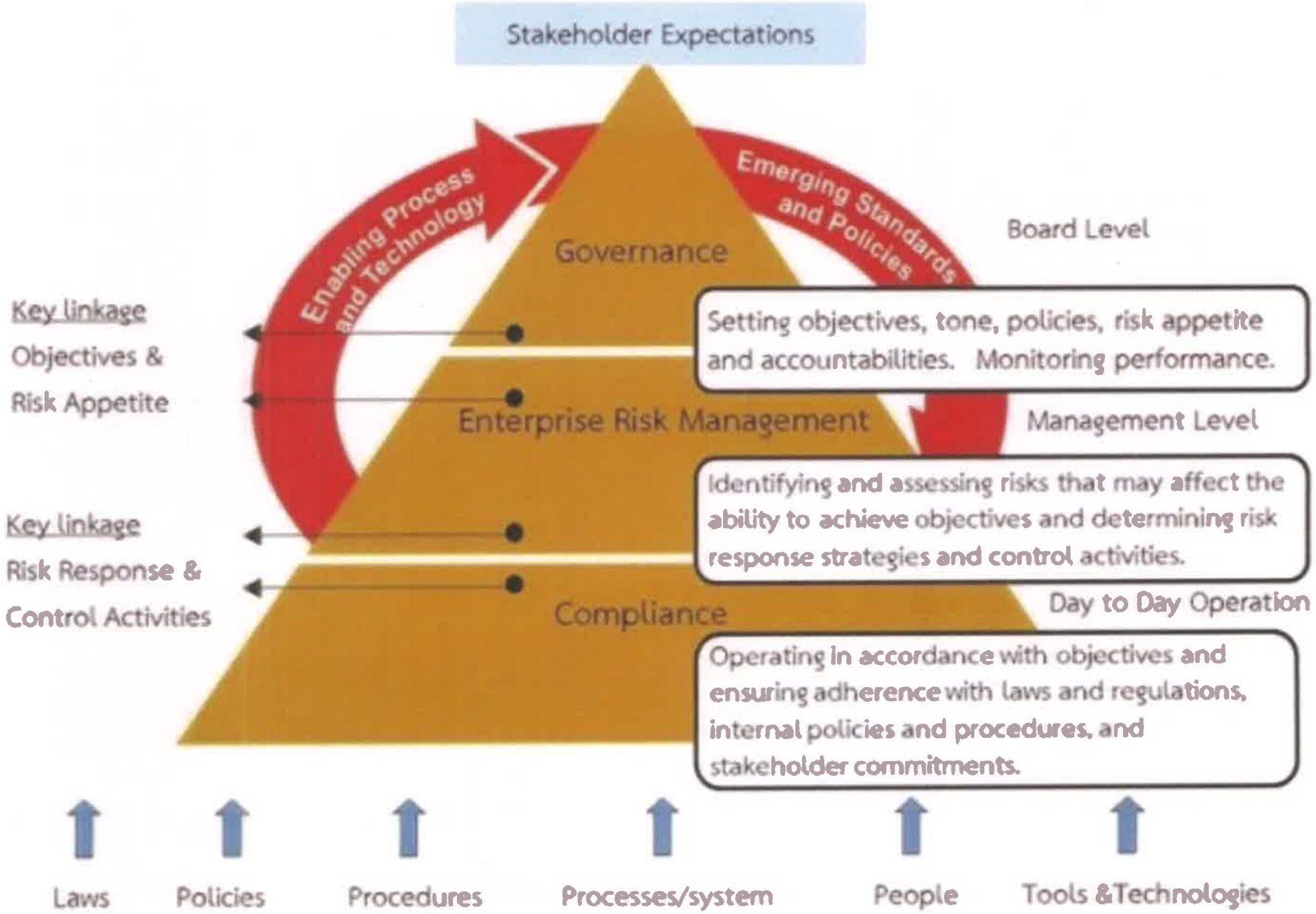


การจัดระดับความเสี่ยง (Action required by risk rating)

ระดับความเสี่ยง	การดำเนินการ
สูงมาก	ยังไม่มีมาตรการรองรับ ต้องรีบดำเนินการจัดการอย่างเร่งด่วน
สูง	มีมาตรการรองรับแล้ว แต่ยังไม่ดีเพียงพอ ต้องหามาตรการใหม่เพิ่มเติม
ปานกลาง	มีมาตรการรองรับที่ดีอยู่แล้ว แต่ยังไม่มีการปฏิบัติอย่างจริงจัง ต้องปฏิบัติให้เข้มข้นขึ้น
ต่ำ	มีมาตรการรองรับที่ดีอยู่แล้ว สามารถดำเนินการได้ตามปกติ
ต่ำมาก	มีมาตรการรองรับที่ดีอยู่แล้ว สามารถดำเนินการได้ตามเป้าหมาย

หมายเหตุ

ปัจจัยเสี่ยงที่มีระดับความรุนแรง สูงมาก และ สูง นำมาบริหารความเสี่ยงระดับองค์กร (อยู่เหนือเส้น Risk Boundary)


Stakeholder Expectations
Enabling Process and Technology
Emerging Standards and Policies
Governance
Board Level
Key linkage
Objectives &
Risk Appetite
Setting objectives, tone, policies, risk appetite and accountabilities. Monitoring performance.
Enterprise Risk Management
Management Level
Identifying and assessing risks that may affect the ability to achieve objectives and determining risk response strategies and control activities.
Key linkage
Risk Response &
Control Activities
Compliance
Day to Day Operation
Operating in accordance with objectives and ensuring adherence with laws and regulations, internal policies and procedures, and stakeholder commitments.
Laws
Policies
Procedures
Processes/system
People
Tools &Technologies

ขั้นตอนการนำ GRC Policy ไปสู่การปฏิบัติ ของ บมจ.โทรคมนาคมแห่งชาติ

ขั้นตอน	แนวทางปฏิบัติ	อ้างอิง
1. กำหนดวัตถุประสงค์ทางธุรกิจ เพื่อให้สอดคล้องกับมูลค่าและความเสี่ยงที่เกี่ยวข้อง	1. การกำหนด/พัฒนากลยุทธ์ ด้วยความเข้าใจที่ถูกต้องเกี่ยวกับบริบทขององค์กร วัฒนธรรมขององค์กร ประเด็นความยั่งยืน และความคาดหวังของผู้มีส่วนได้ส่วนเสียอย่างรอบด้าน จนสามารถนำมาใช้เป็นแนวทางในการกำหนดรูปแบบการดำเนินธุรกิจ/กลยุทธ์ระยะยาว ได้อย่างเหมาะสม เพื่อนำไปสู่การประเมินและวางระบบการบริหารความเสี่ยงทั้งในระดับองค์กรและสายงาน ตลอดจนมีการประเมินและควบคุมให้มีการปฏิบัติงานถูกต้องตามกฎหมายและระเบียบกฎเกณฑ์ต่าง ๆ ที่เกี่ยวข้อง 2. นำเสนอข้อมูลเชิงบูรณาการต่อคณะกรรมการเพื่อประกอบการพิจารณาขออนุมัติแผนกลยุทธ์ ดังนี้ 2.1 ประเมินความเหมาะสมของทิศทาง/รูปแบบการดำเนินธุรกิจในปัจจุบันว่ามีประสิทธิภาพเพียงพอที่จะรับมือกับความท้าทายต่าง ๆ ที่กิจการเผชิญอยู่ตลอดจนสอดรับกับสภาพแวดล้อม ทางธุรกิจที่เปลี่ยนแปลงไปอย่างรวดเร็วหรือไม่อย่างไร 2.2 จัดทำร่างแผนกลยุทธ์ที่เหมาะสม ควบคู่กับการประเมินความเสี่ยงระดับกลยุทธ์ 2.3 ระบุวิธีจัดการความเสี่ยงว่าสามารถทำได้หรือไม่ อย่างไร 2.4 พิจารณาว่ามีความจำเป็นต้องปรับโครงสร้าง หรือแผนการดำเนินงานภายในองค์กรเพื่อให้สอดรับกับกลยุทธ์นั้นหรือไม่ อย่างไร 2.5 พิจารณาว่าการดำเนินงานตามกลยุทธ์ที่นำเสนอมานั้น มีแนวโน้มที่จะเกิดความเสี่ยงจากการไม่ปฏิบัติตามกฎระเบียบ / ข้อบังคับหรือไม่ 3. คณะกรรมการพิจารณาอนุมัติแผนกลยุทธ์	แนวปฏิบัติที่ดีสำหรับคณะกรรมการเกี่ยวกับการบูรณาการ GRC (IOD) หน้า 12 หัวข้อ 1.3.2 หน้า 13 หัวข้อ 1.4.1, 1.4.2, 1.4.3.1 และ หน้า 19 ข้อ 2.2.3

ขั้นตอน	แนวทางปฏิบัติ	อ้างอิง
2. บรรลุวัตถุประสงค์ตามเป้าหมายที่กำหนดและสามารถเพิ่มประสิทธิภาพในการเฝ้าระวัง ความเสี่ยง (Risk Profile) และปกป้องคุณค่าขององค์กร (Value)	1. จัดทำและนำเสนอคณะกรรมการเพื่อขออนุมัติแผนแม่บท/แผนปฏิบัติการ แผนการลงทุน หรือการทำรายการที่มีสาระสำคัญที่สอดรับกับทิศทางกลยุทธ์ที่วางไว้ โดยมีระบบบริหารความเสี่ยงและระบบการติดตามให้มีการปฏิบัติตามกฎเกณฑ์ (Compliance) รวมถึงการควบคุมภายในที่ดี มีข้อมูล บุคลากร และเทคโนโลยีที่ มีคุณภาพ สามารถสนับสนุนการตัดสินใจได้อย่างทันเวลา 2. คณะกรรมการพิจารณาอนุมัติแผนแม่บท/แผนปฏิบัติการ แผนการลงทุน หรือการทำรายการที่มีสาระสำคัญ 3. การติดตามผลการดำเนินงานตามกลยุทธ์ : มีการวางกระบวนการให้มีการรายงานภาพรวมของการดำเนินงานอยู่เป็นระยะ เพื่อให้มั่นใจว่าแผนการดำเนินงานนั้นสอดรับกับทิศทางกลยุทธ์ที่วางไว้ และมั่นใจถึงความมีประสิทธิภาพของกระบวนการดำเนินงานตามหลักการ GRC (ทั้งการรายงานผลการดำเนินงานตามกลยุทธ์ รายงานผลการจัดการความเสี่ยงและการควบคุมภายในที่สำคัญ) เพื่อนำผล/ข้อแนะนำ ไปสู่การปรับปรุงแผนกลยุทธ์ให้เหมาะสมและหาโอกาสในการสร้างมูลค่าเพิ่มให้แก่ธุรกิจได้	แนวปฏิบัติที่ดีสำหรับคณะกรรมการเกี่ยวกับการบูรณาการ GRC (IOD) หน้า 14 หัวข้อ 1.4.3.2 หัวข้อ 1.4.3.3 หน้า 19 ย่อหน้าสุดท้าย
3. ดำเนินการภายใต้ขอบเขตของกฎหมาย สัญญา ระบบภายในสังคม และจริยธรรม	1. นำเสนอข้อมูลด้าน Compliance ต่อคณะกรรมการเพื่อใช้ประกอบการพิจารณาอนุมัติกลยุทธ์ ดังต่อไปนี้ 1.1 ประเด็นทางกฎหมาย จริยธรรม หรือ เรื่องที่มีผลกระทบทางลบต่อผู้มีส่วนได้ส่วนเสียที่อาจเกิดขึ้นได้ พร้อมแนวทางการบริหารจัดการ (Laws, Ethics and Stakeholder Concerns) 1.2 มีความสอดคล้องหรือเป็นไปตามมาตรฐานอุตสาหกรรมหรือแนวปฏิบัติที่ดี (Standard or Best Practices) ที่เกี่ยวข้องหรือไม่	หน้า 21 หัวข้อ 2.4 การกำกับการปฏิบัติตามกฎเกณฑ์ หน้า 18 หัวข้อ 2.1.3

ขั้นตอน	แนวทางปฏิบัติ	อ้างอิง
	1.3 มีแนวทางการตรวจสอบ (Audit) เพื่อให้เกิดความมั่นใจว่ามีการปฏิบัติตามกฎระเบียบ และข้อบังคับ อย่างไร 1.4 มีกระบวนการรายงาน (Reporting Procedure) ต่อคณะกรรมการและผู้มีส่วนได้ส่วนเสีย (Stakeholders) ที่สำคัญขององค์กรอย่างไร 2. มีการประเมินความเสี่ยงด้าน Compliance และกำหนดวิธีจัดการเพื่อลดความเสี่ยงดังกล่าว รวมทั้งรายงานผลให้คณะกรรมการบริษัททราบอย่างสม่ำเสมอ	
4. ให้ข้อมูลที่เกี่ยวข้องเชื่อถือได้ และทันเวลาต่อผู้มีส่วนได้เสีย	1. การเปิดเผยข้อมูลผ่านรายงานประจำปี ที่มีข้อมูลครบถ้วน ถูกต้อง ทันกาล เชื่อถือได้ 2. มีการรายงานความเสี่ยง (Risk Report) ที่สำคัญพร้อมทั้งวิธีจัดการความเสี่ยงนั้นให้คณะกรรมการบริษัททราบอย่างสม่ำเสมอหรืออย่างน้อยทุกไตรมาส เมื่อคณะกรรมการบริษัทได้รับรายงานแล้ว ควรพิจารณาความถูกต้องและครบถ้วนของความเสี่ยง ความเหมาะสมของวิธีจัดการความเสี่ยง และให้ความเห็นหรือข้อแนะนำเกี่ยวกับความเสี่ยงและวิธีจัดการความเสี่ยงที่มีประสิทธิภาพมากขึ้น หรืออาจเป็นข้อแนะนำในการปรับปรุงแผนกลยุทธ์ให้เหมาะสมกับความเสี่ยงที่ประเมินได้ 3. กำหนดให้คณะกรรมการชุดย่อยต่าง ๆ ต้องรายงานผลการปฏิบัติงานให้คณะกรรมการบริษัทรับทราบอย่างสม่ำเสมอหรืออย่างน้อยทุกไตรมาส 4. นำระบบเทคโนโลยีสารสนเทศมาใช้ให้เป็นประโยชน์ต่อการบูรณาการ GRC ตั้งแต่การรวบรวม วิเคราะห์ ติดตาม ประเมิน และรายงานผลต่อผู้บริหารและคณะกรรมการ	1. SEAM หมวด 1 หน้า 1-4 2. IOD หน้า 20 ข้อ 2.3.4 3. IOD หน้า 22 ข้อ 3.5 4. IOD หน้า 27 ข้อ 18

ขั้นตอน	แนวทางปฏิบัติ	อ้างอิง
5. ส่งเสริมการวัดผลของระบบการดำเนินงานและการมีประสิทธิผล	1. ผลการดำเนินงาน Risk Management แสดงการดำเนินมาตรการที่มุ่งขจัดความเสี่ยง รวมถึงการใช้เป็น "สัญญาณเตือนภัยล่วงหน้า" (Early Warning Signs) ที่ทำให้กรรมการเห็นถึงจุดอ่อนของการกำกับดูแล (Governance) และมาตรการปฏิบัติตามกฎเกณฑ์ (Compliance) อันนำไปสู่การแก้ไขได้อย่างทันท่วงที 2. ผลการดำเนินงานด้าน Compliance ที่ครอบคลุมมากกว่าการมุ่งปฏิบัติตามกฎเกณฑ์ภาคบังคับ รวมถึงการมุ่งตอบสนองความคาดหวังของผู้มีส่วนได้ส่วนเสียอย่างเป็นธรรม ตลอดจนการดำเนินงานตามหลักจริยธรรม แนวปฏิบัติที่ดี และมาตรฐานสากล 3. คณะกรรมการตรวจสอบ (Audit Committee) ติดตามดูแลและสอบทานภาพรวมของการดำเนินงานขององค์กร การกำกับดูแลกิจการ การบริหารความเสี่ยง และการติดตามดูแลให้มี การปฏิบัติตามกฎ ระเบียบ และข้อบังคับร่วมด้วย	1. และ 2. IOD หน้า 26 ภาคผนวก GRC Health Check 3. IOD หน้า 25 ข้อ 4.4.2