ประกาศการกีฬาแห่งประเทศไทย

เรื่อง นโยบายและแนวปฏิบัติการการบริหารจัดการความเสี่ยง ด้านความมั่นคงปลอดภัยสารสนเทศของการกีฬาแห่งประเทศไทย (Information Security Risk Management)

.....

เพื่อให้ระบบสารสนเทศของการกีฬาแห่งประเทศไทย มีความมั่นคง ปลอดภัย สามารถดำเนินงานได้อย่างมีประสิทธิภาพ สามารถประเมินและลดความเสี่ยงที่จะเกิดขึ้นในรูปแบบต่าง ๆ ในระบบสารสนเทศ รวมทั้งป้องกันปัญหาที่อาจเกิดขึ้นจากการถูกคุกคามจากภัยต่าง ๆ การกีฬาแห่งประเทศไทย จึงได้จัดทำนโยบายและแนวปฏิบัติในการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศขึ้น เพื่อเผยแพร่ให้บุคลากรทุกระดับปฏิบัติตามอย่างเคร่งครัดและกำหนดให้มีการทบทวนอย่างสม่ำเสมอ ปีละ ๑ ครั้ง

อาศัยอำนาจตามความในมาตรา ๒๓ แห่งพระราชบัญญัติการกีฬาแห่งประเทศไทย พ.ศ. ๒๕๕๘ และที่แก้ไขเพิ่มเติม การกีฬาแห่งประเทศไทย จึงออกประกาศการกีฬาแห่งประเทศไทย เรื่อง การบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศของการกีฬาแห่งประเทศไทย (Information security risk management) ดังต่อไปนี้

๑. นโยบายและแนวปฏิบัติในการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศของการกีฬาแห่งประเทศไทย มีวัตถุประสงค์ ดังนี้

๑.๑ เพื่อให้มีโครงสร้างและบทบาทหน้าที่ ในการกำกับดูแล และสนับสนุนการบริหารความเสี่ยง ด้านเทคโนโลยีสารสนเทศอย่างเพียงพอ เหมาะสมและสอดคล้องกับการดำเนินงานภายในของการกีฬาแห่งประเทศไทย

๑.๒ เพื่อให้ผู้บริหารและผู้ปฏิบัติงาน เข้าใจหลักการ และกระบวนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

๑.๓ เพื่อให้การจัดการระบบงานสารสนเทศภายในการกีฬาแห่งประเทศไทยมีประสิทธิภาพและมีความยืดหยุ่นในการปรับตัวให้ทันต่อการเปลี่ยนแปลงของเทคโนโลยีสารสนเทศสมัยใหม่ รวมทั้งลดโอกาสที่จะก่อให้เกิดความเสียหายที่ไม่ต้องการกับระบบเทคโนโลยีสารสนเทศ

๑.๔ เพื่อให้ผู้ปฏิบัติงานได้รับทราบขั้นตอน และกระบวนการในการวางแผนบริหารความเสี่ยง

๑.๕ เพื่อให้มีการปฏิบัติตามกระบวนการบริหารความเสี่ยงอย่างเป็นระบบและต่อเนื่อง

๑.๖ เพื่อลดโอกาสและผลกระทบของความเสี่ยงที่จะเกิดขึ้นกับการกีฬาแห่งประเทศไทย

๑.๗ เพื่อเป็นแนวทางานการดำเนินการกำกับดูแล ตรวจสอบเกี่ยวกับการบริหารจัดการและการเผยแพร่ ความรู้ความเข้าใจเกี่ยวกับการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศภายในการกีฬาแห่งประเทศไทย

๑.๘ เพื่อช่วยเพิ่ม ...

๑.๘ เพื่อช่วยเพิ่มประสิทธิภาพการตัดสินใจ โดยคำนึงถึงปัจจัยเสี่ยงและความเสี่ยงในด้านต่าง ๆ ที่จะมีผลกระทบกับการดำเนินงาน วัตถุประสงค์และนโยบาย แล้วพิจารณาหาแนวทางในการป้องกันหรือจัดการกับความเสี่ยงเหล่านั้น ก่อนที่จะเริ่มปฏิบัติงานหรือดำเนินงานตามแผน

๒. นโยบายและแนวปฏิบัติในการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศของการกีฬาแห่งประเทศไทยสารสนเทศของการกีฬาแห่งประเทศไทย สามารถแบ่งออกได้ดังนี้

๒.๑ การประเมินความเสี่ยง (Risk assessment)

๒.๒ การจัดการความเสี่ยง (Risk Treatment)

๒.๓ การติดตามและทบทวนความเสี่ยง (Risk monitoring and review)

๒.๔ การรายงานความเสี่ยง (Risk reporting)

๓. การกำหนดผู้รับผิดชอบ

๓.๑ ระดับนโยบาย

ผู้บริหารระดับสูงสุด (Chief Executive Officer : CEO) เป็นผู้กำหนดแผนการดำเนินงาน แนวนโยบายและแนวปฏิบัติ รวมถึงกำกับดูแล ให้เป็นไปตามนโยบายและแนวปฏิบัติการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ

ผู้บริหารระดับสูงด้านเทคโนโลยีสารสนเทศ (Chief Information Officer : CIO) เป็นผู้รับผิดชอบในการสั่งการตามแนวนโยบายและแนวปฏิบัติการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ

ผู้อำนวยการฝ่ายสารสนเทศและวิชาการกีฬา เป็นผู้รับผิดชอบติดตาม กำกับดูแล ควบคุม ตรวจสอบ รวมทั้งให้ข้อเสนอแนะ ให้คำปรึกษา แก่เจ้าหน้าที่ระดับปฏิบัติ

๓.๒ ระดับปฏิบัติ

เพื่อให้การปฏิบัติตามแนวนโยบายและแนวปฏิบัติการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศของการกีฬาแห่งประเทศไทยเป็นไปอย่างมีประสิทธิภาพ จึงได้กำหนดให้ ฝ่ายสารสนเทศและวิชาการกีฬา มีหน้าที่เป็นผู้ดูแลระบบ เป็นผู้รับผิดชอบระบบสารสนเทศหรือผู้ที่ได้รับมอบหมาย เป็นผู้รับผิดชอบดำเนินการให้เป็นไปตามประกาศนี้ และให้มีการทบทวน ปรับปรุงนโยบายและแนวปฏิบัติในบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศให้เป็นปัจจุบันอยู่เสมอ อย่างน้อยปีละ ๑ ครั้ง และหากมีการเปลี่ยนแปลงนโยบายและแนวปฏิบัติให้ประกาศให้เจ้าหน้าที่ทุกระดับในหน่วยงานการกีฬาแห่งประเทศไทย รับทราบทุกครั้ง

๔. นโยบายและแนวปฏิบัติการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศของการกีฬาแห่งประเทศไทย จัดเป็นมาตรฐานด้านการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของการกีฬาแห่งประเทศไทย เพื่อใช้เป็นแนวทางในการลดความเสี่ยงในรูปแบบต่าง ๆ ของระบบสารสนเทศที่สามารถเกิดขึ้นได้ จึงให้ใช้แนวปฏิบัติการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศของการกีฬาแห่งประเทศไทยตามเอกสารแนบท้ายประกาศนี้ ซึ่งเจ้าหน้าที่ของการกีฬาแห่งประเทศไทยและหน่วยงานที่เกี่ยวข้องต้องถือปฏิบัติอย่างเคร่งครัด

๕. นโยบาย ...

๕. นโยบายและแนวปฏิบัติการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศของการกีฬาแห่งประเทศไทย จัดเป็นมาตรฐานด้านการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศของการกีฬาแห่งประเทศไทย ของการกีฬาแห่งประเทศไทย เพื่อใช้เป็นแนวทางในการดำเนินการควบคุม และลดความเสี่ยงที่จะเกิดขึ้นภายในระบบสารสนเทศ จึงให้ใช้แนวปฏิบัติการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศของการกีฬาแห่งประเทศไทย ตามเอกสารแนบท้ายประกาศนี้ ซึ่งเจ้าหน้าที่ของการกีฬาแห่งประเทศไทย และหน่วยงานที่เกี่ยวข้องต้องถือปฏิบัติอย่างเคร่งครัดต่อไป

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

ประกาศ ณ วันที่ ๑๓ สิงหาคม พ.ศ. ๒๕๖๓

(นายก้องศักด ยอดมณี)
ผู้ว่าการการกีฬาแห่งประเทศไทย

เอกสารแนบท้ายประกาศ
แนวนโยบายและแนวปฏิบัติ
ในการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ
ขององค์กร (Information Security Risk Management)
ของการกีฬาแห่งประเทศไทย
พ.ศ. ๒๕๖๓

ความหมายและคำจำกัดความ

๑. **“กกท.”** หมายความว่า การกีฬาแห่งประเทศไทย

๒. **หน่วยงาน** หมายความว่า ฝ่าย/สำนัก/สายงาน/ศูนย์ ที่เป็นส่วนราชการตามโครงสร้างของการกีฬาแห่งประเทศไทย

๓. **หน่วยงานภายนอก** หมายความว่า องค์กร หรือหน่วยงานภายนอกที่ได้รับอนุญาตให้มีสิทธิในการเข้าถึงและการใช้งานข้อมูลหรือสินทรัพย์ต่าง ๆ ของการกีฬาแห่งประเทศไทย โดยจะได้รับสิทธิในการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับข้อมูล

๔. **ผู้บริหารระดับสูงสุด (Chief Executive Officer : CEO)** หมายความว่า ผู้ว่าการการกีฬาแห่งประเทศไทย

๕. **ผู้บริหารด้านเทคโนโลยีสารสนเทศระดับสูง (Chief Information officer : CIO)** หมายความว่า รองผู้ว่าการ ที่มีหน้าที่ดูแลรับผิดชอบด้านเทคโนโลยีสารสนเทศ ซึ่งมีบทบาทหน้าที่และความรับผิดชอบในส่วนของการกำหนดนโยบายมาตรฐานการควบคุมการใช้งานระบบเทคโนโลยีสารสนเทศ

๖. **ผู้บริหาร** หมายความว่า ผู้อำนวยการฝ่ายสารสนเทศและวิชาการกีฬา ผู้อำนวยการกองสารสนเทศ หัวหน้างานบริการเทคโนโลยีสารสนเทศ หัวหน้างานปฏิบัติการคอมพิวเตอร์ ที่ได้รับมอบหมายให้ดูแลด้านไอที

๗. **ผู้บังคับบัญชา** หมายความว่า ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารขององค์กร

๘. **ผู้พัฒนาระบบ** หมายความว่า ผู้ซึ่งได้รับมอบหมายให้รับผิดชอบในการพัฒนาระบบสารสนเทศ

๙. **เจ้าหน้าที่** หมายความว่า บุคลากรทุกประเภทของการกีฬาแห่งประเทศไทย

๑๐. **ความเสี่ยง (Risk)** หมายความว่า เหตุการณ์ที่มีความไม่แน่นอน อาจเกิดขึ้นและมีผลกระทบในเชิงลบต่อการบรรลุวัตถุประสงค์และเป้าหมาย

๑๑. **โอกาส (Likelihood)** หมายความว่า โอกาสหรือความเป็นไปได้ที่เหตุการณ์จะเกิดขึ้น

๑๒. **ผลกระทบ (Impact)** หมายความว่า ผลกระทบจากเหตุการณ์ที่เกิดขึ้นทั้งที่เป็นตัวเงินและไม่เป็นตัวเงิน

๑๓. **การระบุปัจจัยเสี่ยง (Risk Identification)** หมายความว่า การระบุปัจจัยเสี่ยง เป็นขั้นตอนในการค้นหาว่าปัจจัยเสี่ยงใดบ้างที่ส่งผลกระทบต่อเป้าหมาย

๑๔. **ความเสี่ยงที่เหลืออยู่ (residual risk)** หมายความว่า ระดับความเสี่ยงที่เหลืออยู่หลังจากใส่การควบคุมที่มีอยู่เข้าไปในการบริหารงานแล้ว ซึ่งหากยังคงเหลืออยู่ในระดับสูง-สูงมาก หน่วยงานก็ควรให้ความสนใจเป็นพิเศษและจัดทำแผนเพื่อลดความเสี่ยงให้อยู่ในระดับที่เหมาะสมต่อไป

๑๕. **Risk Appetite** หมายความว่า ระดับความเสี่ยงโดยรวมที่องค์กรยอมรับได้เพื่อมุ่งไปสู่พันธกิจหรือวิสัยทัศน์ของ องค์กร

๑๖. **Degree of Risk** หมายความว่า ระดับของการยอมรับความเสี่ยง

๑๗. **IT key risk indicators** หมายความว่า ตัวชี้วัดเชิงปริมาณ กิจกรรม หรือเหตุการณ์ ที่บ่งบอกถึงการเปลี่ยนแปลงของความเสี่ยงสำคัญ ที่ส่งผลกระทบต่อเป้าหมายได้ โดยสามารถใช้ประโยชน์ในการบริหารความเสี่ยง เพื่อติดตามผลการบริหารความเสี่ยงว่าเป็นไปตามเป้าหมายหรือไม่ เพื่อ จะได้ปรับปรุง/เปลี่ยนแปลงแผนการบริหารความเสี่ยงให้มีประสิทธิภาพมากยิ่งขึ้น

สารบัญ

ประกาศการกีฬาแห่งประเทศไทย
ความหมายและคำจำกัดความ
การบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร
(information security risk management) ๑
๑. วัตถุประสงค์
๒. กระบวนการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ
(Information Security Risk Management) ๒
๓. ปัจจัยของความเสี่ยง
๓.๑. ความเสี่ยงที่เกิดจากภายใน
๓.๒. ความเสี่ยงที่เกิดจากภายนอก ๓
๔. นโยบายการบริหารความเสี่ยง
๔.๑ โครงสร้างและบทบาทหน้าที่
๕. หลักเกณฑ์ ระเบียบวิธีปฏิบัติ และกระบวนการในการบริหารความเสี่ยง ๔
ด้านความมั่นคงปลอดภัยสารสนเทศ
๕.๑ การประเมินความเสี่ยง (Risk assessment)
๕.๒ การจัดการความเสี่ยง (Risk Treatment) ๗
๕.๓ การติดตามและทบทวนความเสี่ยง (Risk monitoring and review) ๘
๕.๔ การรายงานความเสี่ยง (Risk reporting)

ภาคผนวก
ตัวอย่าง ตารางระบุความเสี่ยงและผลกระทบด้านต่างๆ ที่จะเกิดขึ้น

การบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร (Information security risk management)

การบริหารงานขององค์กรทุกประเภท ทั้งภาครัฐ และภาคเอกชน ต่างมีวัตถุประสงค์ของตนเอง และมุ่งหวังที่จะทำงานไปให้ถึงเป้าหมายที่วางไว้อย่างดีที่สุด สูญเสียทรัพยากรให้น้อยที่สุด แต่การดำเนินการใดๆ เพื่อบรรลุวัตถุประสงค์ที่วางไว้ มักจะต้องประสบความไม่แน่นอนที่จะประสบความสำเร็จมาก น้อยแล้วแต่สภาวะที่แวดล้อมอยู่ ดังนั้นความเสี่ยงจึงเป็นภาวะคุกคาม ปัญหา อุปสรรค หรือการสูญเสียโอกาสที่ทำให้องค์กรไม่สามารถบรรลุวัตถุประสงค์ตามที่กำหนดไว้ หรือก่อผลเสียหายแก่องค์กร ทั้งในด้านยุทธศาสตร์ การดำเนินงาน การเงิน ทรัพยากรต่างๆ หรือแม้แต่ชื่อเสียง ภาพลักษณ์

ประเด็นที่สำคัญในเรื่องความเสี่ยง (Risk) คือ ความไม่แน่นอน (Uncertainty) ของผลลัพธ์ที่อาจเป็นในเชิงบวก หรือเชิงลบก็ได้ หากองค์กรสามารถเข้าไปบริหารความเสี่ยงได้อย่างถูกต้อง ภาวะคุกคามปัญหาอุปสรรคทั้งหลายที่คาดไว้อาจก่อให้เกิดโอกาสและนำไปสู่นวัตกรรมได้ ทั้งยังเกิดโอกาสในการพัฒนาประสิทธิภาพในการทำงาน และการให้บริการ ความเสี่ยงเป็นเรื่องประกอบกันระหว่างองค์ประกอบที่สำคัญ ๒ ส่วน คือ โอกาสที่น่าจะเกิดขึ้นของสิ่งที่ไม่พึงประสงค์ กับผลกระทบที่ตามมา การบริหารความเสี่ยงอย่างเหมาะสมจะเป็นการสนับสนุน กลยุทธ์และแผนงานให้บรรลุเป้าหมายตามที่วางไว้ เข้าใจภัยคุกคามของการปฏิบัติงานในองค์กรมีประสิทธิภาพมากขึ้น สนับสนุนให้มีการปรับปรุงงานอย่างต่อเนื่อง มีการสื่อสารในองค์กรมากขึ้น ความสัมพันธ์ต่างๆ ก็ดีตามมา การบริหารความเสี่ยงระดับองค์กร เป็นการผสมผสานการบริหารความเสี่ยงโดยพิจารณาจากความเสี่ยงทั้งหมด เป็นกระบวนการเชิงระบบเพื่อระบุ ประเมิน ควบคุม และสื่อสารความเสี่ยง โดยให้คลอบคลุมทั้งองค์กร ให้มีกระบวนคิดในการที่จะมองไปข้างหน้า โดยได้รับการสนับสนุน และมีส่วนร่วมจากผู้บริหารในทุกระดับ และจากทุกคนในองค์กร

๑.วัตถุประสงค์

๑. เพื่อให้องค์กรมีโครงสร้างและบทบาทหน้าที่ ในการกำกับดูแลและสนับสนุนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศอย่างเพียงพอเหมาะสมและสอดคล้องกับการดำเนินงานภายในองค์กร

๒. เพื่อให้ผู้บริหารและผู้ปฏิบัติงาน เข้าใจหลักการ และกระบวนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

๓. เพื่อให้การจัดการระบบงานสารสนเทศภายในกกท.มีประสิทธิภาพและมีความยืดหยุ่นในการปรับตัวให้ทันต่อการเปลี่ยนแปลงของเทคโนโลยีสารสนเทศสมัยใหม่ รวมทั้งลดโอกาสที่จะก่อให้เกิดความเสียหายที่ไม่ต้องการกับระบบเทคโนโลยีสารสนเทศ

๔. เพื่อให้ผู้ปฏิบัติงานได้รับทราบขั้นตอน และกระบวนการในการวางแผนบริหารความเสี่ยง

๕. เพื่อให้มีการปฏิบัติตามกระบวนการบริหารความเสี่ยงอย่างเป็นระบบและต่อเนื่อง

๖. เพื่อลดโอกาสและผลกระทบของความเสี่ยงที่จะเกิดขึ้นกับองค์กร

๗. เพื่อเป็นแนวทางานการดำเนินการกำกับดูแล ตรวจสอบเกี่ยวกับการบริหารจัดการและการเผยแพร่ ความรู้ความเข้าใจเกี่ยวกับการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศภายกกท.

๘. เพื่อช่วยเพิ่มประสิทธิภาพการตัดสินใจ โดยคำนึงถึงปัจจัยเสี่ยงและความเสี่ยงในด้านต่างๆ ที่จะมีผลกระทบกับการดำเนินงาน วัตถุประสงค์และนโยบาย แล้วพิจารณาหาแนวทางในการป้องกันหรือจัดการกับความเสี่ยงเหล่านั้น ก่อนที่จะเริ่มปฏิบัติงานหรือดำเนินงานตามแผน

๒. กระบวนการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Risk Management)

กระบวนการบริหารความเสี่ยง เป็นกระบวนการที่ใช้ในการระบุ วิเคราะห์ ประเมิน และจัดลำดับความเสี่ยงที่มีผลกระทบต่อการบรรลุวัตถุประสงค์ในการดำเนินงานขององค์กร รวมทั้งการจัดทำแผนบริหารจัดการความเสี่ยง โดยกำหนดแนวทางการควบคุมเพื่อป้องกันหรือลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้

๓. ปัจจัยของความเสี่ยง

ต้นเหตุหรือสาเหตุที่มาของความเสี่ยง ที่จะทำให้ไม่บรรลุวัตถุประสงค์ที่กำหนดไว้ โดยต้องระบุได้ด้วยว่าเหตุการณ์นั้นจะเกิดที่ไหน เมื่อใด และเกิดขึ้นได้อย่างไร และทำไม ทั้งนี้สาเหตุของความเสี่ยงที่ระบุควรเป็นสาเหตุที่แท้จริง เพื่อจะได้วิเคราะห์และกำหนดมาตรการลดความเสี่ยงในภายหลังได้อย่างถูกต้อง โดยปัจจัยเสี่ยงแบ่งได้ ๒ ด้าน ดังนี้

๓.๑. ความเสี่ยงที่เกิดจากภายใน

ความเสี่ยงที่สามารถควบคุมการเกิดได้โดยองค์กร เช่น

๑) การพัฒนาระบบ เช่น ผู้พัฒนาระบบไม่ทราบความต้องใช้อย่างแท้จริง ระบบมีฟังก์ชั่นงานไม่ครบถ้วน, ผู้พัฒนาระบบไม่มีความรู้เพียงพอ ออกแบบระบบผิดพลาด ไม่ครบถ้วน รวมทั้งอาจมีการฝังโปรแกรมอันตรายเอาไว้ เพื่อลักลอบส่งข้อมูลออก

๒) การใช้ระบบ เช่น ผู้ใช้ไม่มีอำนาจในการเข้าถึงข้อมูลอาจเข้าได้โดยให้รหัสผ่านกัน, การบันทึกข้อมูลไม่ครบถ้วน ผิดพลาด บกพร่องทั้งคู่มือและรายงานต่างๆ ผู้ใช้ไม่สามารถสืบค้นหรือเรียกข้อมูลที่ต้องการใช้

๓) ความเสี่ยงเกี่ยวกับอุปกรณ์ เช่น คอมพิวเตอร์และอุปกร์ไม่สามารถทำงานร่วมกันได้ สมรรถนต่ำ ทำงานช้า อุปกรณ์เกิดความเสียหายเพราะไม่ได้รับการบำรุงรักษาอย่างถูกวิธี การถูกโจรกรรม ถูกทำลายด้วยผู้บุกรุก ไม่มีการปรับปรุงเครื่องให้ทันสมัยสามารถใช้งานร่วมกับหน่วยงานอื่นได้

๔) ความเสี่ยงจากบุคลากรภายใน บุคลากรเจ้าหน้าที่หรือผู้ที่เกี่ยวข้องขององค์กร เช่น เจ้าหน้าที่หรือบุตรหลานอาจจะนำเกมจากบ้านมาเล่นกับคอมพิวเตอร์สำนักงาน มีการก็อปปี้ข้อมูลไปให้บุคคลภายนอกซึ่งอาจจะเป็นความลับ อาจเกิดการไม่พอใจสำนักงานหรือผู้บังคับบัญชาแอบทำงานข้อมูลหรืออุปกรณ์ภายใน การใช้โปรแกรมที่ไม่ได้รับการฝึกอบรม หรือเจ้าหน้าที่อาจจะแอบแก้ไขโปรแกรมและข้อมูลระหว่างทำงาน

๓.๒. ความเสี่ยงที่เกิดจากภายนอก

ความเสี่ยงที่ไม่สามารถควบคุมการเกิดได้โดยองค์กรในด้านข้อมูล นโยบายการบริหารและการจัดการ ระบบสารสนเทศอาจประสบปัญหาได้หลายเรื่อง เช่น การบุกรุกมาโจรกรรมอุปกรณ์ ในช่วงที่ไม่มีใครดูแล ถูกไวรัสก่อกวนจากอินเตอร์เน็ต อีเมล์ เกม flash drive แฮคเกอร์บุกรุกเข้ามาทางระบบอินเตอร์เน็ตเพื่อทำลายซอฟต์แวร์ เว็บหรือข้อมูล ความรู้ความสามารถของบุคลากรในกระบวนการทำงาน

๔. นโยบายการบริหารความเสี่ยง

เพื่อสร้างความตระหนักและกระตุ้นให้ผู้บริหาร พนักงาน ภายในกกท. เห็นถึงความจำเป็นในการระมัดระวังต่อสถานการณ์ที่คุกคามต่อประสิทธิภาพการปฏิบัติงาน การบริหารงานและอาจทำให้เกิดความเสียหายต่อระบบสารสนเทศซึ่งเป็นเครื่องมือที่สำคัญในการให้บริการแก่เจ้าหน้าที่ภายในกกท. รวมถึงบุคคลภายนอก การกำหนดนโยบายหรือแผนบริหารความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ จะทำให้เจ้าหน้าที่ทุกคนที่เกี่ยวข้องทราบถึงแนวทางในการปฏิบัติ ซึ่งจะถือเป็นส่วนหนึ่งของการดำเนินงาน การปฏิบัติงานเพื่อหลีกเลี่ยงความเสี่ยงต่าง ๆ หรือลดความรุนแรงของผลเสียหายต่าง ๆ ที่อาจเกิดขึ้นต่อระบบงานของกกท. การดำเนินงานการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศของกกท. จะประกอบไปด้วย ๒ ส่วน คือ โครงสร้างและบทบาทหน้าที่ของผู้เกี่ยวข้องในการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ และหลักเกณฑ์ ระเบียบวิธีปฏิบัติ และกระบวนการในการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ

๔.๑ โครงสร้างและบทบาทหน้าที่

โครงสร้างการบริหารความเสี่ยง ประกอบไปด้วย การกำกับดูแล การตัดสินใจ การจัดทำแผนการดำเนินการ การติดตามประเมินผล และการสอบทาน ซึ่งในแต่ละองค์ประกอบมีอำนาจหน้าที่ดังนี้

๔.๑.๑ ผู้บริหารระดับสูงสุด

๑) รับผิดชอบในการกำหนดนโยบาย ส่งเสริมให้มีการดำเนินงานบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ

๒) ให้ความเห็นชอบและให้ข้อเสนอแนะต่อระบบและแผนการบริหารจัดการความเสี่ยง

๓) รับทราบผลการบริหารความเสี่ยงและเสนอแนะแนวทางการพัฒนา

๔.๑.๓ ผู้บริหารระดับสูง

๑) แต่งตั้งคณะทำงานบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

๒) ส่งเสริมและติดตามให้มีการบริหารความเสี่ยงอย่างมีประสิทธิภาพและเหมาะสม

๓) พิจารณาให้ความเห็นชอบและอนุมัติแผนการบริหารความเสี่ยง

๔) พิจารณาผลการบริหารความเสี่ยงและเสนอแนะแนวทางการพัฒนา

๔.๑.๔ งานปฏิบัติการคอมพิวเตอร์

๑) สอบทานกระบวนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

๒) นำเสนอผลการบริหารความเสี่ยงให้ผู้บริหารตรวจสอบและประเมินรับทราบและให้ข้อเสนอแนะ

๔.๑.๕ งานบริการเทคโนโลยีสารสนเทศ

๑) จัดให้มีระบบและกระบวนการบริหารความเสี่ยงที่เป็นระบบมาตรฐานเดียวกันทั้งองค์กร

๒) ดำเนินการตามกระบวนการบริหารความเสี่ยง และการปฏิบัติตามมาตรการลดและควบคุมความเสี่ยง

๓) รายงานและติดตามผลการดำเนินงานตามแผนการบริหารความเสี่ยงที่สำคัญ เสนอต่อผู้อำนวยการเพื่อพิจารณา

๔.๑.๖ ผู้ปฏิบัติงาน

๑) สนับสนุนข้อมูลที่เกี่ยวข้องให้กับคณะทำงานบริหารความเสี่ยง

๒) ให้ความร่วมมือในการปฏิบัติงานตามแผนบริหารความเสี่ยง

๕. หลักเกณฑ์ ระเบียบวิธีปฏิบัติ และกระบวนการในการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ

๕.๑ การประเมินความเสี่ยง (Risk assessment)

การวิเคราะห์ความเสี่ยง จากการวิเคราะห์ความเสี่ยงด้านสารสนเทศของกรมสามารถแยกประเภทความเสี่ยงเป็น ๔ ประเภท ดังนี้

๑) ความเสี่ยงด้านเทคนิค เป็นความเสี่ยงที่อาจเกิดขึ้นจากระบบคอมพิวเตอร์เครื่องมือและอุปกรณ์เอง อาจเกิดถูกโจมตีจากไวรัสหรือโปรแกรมไม่ประสงค์ดี การถูกก่อกวนจาก Hacker ถูกเจาะทำลายระบบจาก Cracker เป็นต้น

๒) ความเสี่ยงจากผู้ปฏิบัติงาน เป็นความเสี่ยงที่อาจเกิดขึ้นจากการดำเนินการ การจัดความสำคัญในการ เข้าถึงข้อมูลไม่เหมาะสมกับการใช้งานหรือการให้บริการ โดยผู้ใช้อาจเข้าสู่ระบบเทคโนโลยีสารสนเทศและการสื่อสาร หรือใช้ข้อมูลต่างๆ ของกกท. เกินกว่าอำนาจหน้าที่ของตนเองที่มีอยู่และอาจทำให้เกิดความเสียหายต่อ ข้อมูลสารสนเทศได้

๓) ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน เป็นความเสี่ยงที่อาจเกิดจากภัยพิบัติตามธรรมชาติหรือ สถานการณ์ร้ายแรงที่ก่อให้เกิดความเสียหายร้ายแรงกับข้อมูลสารสนเทศ เช่น ไฟฟ้าขัดข้อง น้ำท่วม ไฟไหม้ อาคารถล่ม การชุมนุมประท้วง หรือความไม่สงบเรียบร้อยในบ้านเมือง เป็นต้น

๔) ความเสี่ยงด้านการบริหารจัดการ เป็นความเสี่ยงจากแนวนโยบายในการบริหารจัดการที่อาจส่งผล กระทบต่อการดำเนินการด้านสารสนเทศ

การประเมินความเสี่ยง มีกระบวนการในการดำเนินการ โดยแบ่งเป็น ๓ หัวข้อหลักดังนี้

๕.๑.๑ การระบุความเสี่ยง (Risk identification)

เป็นกระบวนการที่ผู้บริหารและผู้ปฏิบัติงานร่วมกันระบุความเสี่ยงและปัจจัยเสี่ยงที่เกี่ยวข้องกับระบบสารสนเทศภายในองค์กร เพื่อให้ทราบถึงเหตุการณ์ที่เป็นความเสี่ยง ที่อาจมีผลกระทบต่อการดำเนินงาน วัตถุประสงค์ซึ่งต้องคำนึงถึงสภาพแวดล้อมทั้งภายนอกและภายในองค์กร วิธีการในการระบุความเสี่ยงมีหลายวิธีเช่น

๑. การประชุมร่วมมือเพื่อให้ได้ความเสี่ยงที่หลากหลาย
๒. การใช้ Checklist
๓. การวิเคราะห์สถานการณ์จากการตั้งคำถาม “What-if”
๔. การวิเคราะห์ขั้นตอนการปฏิบัติงานในแต่ละขั้นตอน

ในขั้นตอนนี้ควรมีการเก็บข้อมูลความสูญเสียที่เกิดขึ้นในรูปของความถี่ของการเกิดความสูญเสีย และความรุนแรงของความสูญเสีย รวมทั้งข้อมูลการดำเนินการใดๆ เพื่อลดความสูญเสียที่เกิดขึ้นในอดีตทั้งที่ ประสบผลสำเร็จ และปัญหาอุปสรรคซึ่งจะเป็นประโยชน์ในการดำเนินการต่อไป

การระบุความเสี่ยงและผลกระทบด้านต่าง ๆ ที่จะเกิดขึ้น คณะผู้บริหารหรือคณะทำงานอาจมีการดำเนินการจัดทำข้อมูลตามตารางตัวอย่างในภาคผนวกที่ ๑

๕.๑.๒ การวิเคราะห์และประเมินความเสี่ยง (Risk analysis)

การประเมินความเสี่ยงเป็นกระบวนการที่ประกอบด้วยการวิเคราะห์ การประเมิน และการจัดระดับความเสี่ยง ประกอบด้วย ๔ ขั้นตอน คือ

๑. การกำหนดเกณฑ์การประเมินมาตรฐาน เป็นเกณฑ์ที่จะใช้ประเมินความเสี่ยงได้แก่ โอกาสที่จะเกิดความเสี่ยง (Likelihood) ระดับความรุนแรงของผลกระทบ (Impact) และระดับของความเสี่ยง (Degree of Risk) คณะกรรมการบริหารความเสี่ยงต้องกำหนดเกณฑ์ของหน่วยงานขึ้น ซึ่งอาจกำหนดได้ทั้งเกณฑ์เชิญปริมาณและเชิงคุณภาพ การกำหนดเกณฑ์ของโอกาสที่เกิดความเสี่ยงอาจกำหนดเป็นเกณฑ์ ๕ ระดับ (สูงมาก/รุนแรงมากที่สุด สูง/ค่อนข้างรุนแรง ปานกลาง น้อย และ น้อยมาก) ส่วนระดับของความเสี่ยงอาจกำหนดเป็นเกณฑ์ ๔ ระดับ (สูงมาก สูง ปานกลาง และ น้อย)

๒. การประเมินโอกาสและผลกระทบของความเสี่ยง เป็นการนำความเสี่ยงและปัจจัยเสี่ยงแต่ละปัจจัยที่ระบุไว้มาประเมินโอกาสที่จะเกิดเหตุการณ์ความเสี่ยงเหล่านั้นและประเมินระดับความรุนแรงหรือมูลค่าความเสียหายจากความเสี่ยงตามเกณฑ์มาตรฐานที่กำหนดเพื่อให้เห็นระดับความเสี่ยง ซึ่งแต่ละความเสี่ยง ก็จะมีความรุนแรงแตกต่างกัน ทั้งนี้การควบคุมความเสี่ยงหรือหลีกเลี่ยงความเสี่ยงนั้น ก็จะขึ้นอยู่

กับมาตรการควบคุมความเสี่ยงของแต่ละหน่วยงาน โดยมีการประเมินใน ๒ มิติ ได้แก่ มิติผลกระทบ และมิติโอกาสของความเสี่ยงที่จะเกิดขึ้น

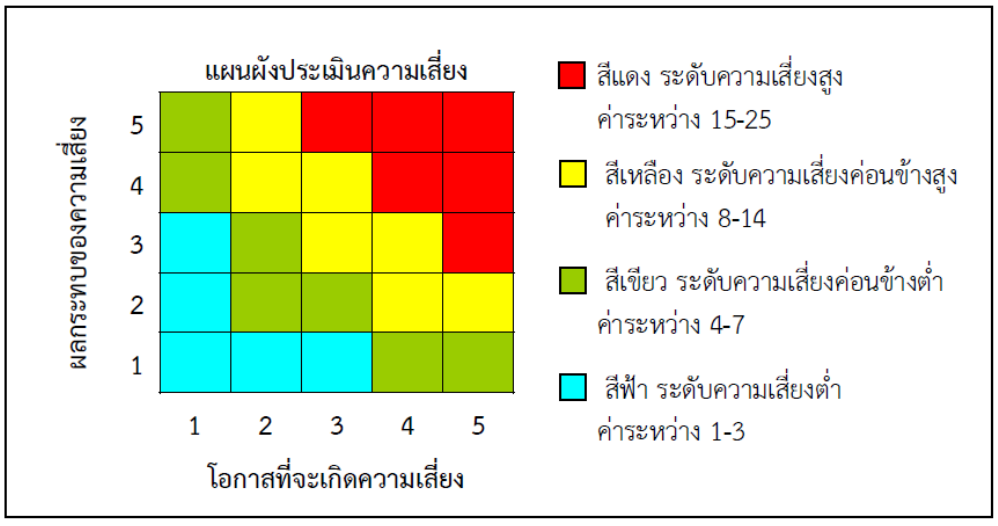
เกณฑ์การประเมินผลกระทบ (ความน่าเชื่อถือ/ความพึงพอใจของผู้ใช้บริการ) เป็นดังนี้

ระดับ	การประเมิน
๑	น้อยมาก (แทบไม่มีผลกระทบเลย)
๒	น้อย (เจ้าหน้าที่ได้รับเสียงบ่นหรือถูกตำหนิ)
๓	ปานกลาง (เจ้าหน้าที่ถูกร้องเรียนหรือถูกลงโทษทางวินัย)
๔	สูง (ผู้บริหารถูกตำหนิหรือถูกร้องเรียน)
๕	สูงมาก (ผู้บริหารถูกลงโทษทางวินัย)

เกณฑ์การประเมินโอกาสของการเกิดความเสี่ยง เป็นดังนี้

ระดับ	การประเมิน
๑	เกิดขึ้นน้อยมาก นาน ๆ ครั้ง (แทบไม่เกิดขึ้นเลย)
๒	เกิดขึ้นน้อย ไม่บ่อย (อาจเกิดขึ้นได้ทุก ๕ ปี)
๓	เกิดขึ้นปานกลาง (อาจเกิดขึ้นได้ทุกปี)
๔	เกิดขึ้นสูง หรือ บ่อย (อาจเกิดขึ้นได้ทุกเดือน)
๕	เกิดขึ้นสูงมาก หรือ บ่อยมาก (อาจเกิดขึ้นได้ทุกวัน)

๓. การวิเคราะห์ความเสี่ยง เป็นการดูความสัมพันธ์ระหว่างโอกาสที่จะเกิดความเสี่ยงและผลกระทบของความเสี่ยงต่อองค์กรว่าจะก่อให้เกิดระดับความเสี่ยงในระดับใด โดยใช้ตารางระดับความเสี่ยงสูงสุดที่จะต้องบริหารจัดการก่อน ดังรูป



๔. การจัดลำดับความเสี่ยง เป็นการจัดลำดับความรุนแรงของความเสี่ยงที่ผลต่อองค์กรเพื่อพิจารณากำหนดกิจกรรมการควบคุมในแต่ละสาเหตุของความเสี่ยงที่สำคัญให้เหมาะสม โดยพิจารณาจากระดับความเสี่ยงที่ประเมินได้แล้ว เลือกความเสี่ยงที่มีระดับสูงมากหรือสูง มาจัดทำแผนการบริหารความเสี่ยงก่อน

๕.๑.๓ การประเมินค่าความเสี่ยง (Risk evaluation)

การประเมินค่าความเสี่ยงจะพิจารณาจากปัจจัยขั้นตอนที่ผ่านมา ได้แก่ โอกาสที่ภัยคุกคามที่เกิดขึ้นทำให้ระบบขาดความมั่นคง ระดับผลกระทบหรือความรุนแรงของภัยคุกคามที่มีต่อระบบและประสิทธิภาพ ของแผนการควบคุมความปลอดภัยของระบบ การวัดระดับความเสี่ยงมีการกำหนดแผนภูมิความเสี่ยงที่ได้จากการพิจารณาจัดระดับความสำคัญของความเสี่ยงจากโอกาสที่จะเกิดความเสี่ยงและผลกระทบที่เกิดขึ้นและขอบเขตของระดับความเสี่ยงที่สามารถยอมรับได้

ระดับความเสี่ยง = โอกาสที่จะเกิดหรือความถี่ x ความรุนแรงหรือผลกระทบ

ซึ่งเกณฑ์ในการจัดแบ่งระดับความเสี่ยงอาจจะแบ่งได้ตามตัวอย่างดังนี้

ระดับคะแนนความเสี่ยง	จัดระดับความเสี่ยง	กลยุทธ์ในการจัดการความเสี่ยง	พื้นที่สี
๑-๓	ต่ำ	ยอมรับความเสี่ยง	**ฟ้า**
๔-๗	ปานกลาง	ยอมรับความเสี่ยง (มีมาตรการติดตาม)	**เขียว**
๘-๑๔	สูง	ควบคุมความเสี่ยง (มีแผนควบคุมความเสี่ยง)	**เหลือง**
๑๕-๒๕	สูงมาก	ถ่ายโอนความเสี่ยง	**แดง**

๕.๒ การจัดการความเสี่ยง (Risk treatment)

ควรจัดให้มีแนวทางในการจัดการ ควบคุม และป้องกันความเสี่ยงด้านเทคโนโลยีสารสนเทศที่เหมาะสมและสอดคล้องกับผลการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ เพื่อให้ความเสี่ยง ที่เหลืออยู่ (residual risk) อยู่ในระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศที่ยอมรับได้ (IT risk appetite) โดยควรครอบคลุมอย่างน้อย ดังนี้

๑) กำหนดแนวทางในการจัดการและควบคุมความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยการเลือก แนวทางในการจัดการและควบคุมความเสี่ยงด้านเทคโนโลยีสารสนเทศ ควรพิจารณาถึง ความคุ้มค่าและวิธีการที่เหมาะสมสำหรับหน่วยงาน เช่น การหยุดหรือหลีกเลี่ยงความเสี่ยง การลดหรือบรรเทาโอกาสเกิดความเสี่ยง การลดหรือบรรเทาผลกระทบที่เกิดขึ้น การแบ่ง หรือโอนความเสี่ยงให้หน่วยงานอื่น การยอมรับความเสี่ยงไว้ โดยแจ้งเหตุผลให้ผู้บริหารทราบ เพื่อตัดสินใจในการยอมรับความเสี่ยง เป็นต้น

๒) ระบุรายละเอียดของงานที่ต้องดำเนินการ ผู้รับผิดชอบ ระยะเวลาที่ใช้ในการดำเนินการ

๓) ประเมินระดับค่าความเสี่ยงที่เหลืออยู่ (Residual risk) ว่าอยู่ในระดับความเสี่ยงที่ยอมรับได้

๔) จัดทำแผนการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยจัดลำดับความสำคัญในการดำเนินการ

๕) นำเสนอและขออนุมัติแผนการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ

๖) ดำเนินการสื่อสารแผนการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ นอกจากนี้ หน่วยงานควรจัดให้มีการกำหนดดัชนีชี้วัดความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT key risk indicators) ให้สอดคล้องกับความสำคัญของงานเทคโนโลยีสารสนเทศ แต่ละงานเพื่อใช้ติดตามและทบทวนความเสี่ยง

๕.๓ การติดตามและทบทวนความเสี่ยง (Risk monitoring and review)

การติดตามผลการดำเนินงาน การนำกลยุทธ์ มาตรการ หรือแนวทางมาใช้ปฏิบัติ เพื่อลดโอกาสที่เกิดความเสี่ยง หรือลดความเสียหายของผลที่อาจเกิดขึ้นจากความเสี่ยง ในระบบสารสนเทศของกกท. ที่ยังไม่มีกิจกรรมควบคุมความเสี่ยง หรือมีแต่ไม่เพียงพอ และนำมาวางแผนจัดการความเสี่ยง ทางเลือกในการ บริหารความเสี่ยงมีหลายวิธีซึ่งสามารถปรับเปลี่ยนหรือนำมาผสมผสานให้เหมาะสมกับสถานการณ์ อาจเป็น การยอมรับความเสี่ยง การลด/การควบคุมความเสี่ยง การกระจายความเสี่ยง หรือการหลีกเลี่ยงความเสี่ยง เมื่อองค์กรทราบความเสี่ยงที่ยังเหลืออยู่จากการประเมินความเสี่ยง และการประเมินการควบคุมแล้วให้ พิจารณาความเป็นไปได้และค่าใช้จ่ายแต่ละทางเลือก เพื่อตัดสินใจเลือกมาตรการลดความเสี่ยงที่เหมาะสมโดย พิจารณาจาก

๑) พิจารณาว่ายอมรับความเสี่ยง หรือจะกำหนดกิจกรรมควบคุมเพื่อลดความเสี่ยงให้อยู่ใน ระดับที่ยอมรับได้

๒) เปรียบเทียบค่าใช้จ่ายหรือต้นทุนในการจัดการให้มีมาตรการควบคุมกับผลประโยชน์ที่จะได้รับจากมาตรการดังกล่าวว่าคุ้มค่าหรือไม่

๓) กรณีเลือกกำหนดกิจกรรมควบคุมเพื่อลดความเสี่ยงให้กำหนดวิธีควบคุมในแผนบริหาร ความเสี่ยง

๔) ในรอบปีต่อไป ให้พิจารณาผลการติดต่อการบริหารความเสี่ยงก่อนที่ดำเนินการ มาบริหารความเสี่ยงตามกระบวนการเหล่านั้น หากพบว่ายังมีความเสี่ยงที่มีนัยสำคัญซึ่งอาจมีผลต่อระบบสารสนเทศการบรรลุวัตถุประสงค์และเป้าหมายตามแผนปฏิบัติงานขององค์กร ให้นำมาระบุการควบคุมในแผนบริหารความเสี่ยง ด้วยการรายงานผลการวิเคราะห์ประเมินและบริหารจัดการความเสี่ยง ว่ามีความเสี่ยงที่ยังเหลืออยู่หรือไม่ถ้าไม่มีเหลืออยู่ มีอยู่ในระดับความเสี่ยงสูงมากเพียงใด และมีวิธีการจัดการความเสี่ยงนั้นอย่างไรเสนอต่อผู้บริหารเพื่อทราบและสั่งการ

๕.๔ การรายงานความเสี่ยง (Risk reporting)

การรายงานผลการบริหารและจัดการความเสี่ยง (Reporting) หน่วยงานควรมีกระบวนการดังต่อไปนี้

- รายงานผลการประเมินความเสี่ยงที่มีผลต่อผู้ที่มีส่วนได้เสียที่เกี่ยวข้องทั้งหมดในรูปแบบที่สามารถนำไป ประกอบการตัดสินใจได้ เช่น ความเป็นไปได้ของผลประโยชน์ หรือการสูญเสียที่อาจเกิดเปรียบเทียบกับ ระดับความมั่นใจที่ผู้บริหารพิจารณาระหว่างความเสี่ยงและประโยชน์ที่อาจได้รับ

- นำเสนอข้อมูลที่เกี่ยวข้องกับผู้มีหน้าที่ตัดสินใจ โดยข้อมูลอาจรวมถึงเหตุการณ์ที่แย่หรือดีที่สุดที่อาจเกิดขึ้น การทำความเข้าใจผลกระทบ รวมทั้งพิจารณาถึงภาพลักษณ์ชื่อเสียง กฎหมาย และกฎระเบียบข้อบังคับต่าง ๆ ๑๔

- รายงานรายการความเสี่ยงในปัจจุบันให้กับผู้มีส่วนได้ส่วนเสีย รวมถึงรายงานผลการบริหารและจัดการ ความเสี่ยง ประสิทธิผลของการควบคุม ข้อตรวจพบ หรือข้อปรับปรุง รวมทั้งผลกระทบกับรายการความเสี่ยง

- สอบทานวัตถุประสงค์จากการตรวจสอบโดยผู้ตรวจสอบอิสระ ผู้ตรวจสอบภายในและการตรวจสอบ เพื่อวัดคุณภาพ โดยเชื่อมโยงกับรายการความเสี่ยงและพิจารณาถึงความเสี่ยงเพิ่มเติม

- ควรมีการสื่อสารเป็นประจำกับผู้ที่เกี่ยวข้องในเรื่องของความเสี่ยงและโอกาสทางด้านเทคโนโลยีสารสนเทศ เพื่อการพิจารณาถึงการพัฒนาหรือผลกำไรที่เพิ่มขึ้นจากการยอมรับความเสี่ยงทางด้านเทคโนโลยีสารสนเทศ ที่เพิ่มขึ้น

ภาคผนวก

ตารางที่ ๑ ระบุความเสี่ยงและผลกระทบด้านต่างๆ ที่จะเกิดขึ้น

กิจกรรม / กระบวนงาน : ระบบเทคโนโลยีสารสนเทศ ฝ่ายสารสนเทศและวิชาการกีฬา				
ที่มาความเสี่ยง /ปัจจัยเสี่ยง	**ผลกระทบด้านต่างๆ**			
	ชื่อเสียง	**เวลา**	**การบริการ**	**บุคลากร**
๑. ระบบงานและข้อมูล (System &Information) ทำงานไม่ได้ เสียหายหรือถูกทำลาย	- ถูกเจ้าหน้าที่ภายในกกท.วิจารณ์ - เจ้าหน้าที่ขาดความเชื่อมั่นในระบบเครือข่าย	- ทำให้เจ้าหน้าที่ในกกท. ไม่สามารถใช้ระบบงานและข้อมูลได้ - เสียเวลาในการกู้คืนระบบงานและข้อมูล	บุคลากรไม่สามารถใช้ระบบงานและข้อมูลในการปฏิบัติงาน และให้บริการ	- บุคลากรกกท.ถูกตำหนิ - เจ้าหน้าที่ดูแลระบบถูกตำหนิในเรื่องความสามารถในการดูแลระบบ
๒. ระบบให้บริการ Internet ล่ม	- ถูกเจ้าหน้าที่ภายในกกท.วิจารณ์ - เจ้าหน้าที่ขาดความเชื่อมั่นในระบบเครือข่าย	- ทำให้ระบบสารสนเทศต่างๆ ของกกกท.ไม่สามารถทำงานได้ - ทำให้ไม่สามารถรับส่งข้อมูลที่สำคัญในการปฏิบัติงานอิเล็คทรอนิกส์	- บุคลากรไม่สามารถใช้ระบบสารสนเทศในการปฏิบัติงาน - ประชาชนไม่สามารถใช้บริการผ่านระบบอินเตอร์เน็ต	เจ้าหน้าที่ดูแลระบบถูกตำหนิในเรื่องความสามารถในการดูแลระบบ
๓. เครื่อง Server ติดไวรัส	ถูกวิจารณ์ถึงประสิทธิภาพการทำงาน	ทำให้ระบบสารสนเทศทำงานได้ช้าหรือทำงานไม่ได้	เจ้าหน้าที่หน่วยงานต่างๆ ไม่สามารถทำงานได้	เจ้าหน้าที่ถูกตำหนิในเรื่องการดูแลความปลอดภัยของระบบ
๔. เครื่อง Client ติดไวรัส		เครื่องของเจ้าหน้าที่ทำงานไม่ได้ทำให้งานหยุดชะงัก	ทำให้เครื่องคอมพิวเตอร์บางเครื่องไม่สามารถให้บริการได้ตามปกติ	การดำเนินงานของเจ้าหน้าที่หยุดชะงักเสียเวลาในการจัดการกับไวรัส
๕. ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่	ถูกวิจารณ์ถึงประสิทธิภาพการทำงาน	การทำงานหยุดชะงัก	เครื่องแม่ข่ายคอมพิวเตอร์ ถูกปิดโดยไม่สมบูรณ์ อาจทำให้ข้อมูลสารสนเทศบางส่วนเกิดการสูญหายและการให้บริการบางประเภทไม่สามารถเปิดใช้งานได้โดยอัตโนมัติ	
๖. ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน - ไฟไหม้ จากอุบัติเหตุไฟฟ้าลัดวงจร การวางเพลิง - ภัยธรรมชาติ		ทำให้ระบบเสียหาย การทำงานหยุดชะงักและต้องใช้เวลาในการกู้คืนและปรับปรุงระบบนาน	ระบบคอมพิวเตอร์และระบบเครือข่ายหลักได้รับความเสียหาย ต้องดำเนินการตัดกระแสไฟฟ้าและไม่สามารถใช้งานระบบคอมพิวเตอร์และระบบเครือข่ายหลักได้	
๗. ความเสี่ยงจากสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง		ต้องใช้เวลาในการดำเนินงานและปรับปรุงระบบในช่วงเวลาที่ไม่สามารถดำเนินการได้	บุคลากรไม่สามารถปฏิบัติงานและให้บริการได้ตามปกติ	บุคลากรไม่สามารถปฏิบัติงานได้ตามปกติ