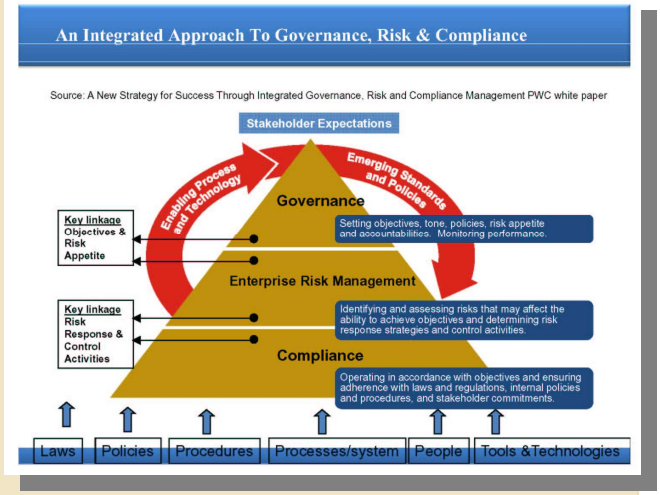
การกำกับดูแลกิจการที่ดี

“GRC กับการรักษาความปลอดภัยข้อมูลองค์กรในยุคโลกาภิวัตน์”

โดย : กลุ่มงานธรรมาภิบาล กฟผ.
สำนักผู้ว่าการ



โลกในยุคโลกาภิวัตน์หรือโลกไร้พรหมแดน ซึ่งเป็นผลจากการพัฒนาการติดต่อสื่อสาร การคมนาคมขนส่ง และเทคโนโลยีสารสนเทศ โดยเฉพาะองค์กรธุรกิจในปัจจุบันต่างก็เห็นความสำคัญของการรักษาความปลอดภัยด้านไอทีให้พ้นจากภัยคุกคามระบบคอมพิวเตอร์ทุกรูปแบบ การโจมตีทางไซเบอร์ที่รู้จักกันดี รวมถึงการละเมิดความปลอดภัยที่เป็นเรื่องเป็นราวปรากฏเป็นข่าวในหนังสือพิมพ์รายวัน ซึ่งสถานการณ์นี้ยังคงเกิดขึ้นอยู่เป็นประจำในปัจจุบัน สร้างความกังวลให้แก่องค์กรธุรกิจปัจจุบันอย่างมาก

หลายคนอาจจะยังไม่เคยได้ยินศัพท์คำว่า "GRC" ซึ่งย่อมาจาก "Governance Risk and Compliance" แนวคิด "GRC" นั้นเป็นแนวคิดใหม่ที่รวมองค์ประกอบ ๓ องค์ประกอบเข้าด้วยกัน ได้แก่ องค์ประกอบที่ ๑ "Governance" องค์ประกอบที่ ๒ "Risk Management" และ องค์ประกอบที่ ๓ "Regulatory Compliance" การกำหนดนิยามของคำว่า "GRC" นั้น มาจากนิยามของทั้งสามองค์ประกอบ ได้แก่

"Governance" หมายถึง นโยบาย วัฒนธรรมองค์กร กระบวนการขั้นตอนการปฏิบัติงาน ที่ถูกกำหนดออกมาอย่างชัดเจนในการบริหารจัดการและกำกับดูแลองค์กรโดยผู้บริหารระดับสูงเพื่อการบริหารองค์กรที่โปร่งใสตรวจสอบได้

"Risk Management" หมายถึง การบริหารจัดการความเสี่ยงที่มีเป้าหมายในการลดผลกระทบจากความเสี่ยงที่อาจมีโอกาสเกิดขึ้นได้ในองค์กร หากไม่มีการบริหารจัดการความเสี่ยงที่ดีพอ

"Compliance" หมายถึง การปฏิบัติตามกฎระเบียบข้อบังคับ และ กฎหมาย ตลอดจนการปฏิบัติตามนโยบายด้านสารสนเทศและความปลอดภัยขององค์กรอย่างถูกต้อง ได้ตามมาตรฐาน ยกตัวอย่าง เช่น การปฏิบัติตามประกาศมาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมอิเล็คทรอนิกส์ โดยคณะกรรมการธุรกรรมอิเล็คทรอนิกส์ และการจัดทำแผนเพื่อรองรับ พ.ร.บ. และ พ.ร.ฎ. ด้านความปลอดภัยทางอิเล็คทรอนิกส์ ได้แก่ พ.ร.บ. ว่าด้วยธุรกรรมทางอิเล็คทรอนิกส์ พ.ศ. ๒๕๔๔ พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็คทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ (มาตรา ๓๕) (ร่าง) พ.ร.ฎ. กำหนดวิธีการแบบ (มั่นคง) ปลอดภัยในการประกอบธุรกรรมอิเล็คทรอนิกส์ (มาตรา ๒๕) ซึ่งเป็นข้อแนะนำของสำนักงานคณะกรรมการนโยบายรัฐวิสาหกิจ และบริษัทไทยเรทติ้ง แอนด์ อินฟอร์เมชั่นเซอร์วิส จำกัด (ทริส)

สำหรับ บริษัทมหาชนในยุคโลกาภิวัตน์ การกำกับดูแลองค์กร การบริหารจัดการความเสี่ยง และการปฏิบัติตามกฎระเบียบ (Governance, Risk and Compliance - GRC) จะมีความหมายครอบคลุมคำเหล่านี้ได้แก่ “Corporate Governance”, “IT Governance”, “Financial Risk”, “Strategic Risk”, “Operational”, “IT Risk”, “Corporate Compliance”, “Employment/Labor Compliance”, “Privacy Compliance” รวมถึงต้องปฏิบัติตามกฎหมาย ข้อกำหนด และกฎหมายการแจ้งให้ทราบเกี่ยวกับการละเมิดความปลอดภัยของข้อมูลและความเป็นส่วนตัวของข้อมูลภายในประเทศอื่นๆ ด้วย เช่น กฎหมายเพื่อป้องกันปัญหาด้านบัญชีการเงินที่ผิดพลาดและฉ้อโกงภายในให้กับผู้ถือหุ้น SOX (Sarbanes-Oxley Act) องค์กรสาธารณสุขต้องปฏิบัติตาม HIPAA (Health Information Technology for Economic and Clinical Health) มาตรฐานใช้บังคับกับกลุ่มบริษัท PCI DSS ที่ให้บริการด้านบัตรเครดิต เช่น Visa, Master (Payment Card Industry Data Security Standard) สถาบันบริการทางการเงินต้องปฏิบัติตามข้อกำหนด GLBA (Gramm-Leach-Bliley Act) และ กฎระเบียบข้อบังคับ BASEL II ที่ถูกกำหนดขึ้นโดยธนาคารเพื่อการชำระบัญชีระหว่างประเทศ เหล่านี้เป็นกฎระเบียบมาตรฐานทั่วไปที่มีอยู่

กฎระเบียบดังกล่าวมีเพื่อป้องกันลูกค้า พนักงาน คู่ค้า หรือนักลงทุนจากการหลอกลวงและการขโมยข้อมูลเฉพาะตัว แต่สำหรับองค์กรต่างๆ แล้ว สิ่งเหล่านี้ได้สร้างภาระอันยิ่งใหญ่ให้แก่พนักงานไอทีและก่อให้เกิดการใช้งบประมาณด้านการรักษาความปลอดภัยที่เพิ่มขึ้น ตัวอย่างเช่น องค์กรที่อยู่ในประเทศที่บังคับใช้กฎหมาย การเปิดเผยการละเมิดข้อมูลต่างๆ มีแนวโน้มที่จะจ่ายเงินไปกับการรักษาความปลอดภัยข้อมูลมากกว่าในประเทศที่ไม่มีกฎหมายดังกล่าว

จากการสำรวจของอินฟอร์เมชั่นวีคในปี ๒๕๕๔ พบว่าการปฏิบัติงานตามกฎระเบียบของรัฐบาลและอุตสาหกรรม เป็นปัจจัยที่มีอิทธพลอย่างมากต่อโปรแกรมรักษาความปลอดภัยในปัจจุบัน เนื่องจากบริษัทเริ่มหันมาแปรรูปศูนย์ข้อมูลและสภาพแวดล้อมไอทีของตนให้เป็นระบบเสมือนจริงมากขึ้น ดังนั้น ระดับความซับซ้อนของการรักษาความปลอดภัยจึงเพิ่มขึ้นอย่างต่อเนื่อง

ในปัจจุบันการบริหารจัดการความปลอดภัยระบบสารสานเทศของ กฟผ. ใช้ข้อกำหนด กฟผ.ที่ ๖๒/๒๕๕๑ ว่าด้วยการักษาความมั่นคงปลอดภัยด้านสารสนเทศ ซึ่งข้อกำหนดดังกล่าวสอดคล้อง กับกฎหมาย ข้อกำหนดภาครัฐและมาตรฐานความมั่นคงปลอดภัย ISO ๒๗๐๐๑ อย่างไรก็ตาม ความพยายามจัดการกับปัญหาด้านความปลอดภัยที่หลากหลาย จำเป็นต้องมีการวิเคราะห์ความเสี่ยง ผลตอบแทนการลงทุนที่เหมาะสม และช่วยสร้างโครงสร้างพื้นฐานที่ยืดหยุ่นและปรับขยายได้ อีกทั้งยังจะต้องสามารถปรับเปลี่ยนได้เมื่อองค์กรเกิดการเปลี่ยนแปลงด้วย

เรียบเรียงจาก : วารสารไฟฟ้าและอุตสาหกรรม ปีที่ ๑๘ ฉบับที่ ๓ พฤษภาคม – มิถุนายน ๒๕๕๔,
บทความไอที เรื่อง พร้อมรับมือปี ๒๕๕๔ กันแล้วหรือยัง?

กลุ่มงานธรรมาภิบาล กฟผ. สำนักผู้ว่าการ โทรศัพท์ ๖๓๑๒๐ โทรสาร ๖๓๑๙๓