แนวทางการตรวจสอบ
ธรรมาภิบาล
ด้านเทคโนโลยีสารสนเทศ
(IT Governance)

คำนำ

ธรรมาภิบาลด้านเทคโนโลยีสารสนเทศเป็นส่วนหนึ่งของธรรมาภิบาลขององค์กร มีจุดมุ่งหมายเพื่อทำให้แน่ใจว่าองค์กรสามารถบรรลุเป้าหมายทางธุรกิจได้ โดยมีการใช้เทคโนโลยีสารสนเทศเป็นเครื่องมือสนับสนุน และสามารถจัดการกับความเสี่ยงที่อาจเกิดขึ้นจากเทคโนโลยีสารสนเทศได้อย่างมีประสิทธิภาพ

คู่มือการตรวจสอบธรรมาภิบาลด้านเทคโนโลยีสารสนเทศฉบับนี้จัดทำขึ้นเพื่อให้ผู้ตรวจสอบของสายกำกับสถาบันการเงินใช้เป็นแนวทางในการตรวจสอบและประเมินการบริหารจัดการงานด้านเทคโนโลยีสารสนเทศของสถาบันการเงิน (สง.) โดยศึกษาแนวทาง Board Briefing on IT Governance : Second Edition 2003 ที่จัดทำโดยสถาบันธรรมาภิบาลด้านเทคโนโลยีสารสนเทศ(IT Governance Institute) ซึ่งเป็นสถาบันที่จัดตั้งขึ้นเมื่อปี ค.ศ. 1998 โดยสมาคมผู้ตรวจสอบและควบคุมระบบสารสนเทศ (Information Systems Audit and Control Association - ISACA) ในประเทศสหรัฐอเมริกา เพื่อเสริมสร้างความเข้าใจเกี่ยวกับหลักธรรมาภิบาลด้านเทคโนโลยีสารสนเทศในองค์กรต่าง ๆ

ฝ่ายตรวจสอบความเสี่ยงและเทคโนโลยีสารสนเทศ หวังว่าแนวทางการตรวจสอบในคู่มือฉบับนี้จะเป็นประโยชน์และช่วยพัฒนางานตรวจสอบให้มีประสิทธิภาพต่อไป

ฝ่ายตรวจสอบความเสี่ยงและเทคโนโลยีสารสนเทศ

ธันวาคม 2551

สารบัญ

หน้าที่

บทนำ		1
ส่วนที่ 1	**ความหมายและความสำคัญของธรรมาภิบาลด้านเทคโนโลยีสารสนเทศ**	2
	ความหมาย	2
	ความสำคัญ	2
ส่วนที่ 2	**แนวทางปฏิบัติเกี่ยวกับธรรมาภิบาลด้านเทคโนโลยีสารสนเทศ**	6
	บทบาทหน้าที่ของคณะกรรมการ สง. และผู้บริหารระดับสูง	6
	แนวทางปฏิบัติของคณะกรรมการ สง.	7
	แนวทางปฏิบัติของผู้บริหารระดับสูง	9
	ขอบเขตของธรรมาภิบาลด้านเทคโนโลยีสารสนเทศ	10
ส่วนที่ 3	**แนวทางการตรวจสอบธรรมาภิบาลด้านเทคโนโลยีสารสนเทศ**	15
	วัตถุประสงค์การตรวจสอบ	15
	ขอบเขตการตรวจสอบ	15
	กระบวนการตรวจสอบ	15
	แนวทางการเขียนรายงานการตรวจสอบ	16
	แนวทางการตรวจสอบ	17

บทนำ

การบริหารจัดการด้านเทคโนโลยีสารสนเทศอย่างมีประสิทธิภาพเป็นปัจจัยสำคัญต่อความอยู่รอดและความสำเร็จของสถาบันการเงิน เนื่องจากสภาพการแข่งขันของสถาบันการเงินและการเปลี่ยนแปลงอย่างรวดเร็วของสภาพแวดล้อมในปัจจุบัน การดำเนินงานของสถาบันการเงินต้องอาศัยข้อมูลและระบบเทคโนโลยีสารสนเทศเพื่อเพิ่มศักยภาพในการประกอบธุรกิจมากขึ้น เนื่องจากการลงทุนด้านเทคโนโลยีมีจำนวนสูงและความเสี่ยงด้านเทคโนโลยีสารสนเทศที่เพิ่มขึ้น นอกจากนี้ ผู้บริหารมีความคาดหวังอย่างสูงต่อประโยชน์ที่จะได้รับจากการนำระบบเทคโนโลยีมาใช้งาน ทั้งในด้านการเพิ่มคุณภาพของข้อมูล ความสะดวกในการใช้งาน รวมทั้ง การให้บริการที่ดีและมีประสิทธิภาพยิ่งขึ้น

เนื่องจากเทคโนโลยีสารสนเทศช่วยสร้างโอกาสในการทำธุรกิจและเพิ่มศักยภาพการดำเนินงาน สามารถให้คุณค่าทางธุรกิจ เช่น การให้บริการและวิธีการแก้ปัญหาที่รวดเร็วและมีคุณภาพ ในขณะเดียวกันก็มีความเสี่ยงด้วย ดังนั้น คณะกรรมการและผู้บริหารสถาบันการเงินจึงต้องทราบถึงบทบาทและผลกระทบของเทคโนโลยีสารสนเทศที่มีต่อสถาบันการเงินและตระหนักถึงความสำคัญของเทคโนโลยีสารสนเทศที่มีต่อกลยุทธ์ขององค์กร และการรักษาความสมดุลระหว่างต้นทุนที่ใช้ในเทคโนโลยีสารสนเทศกับคุณค่าที่ได้รับจากข้อมูลสารสนเทศเพื่อให้ได้ผลตอบแทนที่เหมาะสมจากเงินลงทุนในเทคโนโลยีสารสนเทศ ตลอดจนการทำความเข้าใจความเสี่ยงและกำหนดแนวทางการบริหารจัดการความเสี่ยงที่เกี่ยวข้องกับการนำเทคโนโลยีสารสนเทศมาใช้ด้วย

ธรรมาภิบาลด้านเทคโนโลยีสารสนเทศเป็นส่วนหนึ่งของธรรมาภิบาลองค์กรหรือการกำกับดูแลกิจการที่ดี ซึ่งเป็นหน้าที่และความรับผิดชอบของคณะกรรมการและผู้บริหารระดับสูงของสถาบันการเงิน ในการกำหนดกลยุทธ์ วัตถุประสงค์ วัฒนธรรม จริยธรรม การบริหารจัดการมาตรฐานในการปฏิบัติงานภายในองค์กร รวมทั้งการบริหารความเสี่ยงอย่างเหมาะสมเพื่อดำเนินธุรกิจให้มีความมั่นคงปลอดภัยและเป็นไปตามกฎหมาย กฎเกณฑ์และระเบียบที่เกี่ยวข้อง โดยมีการกำกับควบคุมให้การดำเนินงานด้านเทคโนโลยีสารสนเทศเป็นไปตามแนวทางการปฏิบัติที่ดี เพื่อประโยชน์ของผู้มีส่วนได้ส่วนเสียและผู้ที่เกี่ยวข้องกับองค์กร

ส่วนที่ 1 ความหมายและความสำคัญของธรรมาภิบาลด้านเทคโนโลยีสารสนเทศ

1. ความหมาย

ธรรมาภิบาลด้านเทคโนโลยีสารสนเทศหรือการกำกับดูแลที่ดีด้านเทคโนโลยีสารสนเทศ เป็นหน้าที่และความรับผิดชอบของคณะกรรมการ สง. และผู้บริหารระดับสูง ในการจัดให้มีโครงสร้างของความสัมพันธ์และกระบวนการของการกำกับและการควบคุมเพื่อให้องค์กรบรรลุเป้าหมาย โดยการเพิ่มมูลค่าให้องค์กรไปพร้อมกับการรักษาสมดุลระหว่างความเสี่ยงกับผลตอบแทนจากเทคโนโลยีสารสนเทศและกระบวนการที่เกี่ยวข้องเพื่อให้มั่นใจได้ว่ามีการปรับปรุงประสิทธิภาพและประสิทธิผลที่สามารถวัดได้

การบริหารงานด้านเทคโนโลยีสารสนเทศที่ดีควรจะมีการเชื่อมโยงระหว่างกระบวนการบริหารงานด้านเทคโนโลยีสารสนเทศ ทรัพยากรและข้อมูลที่มีประสิทธิภาพ เพื่อสนับสนุนนโยบาย กลยุทธ์ เป้าหมายขององค์กร และการบริหารความเสี่ยงที่เหมาะสม โดยมีการดำเนินการตามแนวทางการปฏิบัติที่ดีเกี่ยวกับการวางแผน การจัดองค์การ การจัดหา การนำระบบออกใช้งานจริง การส่งมอบและการสนับสนุน รวมทั้งการรายงานและการติดตามผลการดำเนินงาน เพื่อให้มั่นใจว่าเทคโนโลยีสารสนเทศที่นำมาใช้สามารถช่วยสนับสนุนกลยุทธ์และบรรลุวัตถุประสงค์ในเชิงธุรกิจ รวมทั้งช่วยสร้างศักยภาพในการแข่งขันและเพิ่มมูลค่าให้องค์กร

คณะกรรมการ สง. และผู้บริหารระดับสูงมีหน้าที่และความรับผิดชอบในการจัดให้มีกระบวนการจัดการและการปฏิบัติงานด้านเทคโนโลยีที่ดีในองค์กร รวมถึงการกำหนดกลยุทธ์การบริหารความเสี่ยง การส่งมอบมูลค่า และการควบคุมและประเมินผลงาน โดยคณะกรรมการและผู้บริหารระดับสูงของสถาบันการเงินจะต้องมีความเข้าใจและกำหนดหน้าที่และความรับผิดชอบให้ผู้ที่เกี่ยวข้องในการนำเทคโนโลยีสารสนเทศไปใช้กับกิจกรรมต่าง ๆ ขององค์กร รวมทั้งตัดสินใจลงทุนและกำหนดแนวทางการจัดการความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศไปใช้งานตลอดจน การควบคุมและการรักษาความปลอดภัยที่เหมาะสมด้วย

2. ความสำคัญ

เนื่องจากเทคโนโลยีสารสนเทศมีส่วนช่วยสนับสนุนและเพิ่มความสามารถในการแข่งขันและเพิ่มศักยภาพในการทำกำไรและบรรลุเป้าหมายขององค์กร แต่ก็ทำให้เกิดความเสี่ยง เช่น การหยุดชะงักของระบบเทคโนโลยีสารสนเทศและเครือข่ายอาจก่อให้เกิดความเสียหายอย่างมากต่อการดำเนินงานของสถาบันการเงิน ดังนั้น จึงจำเป็นต้องมีการควบคุมและระบบการบริหารจัดการความเสี่ยงที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศเพื่อให้บรรลุเป้าหมายขององค์กร และเพื่อให้แน่ใจได้

ว่าองค์กรสามารถบรรลุความคาดหวังในการนำเทคโนโลยีสารสนเทศมาใช้ปรับปรุงกระบวนการปฏิบัติงานและนำกลยุทธ์ที่จำเป็นต่อการขยายธุรกิจในอนาคตไปใช้ในทางปฏิบัติและสามารถลดความเสี่ยงด้านเทคโนโลยีสารสนเทศได้

วัตถุประสงค์ของธรรมาภิบาลด้านเทคโนโลยีสารสนเทศ มีดังนี้

(1) เพื่อให้การดำเนินงานด้านเทคโนโลยีสารสนเทศมีความสอดคล้องกับกลยุทธ์ขององค์กรและช่วยทำให้องค์กรได้รับประโยชน์ตามที่กำหนดไว้

(2) เพื่อนำเทคโนโลยีสารสนเทศมาใช้เพิ่มศักยภาพและโอกาสการแข่งขันให้แก่องค์กรและช่วยทำให้องค์กรได้รับผลตอบแทนสูงสุด

(3) การใช้ทรัพยากรด้านเทคโนโลยีสารสนเทศที่มีอยู่อย่างมีประสิทธิภาพ

(4) การบริหารจัดการความเสี่ยงที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศเป็นไปอย่างเหมาะสม

ธรรมาภิบาลด้านเทคโนโลยีสารสนเทศมีหลายระดับตามสายการบังคับบัญชา ไม่ว่าจะเป็นหัวหน้าทีมรายงานและรับคำสั่งมาจากผู้จัดการ ผู้จัดการรายงานต่อผู้บริหาร หรือผู้บริหารรายงานต่อคณะกรรมการ สง. กรณีรายงานแสดงถึงการปฏิบัติงานที่ไม่เป็นไปตามเป้าหมายที่กำหนดไว้ควรจะมีคำแนะนำแนวทางดำเนินการและได้รับความเห็นชอบจากผู้บริหารระดับสูงด้วย แนวทางปฏิบัติดังกล่าวนี้จะมีประสิทธิภาพได้จะต้องมีการสื่อสารถ่ายทอดกลยุทธ์และเป้าหมายลงไปในแต่ละระดับทั่วทั้งองค์กร

ขอบเขตของธรรมาภิบาลด้านเทคโนโลยีสารสนเทศ ครอบคลุมถึงประเด็นต่าง ๆ ที่คณะกรรมการ สง. และฝ่ายจัดการต้องพิจารณา และจัดให้เกิดขึ้นในองค์กร ได้แก่

(1) การผสมผสานกลยุทธ์ (Strategic Alignment)

(2) การเพิ่มคุณค่า (Value Delivery)

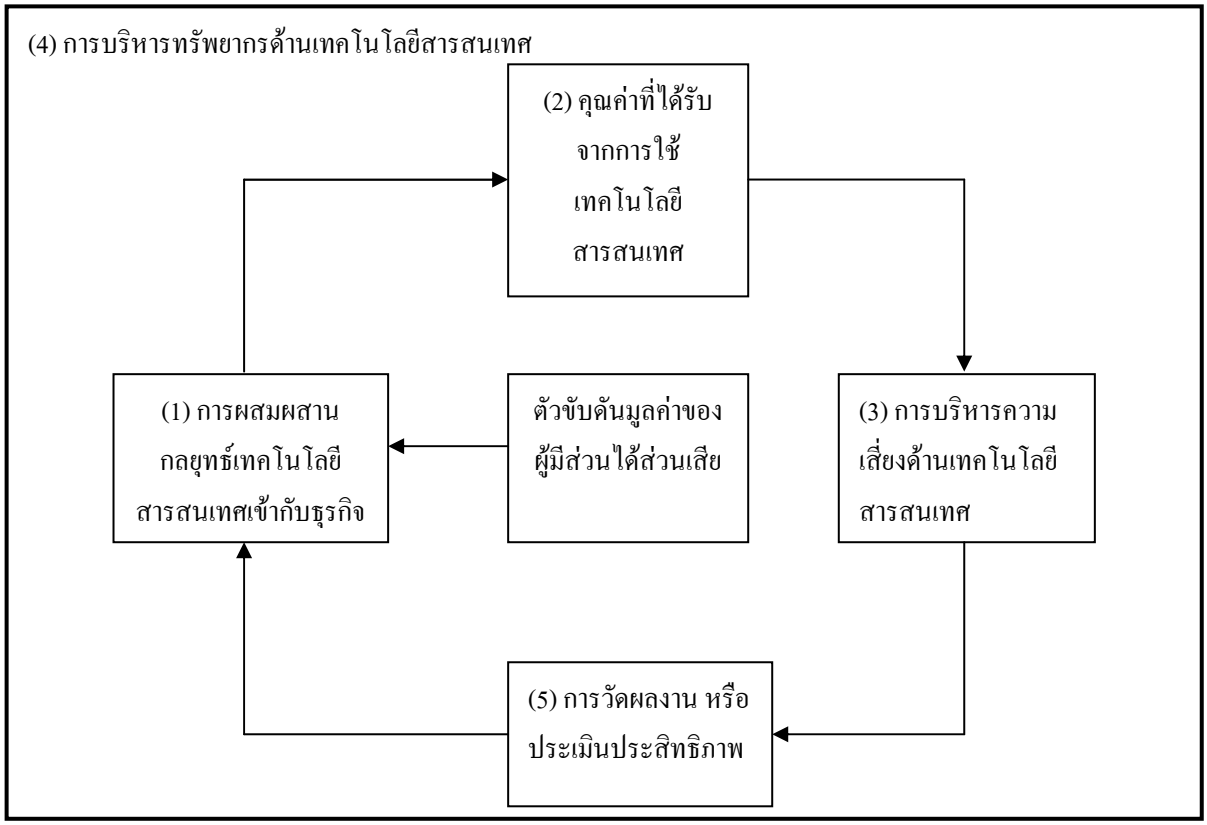
(3) การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk Management)

(4) การบริหารทรัพยากรด้านเทคโนโลยีสารสนเทศ (IT Resource Management)

(5) การวัดผลงานหรือประเมินประสิทธิภาพ (Performance Measurement)

รายละเอียดของขอบเขตของธรรมาภิบาลด้านเทคโนโลยีสารสนเทศ จะได้กล่าวถึงในส่วนที่ 2 แนวทางปฏิบัติเกี่ยวกับธรรมาภิบาลด้านเทคโนโลยีสารสนเทศ

แผนภาพขอบเขตของธรรมาภิบาลด้านเทคโนโลยีสารสนเทศ



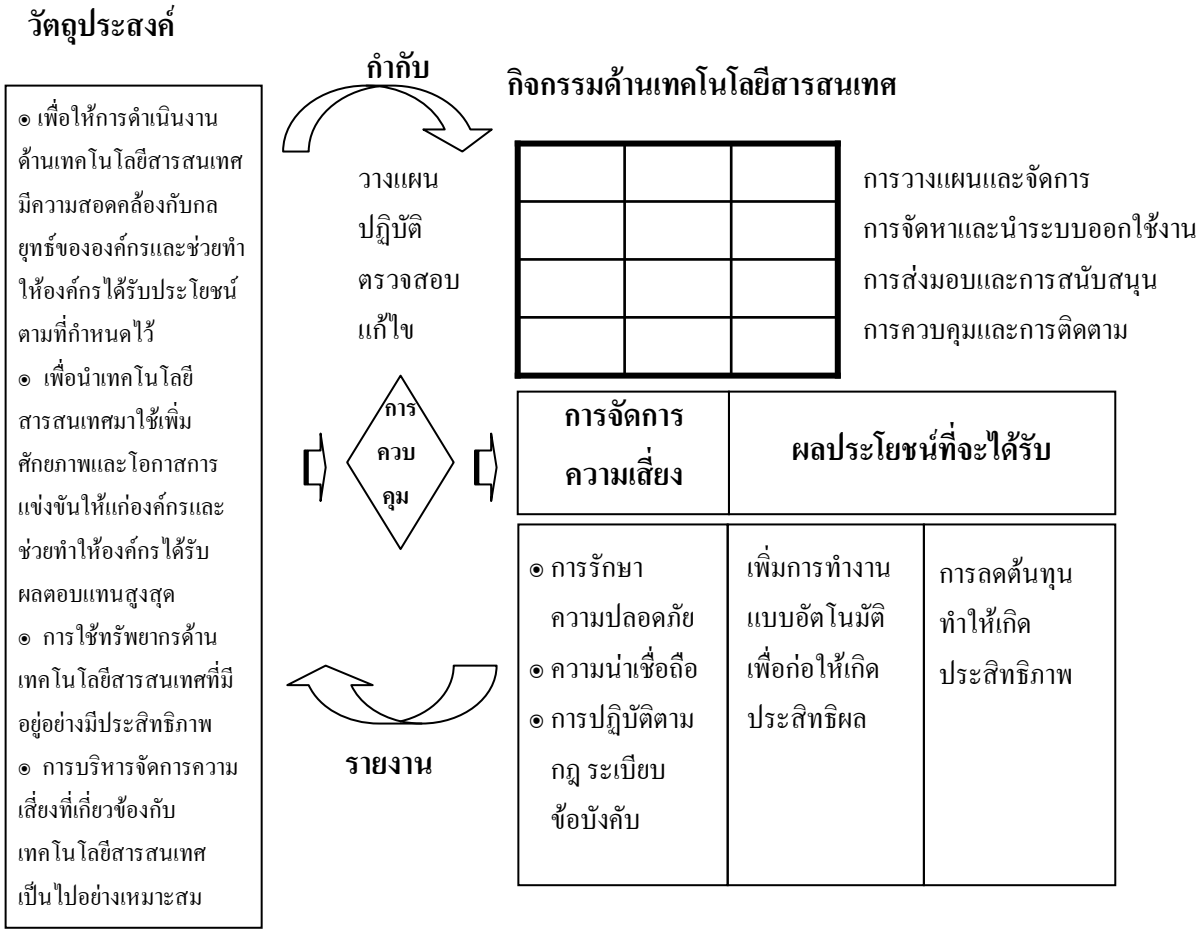
กระบวนการธรรมาภิบาลด้านเทคโนโลยีสารสนเทศ มีดังนี้

(1) การกำหนดวัตถุประสงค์ในการนำเทคโนโลยีสารสนเทศมาใช้

(2) กำหนดกิจกรรมด้านเทคโนโลยีสารสนเทศ ซึ่งเน้นการเพิ่มประสิทธิภาพการดำเนินงานโดยการใช้ระบบอัตโนมัติ และการลดค่าใช้จ่ายเพื่อเพิ่มประสิทธิผลขององค์กร รวมทั้งการบริหารจัดการความเสี่ยงทั้งในเรื่องของความมั่นคงปลอดภัย ความเชื่อถือได้ และการปฏิบัติตามกฎระเบียบข้อบังคับ รวมทั้งกฎเกณฑ์ของทางการด้วย

(3) การติดตามวัดผลงานโดยเปรียบเทียบกับวัตถุประสงค์ที่กำหนดไว้ ซึ่งอาจต้องมีการทบทวนหรือเปลี่ยนแปลงวัตถุประสงค์ของกิจกรรมตามความเหมาะสม

แผนภาพกระบวนการธรรมาภิบาลด้านเทคโนโลยีสารสนเทศ



ผู้บริหารจะต้องกำกับดูแลและจัดการกิจกรรมต่าง ๆ ด้านเทคโนโลยีสารสนเทศให้เกิดความสมดุลระหว่างการจัดการความเสี่ยงและผลประโยชน์ที่จะได้รับ เพื่อให้แน่ใจได้ว่าสามารถบรรลุวัตถุประสงค์ของธุรกิจ ดังนั้น ผู้บริหารจำเป็นต้องระบุกิจกรรมสำคัญที่ต้องดำเนินการ ต้องควบคุมติดตามวัดผลความก้าวหน้าการดำเนินงานเทียบกับเป้าหมาย

ส่วนที่ 2 แนวทางปฏิบัติเกี่ยวกับธรรมาภิบาลด้านเทคโนโลยีสารสนเทศ

1. บทบาทหน้าที่ของคณะกรรมการ สง. และผู้บริหารระดับสูง

คณะกรรมการ สง. และผู้บริหารระดับสูงมีหน้าที่และความรับผิดชอบในการกำกับดูแลที่ดีหรือสร้างธรรมาภิบาลด้านเทคโนโลยีสารสนเทศในองค์กร โดยการกำหนดกลยุทธ์ วัตถุประสงค์และทิศทางดำเนินงานด้านเทคโนโลยีสารสนเทศให้สอดคล้องกับกลยุทธ์ขององค์กร ตลอดจนการกำหนดแนวทางการควบคุมงานด้านเทคโนโลยีสารสนเทศ การประเมินวัดผลงานและการบริหารจัดการความเสี่ยงที่เกี่ยวข้องกับการนำเทคโนโลยีสารสนเทศมาใช้งาน แนวทางปฏิบัติที่ดีเกี่ยวกับธรรมาภิบาลด้านเทคโนโลยีสารสนเทศจะต้องมีการสื่อสารและนำมาใช้ปฏิบัติทั่วทั้งองค์กร โดยเฉพาะอย่างยิ่งระหว่างหน่วยงานด้านเทคโนโลยีสารสนเทศกับหน่วยงานด้านธุรกิจ ซึ่งต้องมีการประสานงานกันเพื่อให้เกิดความมั่นใจว่าองค์กรสามารถดำเนินธุรกิจได้ตามที่ตั้งเป้าหมายไว้

คณะกรรมการ สง. และผู้บริหารระดับสูงส่วนใหญ่จะให้ความสำคัญต่อกลยุทธ์และความเสี่ยงทางธุรกิจมากกว่าความเสี่ยงด้านเทคโนโลยีสารสนเทศ ดังนั้น คณะกรรมการ สง. และผู้บริหารระดับสูงสามารถจัดตั้งคณะกรรมการย่อยซึ่งมีความรู้ความเข้าใจเชิงเทคนิคเพื่อทำหน้าที่และรับผิดชอบการจัดการและกำกับดูแลงานด้านเทคโนโลยีสารสนเทศ การบริหารความเสี่ยงที่เกี่ยวข้องกับการนำเทคโนโลยีมาใช้ ดังนี้

1.1 คณะกรรมการกลยุทธ์ด้านเทคโนโลยีสารสนเทศ (IT Strategy Committee) เป็นคณะกรรมการที่มีความสำคัญในระดับเดียวกับคณะกรรมการ สง. ประกอบด้วยสมาชิกจากคณะกรรมการ สง. ผู้บริหารจากหน่วยงานด้านธุรกิจและหน่วยงานด้านเทคโนโลยีสารสนเทศ เพื่อทำหน้าที่และรับผิดชอบในการกำหนดและให้คำแนะนำกลยุทธ์ด้าน IT รวมทั้ง การกำกับดูแลและบริหารจัดการงานที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศเพื่อมุ่งเน้นการเพิ่มคุณค่าและประสิทธิภาพในการใช้เทคโนโลยีสารสนเทศ (IT Value and Performance) และการบริหารจัดการความเสี่ยงที่เกี่ยวข้อง (IT Risk) เพื่อให้มั่นใจว่าการใช้เทคโนโลยีสารสนเทศของ สง. มีประสิทธิภาพและมีส่วนสนับสนุนให้บรรลุกลยุทธ์และวัตถุประสงค์ขององค์กร

1.2 คณะกรรมการเทคโนโลยีสารสนเทศ (IT Steering Committee) เพื่อทำหน้าที่ดูแลติดตามการลงทุนด้านเทคโนโลยีสารสนเทศ กำหนดลำดับความสำคัญและจัดสรรทรัพยากรด้านเทคโนโลยีสารสนเทศ

1.3 คณะกรรมการตรวจสอบเพื่อทำหน้าที่กำกับดูแลให้สถาบันการเงินมีการตรวจสอบภายในด้านเทคโนโลยีสารสนเทศและมีระบบการควบคุมภายในที่เหมาะสม รวมทั้ง การสอบทานให้มีการปฏิบัติตามกฎระเบียบและกฎหมายที่เกี่ยวข้อง

1.4 คณะกรรมการบริหารความเสี่ยงมีหน้าที่กำหนดนโยบายการบริหารความเสี่ยงโดยรวมของสถาบันการเงินซึ่งต้องครอบคลุมความเสี่ยงประเภทต่างๆ ที่สำคัญ รวมถึงความเสี่ยงด้านเทคโนโลยีสารสนเทศ นอกจากนี้ ต้องมีการติดตาม ดูแลการบริหารจัดการความเสี่ยงของสถาบันการเงินให้อยู่ในระดับที่เหมาะสมและมีการปฏิบัติตามนโยบายที่กำหนดไว้ด้วย

2. แนวทางปฏิบัติของคณะกรรมการ สง. ควรดำเนินการ ดังนี้

2.1 กลยุทธ์ด้านเทคโนโลยีสารสนเทศ

2.1.1 กำหนดทิศทางของกลยุทธ์ด้านเทคโนโลยีสารสนเทศและผสมผสานกลยุทธ์ด้านเทคโนโลยีสารสนเทศเข้ากับกลยุทธ์ด้านธุรกิจและถ่ายทอดกลยุทธ์ด้านเทคโนโลยีสารสนเทศในองค์กรอย่างต่อเนื่องและเหมาะสมกับการปฏิบัติงานของหน่วยงานธุรกิจ

2.1.2 ใช้เทคโนโลยีสารสนเทศเพื่อช่วยปรับปรุงคุณภาพของการให้บริการและวัดผลการปฏิบัติงานว่าเป็นไปตามเป้าหมายที่กำหนดไว้

2.1.3 ตัดสินใจเกี่ยวกับการลงทุนและการจัดสรรทรัพยากรด้านเทคโนโลยีสารสนเทศ สร้างความสมดุลระหว่างระบบงานที่สนับสนุนองค์กรและการเปลี่ยนแปลงรูปแบบองค์กรหรือจัดโครงสร้างที่จะช่วยการขยายธุรกิจและการเข้าไปแข่งขันในธุรกิจใหม่ ๆ เพื่อเพิ่มรายได้ เพิ่มความพึงพอใจให้แก่ลูกค้าและการรักษาฐานลูกค้าไว้

2.1.4 ส่งเสริมวัฒนธรรมองค์กรให้มีการร่วมมือประสานงานระหว่างหน่วยงานต่าง ๆ

2.2 กำกับดูแลให้หน่วยงานเทคโนโลยีสารสนเทศเพื่อให้สามารถส่งมอบผลงานที่มีคุณค่าตามที่กำหนดไว้ในกลยุทธ์ เช่น ส่งมอบงานได้ตรงความต้องการและตรงเวลาภายในงบประมาณที่ตั้งไว้ ระบบสามารถใช้งานง่าย มีระบบการรักษาความปลอดภัย มีการวัดผลงานหรือประเมินประสิทธิภาพ และเสนอแนะแนวทางวิธีการแก้ไขปัญหาและการให้บริการที่มีคุณภาพ

2.2.1 ส่งเสริมให้องค์กรมีชื่อเสียง มีความเป็นผู้นำด้านผลิตภัณฑ์ และมีประสิทธิภาพในการบริหารและควบคุมต้นทุน

2.2.2 ทำให้ลูกค้ามีความเชื่อถือและองค์กรมีศักยภาพในการแข่งขันในตลาดได้

2.3 บริหารจัดการความเสี่ยงของ สง.

2.3.1 กำหนดนโยบายแนวทางดำเนินการและกระบวนการบริหารจัดการความเสี่ยงของ สง. โดยรวม ความเสี่ยงด้านเทคโนโลยีสารสนเทศ รวมถึงความเสี่ยงอื่นที่สำคัญในการปฏิบัติงาน โดยมีการกำหนดระดับของความเสี่ยงที่ยอมรับได้และแนวทางจัดการความเสี่ยง

2.3.2 คณะกรรมการ สง. มีหน้าที่และความรับผิดชอบในการบริหารความเสี่ยงของ สง. ในกรณีที่มีการมอบหมายหน้าที่ดังกล่าวให้ผู้บริหารดำเนินการ จะต้องมีการมอบหมายงานอย่างชัดเจนเป็นลายลักษณ์อักษรและมีกระบวนการรายงานคณะกรรมการ สง. ด้วย

2.3.3 กำหนดและสอบทานระบบการควบคุมภายในเพื่อการบริหารจัดการความเสี่ยง

2.3.4 กำหนดแนวทางการบริหารความเสี่ยงเชิงรุกและมีการมองไปล่วงหน้า (Proactive) เพื่อสร้างความได้เปรียบเชิงแข่งขัน

2.3.5 การปลูกฝังแนวคิดเรื่องการบริหารความเสี่ยงไว้ในการปฏิบัติงานขององค์กร ซึ่งทำให้องค์กรสามารถตอบสนองต่อความเสี่ยงที่เปลี่ยนแปลงไปได้อย่างรวดเร็ว และกำหนดหลักเกณฑ์การรายงานความเสี่ยง เช่น วิธีการรายงาน ประเภทของเหตุการณ์ที่ต้องรายงาน ผู้รายงาน ผู้รับรายงาน และระยะเวลาของการรายงาน

2.3.6 ดำเนินการให้ผู้บริหารนำกระบวนการเทคโนโลยีมาใช้และการสอบทานเกี่ยวกับความปลอดภัยทางเทคโนโลยีสารสนเทศเพื่อให้ธุรกรรมทางธุรกิจมีความน่าเชื่อถือ โดยจัดให้มีระบบป้องกันการบุกรุก ตลอดจนการป้องกันไม่ให้บุคคลที่ไม่ได้รับอนุญาตเข้าถึงข้อมูลสารสนเทศที่สำคัญ และกำหนดกระบวนการกู้ระบบกลับคืนหากมีปัญหาเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ

2.4 การบริหารจัดการทรัพยากรด้านเทคโนโลยีสารสนเทศอย่างมีประสิทธิภาพ

2.4.1 พิจารณาความเหมาะสมของการลงทุนในโครงสร้างและศักยภาพของระบบเทคโนโลยีสารสนเทศโดยคำนึงถึงพัฒนาการด้านเทคโนโลยีสารสนเทศเพื่อนำมาใช้ปรับปรุงประสิทธิภาพของสถาปัตยกรรมด้านเทคโนโลยีสารสนเทศ

2.4.2 การวางแผนและการลงทุนด้านกำลังคนเพื่อรักษาบุคลากรที่มีทักษะทางเทคโนโลยีสารสนเทศและการจัดหาบุคลากรทดแทน

2.4.3 การลงทุนเกี่ยวกับการให้ความรู้แก่บุคลากร การพัฒนาและการฝึกอบรมเพื่อการปฏิบัติงานและพัฒนาการด้านเทคโนโลยีสารสนเทศ รวมถึงความรู้และทักษะการบริหารงานโครงการและการให้บริการงานด้านเทคโนโลยีสารสนเทศ เพื่อนำไปใช้ในการปฏิบัติงาน รวมทั้งการสนับสนุนให้มีการเรียนรู้โดยการจัดหาอุปกรณ์เครื่องมือเครื่องใช้ที่เหมาะสมและให้พนักงานได้มีโอกาสพัฒนาทักษะที่จำเป็น

2.5 กำหนดให้มีการวัดผลงานหรือประสิทธิภาพ

2.5.1 กำหนดและติดตามการวัดผลงานเพื่อให้มั่นใจว่าสามารถบรรลุวัตถุประสงค์

2.5.2 สนับสนุนให้มีเครื่องมือเพื่อวัดผลงาน

3. แนวทางปฏิบัติของผู้บริหารระดับสูง

ผู้บริหารระดับสูงจะเน้นประสิทธิผลในการบริหาร การควบคุมต้นทุน การเพิ่มรายได้ และการสร้างศักยภาพขององค์กร ซึ่งจำเป็นต้องใช้ข้อมูลสารสนเทศ องค์ความรู้สถาปัตยกรรมด้านเทคโนโลยีสารสนเทศ เนื่องจากเทคโนโลยีสารสนเทศมีความซับซ้อนมากขึ้นทำให้การกำกับดูแลงานที่เหมาะสมเป็นปัจจัยสำคัญสู่ความสำเร็จ ผู้บริหารระดับสูงควรดำเนินการ ดังนี้

3.1 ถ่ายทอดกลยุทธ์ นโยบาย และเป้าหมายลงไปในองค์กร และผสมผสานโครงสร้างองค์กรของฝ่ายเทคโนโลยีสารสนเทศเข้ากับเป้าหมายขององค์กร

3.2 กำหนดโครงสร้างองค์กรที่สนับสนุนการนำกลยุทธ์ด้านเทคโนโลยีสารสนเทศมาใช้ในทางปฏิบัติเพื่อให้มีการเผยแพร่ข้อมูลข่าวสารทางธุรกิจมากขึ้น ซึ่งต้องอาศัยความร่วมมือกันระหว่างหน่วยงานธุรกิจและฝ่ายเทคโนโลยีสารสนเทศเพื่อให้การลงทุนทางเทคโนโลยีสารสนเทศประสบความสำเร็จทั้งทางด้านธุรกิจและทางเทคนิค ทั้งนี้ ผู้บริหารสูงสุดด้านสารสนเทศ (CIO) ต้องเป็นผู้ประสานระหว่างหน่วยงานทั้งสองและผู้บริหารสายงานธุรกิจจำเป็นต้องเข้ามามีส่วนร่วมในการตัดสินใจเกี่ยวกับเทคโนโลยีสารสนเทศ

3.3 ปลูกฝังหน้าที่และความรับผิดชอบเกี่ยวกับการบริหารความเสี่ยงและการควบคุมเทคโนโลยีสารสนเทศในองค์กร ให้เป็นไปตามนโยบายการบริหารความเสี่ยงที่ชัดเจน รวมทั้งกำหนดแนวทางการควบคุมที่ครอบคลุมความเสี่ยงที่เกิดขึ้น

3.4 จัดให้มีการวัดหรือประเมินผลงาน โดยกำหนดวิธีการวัดผลงานจากมูลค่าทางธุรกิจที่เกิดขึ้น เช่น การนำ KGI (Key Goal Indicators) และ KPI (Key Performance Indicators) มาใช้วัดผลงาน รวมทั้ง ความได้เปรียบในเชิงการแข่งขันที่เกิดจากการใช้เทคโนโลยีสารสนเทศเป็นตัวขับดันประสิทธิภาพและสร้างประโยชน์ให้แก่องค์กร ซึ่งควรใช้ตัววัดที่แม่นยำเพียงไม่กี่ตัวและเชื่อมโยงโดยตรงกับกลยุทธ์ที่กำหนดไว้

3.5 มุ่งเน้นไปที่ศักยภาพในการแข่งขันของธุรกิจหลักที่ต้องใช้เทคโนโลยีสารสนเทศสนับสนุนเพื่อเพิ่มคุณค่าสินค้าและบริการให้แก่ลูกค้า ทำให้ผลิตภัณฑ์และบริการมีความแตกต่างไปจากคู่แข่ง

3.6 ให้ความสำคัญต่อกระบวนการเทคโนโลยีสารสนเทศเพื่อช่วยเพิ่มมูลค่าให้แก่ธุรกิจ เช่น การบริหารการเปลี่ยนแปลง การจัดการโปรแกรมระบบงานต่าง ๆ และการแก้ไขปัญหาที่เกิดขึ้น ผู้บริหารอาจต้องเข้ามามีส่วนร่วมโดยตรงในการกำหนดกระบวนการเหล่านี้ ตลอดจนกำหนดให้มีผู้มีหน้าที่รับผิดชอบดำเนินการตามกระบวนการดังกล่าว

3.7 สร้างองค์กรที่มีความยืดหยุ่นและสามารถปรับตัวทันเหตุการณ์ เป็นองค์กรแห่ง

การเรียนรู้โดยใช้เทคโนโลยีสารสนเทศในการรวบรวมข้อมูลสารสนเทศ ความรู้และประสบการณ์ที่มีอยู่แล้วนำมาใช้ประโยชน์โดยการสร้างสรรค์ผลิตภัณฑ์ บริการ ช่องทางการจำหน่าย และกระบวนการใหม่ ๆ

3.8 เสริมสร้างการส่งมอบงานที่มีคุณค่า ด้วยการกำหนดมาตรฐานของเทคโนโลยี เช่น การจัดตั้งคณะกรรมการทบทวนเทคโนโลยีและสถาปัตยกรรมที่นำมาใช้ รวมทั้งกำหนดให้มีการควบคุมการบริหารโครงการให้ได้ตามมาตรฐานที่กำหนด เพื่อให้ได้งานที่มีคุณค่าต่อองค์กรสูงสุด

3.9 ให้ความสำคัญต่อการบริหารต้นทุนและค่าใช้จ่ายด้านเทคโนโลยีสารสนเทศอย่างเหมาะสม เพื่อให้องค์กรได้รับคุณค่าที่แท้จริงจากทรัพยากรด้านเทคโนโลยีสารสนเทศ โดยมีต้นทุนที่สมเหตุสมผล

3.10 กำหนดให้มีกลยุทธ์และระเบียบปฏิบัติที่ชัดเจนในการจัดหาทรัพยากรหรือการใช้บริการด้านเทคโนโลยีสารสนเทศจากภายนอก รวมทั้งการจัดการสัญญากับบุคคลภายนอกและข้อตกลงการให้บริการ (Service Level Agreement - SLA) เพื่อสนองความต้องการขององค์กร ซึ่งจำเป็นต้องนำแนวทางปฏิบัติเกี่ยวกับการควบคุมและกำกับดูแลด้านเทคโนโลยีสารสนเทศมาใช้

4. ขอบเขตของธรรมาภิบาลด้านเทคโนโลยีสารสนเทศ

ธรรมาภิบาลด้านเทคโนโลยีสารสนเทศเกี่ยวข้องกับปัจจัยพื้นฐาน 2 ประการ

4.1 การใช้เทคโนโลยีสารสนเทศสร้างมูลค่าเพิ่มให้แก่ธุรกิจ ซึ่งต้องขับเคลื่อนกลยุทธ์ด้านเทคโนโลยีสารสนเทศควบคู่ไปพร้อมกับกลยุทธ์ด้านธุรกิจ

4.2 การควบคุมความเสี่ยงด้านเทคโนโลยีสารสนเทศ ซึ่งต้องปลูกฝังให้เป็นหน้าที่และความรับผิดชอบของทุกคนในองค์กร

ธรรมาภิบาลด้านเทคโนโลยีสารสนเทศเป็นกระบวนการที่เกิดขึ้นอย่างต่อเนื่อง เป็นวัฏจักรเริ่มต้นด้วยการกำหนดกลยุทธ์ด้านเทคโนโลยีให้สอดคล้องกับกลยุทธ์ทางธุรกิจขององค์กร แล้วถ่ายทอดกลยุทธ์ไปใช้ทั่วทั้งองค์กร การนำกลยุทธ์ไปใช้ในทางปฏิบัติ โดยใช้ทรัพยากรเท่าที่จำเป็นเพื่อการปฏิบัติงานตามที่ได้รับมอบหมายอย่างมีประสิทธิภาพ มีการติดตามทบทวนกลยุทธ์ที่ตั้งไว้ โดยมีการวัดประสิทธิภาพ มีการวัดผลงานหรือประเมินประสิทธิภาพและความสำเร็จของงาน การรายงานผลและดำเนินการแก้ไข การกำหนดแนวทางการลดความเสี่ยงและระดับของความเสี่ยงที่ยอมรับได้ รายงานผลการปฏิบัติงานที่เกิดขึ้นจะแสดงให้เห็นว่าสามารถนำแผนกลยุทธ์ไปใช้ได้ในทางปฏิบัติ หรือแสดงให้เห็นว่าอาจต้องมีการปรับทิศทางของแผนกลยุทธ์ โดยปกติองค์กรควรประเมินกลยุทธ์ทุกปีและการปรับกลยุทธ์ใหม่หากจำเป็น

ธรรมาภิบาลด้านเทคโนโลยีสารสนเทศ ครอบคลุมเกี่ยวกับ 5 เรื่อง ดังนี้

(1) การผสมผสานกลยุทธ์ (Strategic Alignment)

การนำเทคโนโลยีสารสนเทศมาใช้ในการเพิ่มประสิทธิภาพการบริหารจัดการ รวมทั้ง เพิ่มมูลค่าและศักยภาพการแข่งขันทางธุรกิจ การลงทุนในเทคโนโลยีสารสนเทศของ สง. ควรมีความสอดคล้องกันกับวัตถุประสงค์เชิงกลยุทธ์ขององค์กรเพื่อสร้างศักยภาพที่จำเป็นต่อการสร้างผลตอบแทนทางธุรกิจให้องค์กร และต้องปฏิบัติงานด้านเทคโนโลยีสารสนเทศให้เข้ากับการปฏิบัติงานในปัจจุบันด้วย

แผนงานเพื่อดำเนินกลยุทธ์จะต้องได้รับความเห็นชอบจากผู้ที่เกี่ยวข้องทั้งหมด แผนงานย่อยต้องมีความชัดเจนระบุผลที่จะเกิดขึ้นต่อธุรกิจและผลตอบแทนที่ได้รับ คณะกรรมการ สง. จะต้องมีการทบทวนแผนกลยุทธ์ ทั้งในเชิงเทคนิคและการเปลี่ยนแปลงกระบวนการปฏิบัติงานให้เหมาะสม การกำหนดกลยุทธ์ด้านเทคโนโลยีสารสนเทศควรพิจารณา ดังนี้

(1.1) วัตถุประสงค์ทางธุรกิจ และสภาพแวดล้อมในการแข่งขัน

(1.2) เทคโนโลยีในปัจจุบันและอนาคต ตลอดจนต้นทุน ความเสี่ยงและผลตอบแทนที่หน่วยงานธุรกิจจะได้รับจากเทคโนโลยีดังกล่าว

(1.3) ความสามารถของหน่วยงานเทคโนโลยีสารสนเทศในการให้บริการแก่หน่วยงานธุรกิจทั้งในปัจจุบันและอนาคต ขอบเขตของการลงทุนและการเปลี่ยนแปลงที่มีผลกับทั้งองค์กร

(1.4) ประสบการณ์ความล้มเหลวและความสำเร็จในอดีต

(2) การเพิ่มคุณค่า (Value Delivery)

คุณค่าของเทคโนโลยีสารสนเทศ หมายถึง การส่งมอบงานที่มีคุณภาพได้ตรงตามความต้องการ ตรงเวลา มีค่าใช้จ่ายที่เหมาะสมและอยู่ในงบประมาณที่กำหนด มีการปรับเปลี่ยนกระบวนการปฏิบัติงานให้มีประสิทธิภาพ เช่น การให้บริการแก่ลูกค้าสะดวกรวดเร็วขึ้น เพิ่มความพึงพอใจของลูกค้า การเพิ่มผลผลิตและกำไรขององค์กรและช่วยลดขั้นตอนการปฏิบัติงานของพนักงาน เป็นต้น หน่วยงานเทคโนโลยีสารสนเทศและหน่วยงานธุรกิจต้องมีการประสานงานกัน และกำหนดความหมายของคำว่า “คุณค่า” ที่ต้องการได้รับจากการนำเทคโนโลยีมาใช้ให้ตรงกัน ซึ่งผลงานที่มีคุณค่าควรมีลักษณะ ดังนี้

(2.1) ผลงานถูกต้องตรงตามความต้องการของหน่วยธุรกิจและสอดคล้องกับวัตถุประสงค์ขององค์กร

(2.2) มีความยืดหยุ่นสามารถปรับเปลี่ยนให้เข้ากับความต้องการของธุรกิจในอนาคต

(2.3) มีระยะเวลาในการปฏิบัติงานเป็นไปตามที่กำหนด

(2.4) การใช้งานง่าย ทนทานและกู้กลับคืนได้ง่ายเมื่อเกิดปัญหา รวมทั้งมีความปลอดภัย

(2.5) ข้อมูลสารสนเทศมีความถูกต้องเชื่อถือได้ แม่นยำ ทันกาล มีประโยชน์ สามารถนำไปใช้งานและเป็นที่ยอมรับ

(3) การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk Management)

การบริหารความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ จะเน้นการเก็บรักษาสินทรัพย์ด้านเทคโนโลยีสารสนเทศ การรักษาความปลอดภัยข้อมูลและการกู้ระบบเมื่อเกิดเหตุฉุกเฉิน

การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศที่มีประสิทธิภาพเริ่มด้วยการวิเคราะห์ความเสี่ยงที่อาจเกิดขึ้นจากการนำเทคโนโลยีมาใช้งาน การทำความเข้าใจอย่างชัดเจนเกี่ยวกับประเภทความเสี่ยงที่มี เช่น ความเสี่ยงด้านการปฏิบัติการและความเสี่ยงจากระบบ (Systemic Risk) ผลกระทบและความเสียหายที่อาจเกิดขึ้น ระดับของความเสี่ยงที่องค์กรยอมรับได้ และการกำหนดวิธีการบริหารความเสี่ยง แนวทางควบคุมการป้องกันรักษาสินทรัพย์ด้านเทคโนโลยีสารสนเทศ และการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ หลังจากนั้นจึงกำหนดกลยุทธ์การบริหารความเสี่ยงและหน้าที่ความรับผิดชอบของบุคคลที่เกี่ยวข้อง

วิธีการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ มีดังนี้

(3.1) ลดหรือบรรเทาความเสี่ยง โดยกำหนดวิธีการควบคุม เช่น จัดหาเทคโนโลยีการรักษาความปลอดภัยมาใช้ป้องกันสถาปัตยกรรมด้านเทคโนโลยีสารสนเทศ

(3.2) ถ่ายหรือโอนความเสี่ยงโดยการหาพันธมิตรมาช่วยรับความเสี่ยงหรือการทำประกันภัย

(3.3) ยอมรับความเสี่ยง โดยการรับรู้ว่ามีความเสี่ยงและติดตามความเสี่ยงนั้น

(3.4) หลีกเลี่ยงความเสี่ยง โดยการหลีกเลี่ยงกิจกรรมที่ก่อให้เกิดความเสี่ยงนั้น ๆ

(4) การบริหารทรัพยากรด้านเทคโนโลยีสารสนเทศ (IT Resource Management) โดยเน้นโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศและการจัดการองค์ความรู้

การบริหารทรัพยากรด้านเทคโนโลยีสารสนเทศ จะรวมถึง ทรัพยากรบุคคล ข้อมูล โปรแกรมระบบงาน เทคโนโลยีและอุปกรณ์ประกอบต่าง ๆ เพื่อตอบสนองความต้องการทางธุรกิจ ทำให้การบริการมีคุณภาพตรงตามต้องการ ประหยัดค่าใช้จ่ายและได้ประโยชน์การใช้เทคโนโลยี ซึ่ง สง. อาจจะใช้บริการงานด้านเทคโนโลยีสารสนเทศจากผู้ให้บริการภายนอก (IT Outsourcing) โดยจะต้องกำหนดแนวทางการจัดการผู้ให้บริการดังกล่าวเสมือนกับ สง. ดำเนินการเอง เพื่อให้ สง. ได้รับผลตอบแทนที่คุ้มค่าในราคาที่ยอมรับได้

ทรัพยากรบุคคลเป็นสินทรัพย์ที่มีต้นทุนหรือค่าใช้จ่ายเป็นสัดส่วนสูงมากเมื่อเทียบกับ

ต้นทุนทั้งหมดและมีแนวโน้มเพิ่มขึ้นด้วย การบริหารทรัพยากรบุคคลจึงจำเป็นต้องมีการกำหนดศักยภาพหลักที่พนักงานต้องมี การจัดหาและว่าจ้าง การรักษาบุคลากรไว้ ตลอดจนมีการฝึกอบรมเพื่อพัฒนาบุคลากรให้มีทักษะเพียงพอต่อการใช้เทคโนโลยีสารสนเทศอย่างมีประสิทธิภาพและเป็นไปตามวัตถุประสงค์ที่ สง. ตั้งไว้

การกำกับดูแลการปฏิบัติงานด้านเทคโนโลยีสารสนเทศที่มีประสิทธิภาพจะต้องมีการควบคุมต้นทุน การควบคุมสินทรัพย์ด้านเทคโนโลยีสารสนเทศและหน่วยงานที่ใช้ นอกจากนี้ควรจัดลำดับความสำคัญของบริการด้านเทคโนโลยีสารสนเทศที่นำไปใช้สนับสนุนการปฏิบัติงานของหน่วยงานธุรกิจโดยมีการกำหนดข้อตกลงการให้บริการที่เน้นหนักทางธุรกิจ (Business-Oriented SLA) เพื่อใช้สำหรับการกำกับดูแลและติดตามบริการด้านเทคโนโลยีสารสนเทศทั้งภายในและภายนอกองค์กร

(5) การวัดผลงานหรือประเมินประสิทธิภาพ (Performance Measurement) โดยเน้นการติดตามความคืบหน้าของโครงการและการควบคุมติดตามดูแลบริการด้านเทคโนโลยีสารสนเทศ

การนำเทคโนโลยีสารสนเทศมาใช้เพิ่มคุณค่าอย่างมีประสิทธิภาพจะต้องมีการวัดผลงานโดยการควบคุมต้นทุนจริงและผลตอบแทนจากการลงทุน สง. ควรกำหนดให้มีเครื่องมือที่จะใช้ในการวัดคุณค่าของงานและตัวชี้วัดที่ใช้ร่วมกันทั้งหน่วยงานธุรกิจและหน่วยงานเทคโนโลยีสารสนเทศโดยได้รับความเห็นชอบจากผู้บริหารระดับสูงของหน่วยงานธุรกิจด้วย

การสร้างคุณค่าขององค์กรได้เปลี่ยนแปลงจากการใช้สินทรัพย์มีตัวตนมาเป็นสินทรัพย์ไม่มีตัวตน ซึ่งการวัดมูลค่าของสินทรัพย์ไม่มีตัวตนนั้นไม่อาจใช้วิธีทางการเงิน ซึ่งองค์กรอาจกำหนดตัวชี้วัดมาใช้ในการประเมินการปฏิบัติจริงเทียบกับเป้าหมายที่กำหนดไว้ ปัจจัยต่าง ๆ ที่มีผลต่อประสิทธิภาพและสินทรัพย์ทางปัญญาต่าง ๆ ที่จำเป็นต่อการแข่งขันในยุคของข้อมูลสารสนเทศ และต้องมีการวัดหรือประเมิน ได้แก่ ระดับความพึงพอใจของลูกค้า ประสิทธิภาพของระบบปฏิบัติการ และความสามารถในการเรียนรู้และการขยายธุรกิจ

การวัดผลและประสิทธิภาพจากการนำเทคโนโลยีสารสนเทศมาใช้ในองค์กรสามารถปฏิบัติได้โดยการกำหนดเป้าหมายที่ชัดเจนและตัววัดที่ดี เพื่อสะท้อนผลกระทบที่เทคโนโลยีสารสนเทศมีต่อการดำเนินธุรกิจ ซึ่งต้องอาศัยความร่วมมือกันระหว่างผู้ที่มีหน้าที่กำกับดูแลแต่ละระดับชั้นในองค์กร และมีการรายงานเพื่อแสดงประสิทธิภาพและคุณค่าที่ได้รับจากการใช้เทคโนโลยีสารสนเทศรวมทั้งความคืบหน้าของการดำเนินงาน เสนอต่อคณะกรรมการ สง. และผู้บริหารระดับสูงเพื่อสื่อสารให้ทราบถึงประสิทธิภาพ ความเสี่ยง และศักยภาพของเทคโนโลยีสารสนเทศ

การกำหนดเป้าหมายและตัวชี้วัดทางเทคโนโลยีสารสนเทศอาจพิจารณาจากประเด็นต่าง ๆ ดังนี้

(5.1) การเตรียมการเพื่ออนาคต (Future Orientation) เป็นการสร้างพื้นฐานสำหรับการดำเนินงานและการขยายกิจการในอนาคต และส่งเสริมให้เกิดการเรียนรู้อย่างต่อเนื่อง กิจกรรมที่เกี่ยวข้องได้แก่ การจัดหาและรักษาบุคลากรที่มีศักยภาพ การฝึกอบรมและพัฒนาให้บุคลากรมีความเป็นมืออาชีพ การสร้างความสำนึกในหน้าที่และความรับผิดชอบของบุคลากร การประเมินผลงานและการพิจารณาความดีความชอบของพนักงานและหน่วยงาน และการจัดเก็บองค์ความรู้เพื่อปรับปรุงประสิทธิภาพ

(5.2) การปฏิบัติงานที่มีความเป็นเลิศ (Operational Excellence) เป็นการเพิ่มความน่าเชื่อถือและบทบาทของการปฏิบัติงานทางเทคโนโลยีสารสนเทศ ปัจจัยที่เกี่ยวข้องได้แก่

(5.2.1) กระบวนการทางเทคโนโลยีสารสนเทศที่ผ่านการทดสอบและปรับปรุงแล้ว มีความคุ้มทุน ใช้เทคโนโลยีที่ได้มาตรฐานและเชื่อถือได้ ตลอดจนการบริหารจัดการเพื่อให้บริการผู้ใช้งานได้อย่างมีประสิทธิภาพ

(5.2.2) โครงการทางเทคโนโลยีสารสนเทศที่ประสบความสำเร็จ สามารถสนับสนุนผู้ใช้งาน

(5.2.3) การเป็นผู้นำทางเทคโนโลยี โดยหน่วยงานเทคโนโลยีสารสนเทศมีความเข้าใจในกลยุทธ์ของหน่วยงานด้านธุรกิจ สามารถนำเสนอผลงานที่องค์กรนำไปใช้ได้ผล มีความเข้าใจในแนวโน้มของเทคโนโลยี และสามารถพัฒนาปรับปรุงโครงสร้างหรือสถาปัตยกรรมทางเทคโนโลยีขององค์กรได้

(5.3) การให้ความสำคัญต่อลูกค้า (Customer Orientation) เป็นความพยายามบรรลุถึงความต้องการทางธุรกิจ สามารถแบ่งออกได้เป็น 2 บทบาท คือ

(5.3.1) ผู้ให้บริการ ซึ่งต้องสามารถให้บริการที่ดี ในขณะที่สามารถควบคุมต้นทุนเพื่อความได้เปรียบในการแข่งขัน

(5.3.2) ผู้ปฏิบัติตามกลยุทธ์ ซึ่งต้องสร้างผลงานที่สามารถสนับสนุนกระบวนการทางธุรกิจ เพื่อให้องค์กรสามารถบรรลุกลยุทธ์ทางธุรกิจ

(5.4) การเป็นส่วนหนึ่งขององค์กร (Corporate Contribution) เป็นการปฏิบัติเพื่อให้องค์กรมีธรรมาภิบาลด้านเทคโนโลยีสารสนเทศที่มีประสิทธิภาพ โดยการประสานกลยุทธ์ทางเทคโนโลยีสารสนเทศเข้ากับเป้าหมายทางธุรกิจ การเพิ่มคุณค่าให้แก่องค์กร การบริหารความเสี่ยงและการบริหารทรัพยากร

ส่วนที่ 3 แนวทางการตรวจสอบธรรมาภิบาลด้านเทคโนโลยีสารสนเทศ

1. วัตถุประสงค์การตรวจสอบ

1.1 เพื่อประเมินว่า สง. มีระบบการกำกับดูแลด้านเทคโนโลยีสารสนเทศที่ดี มีการดำเนินงานที่มีประสิทธิภาพ

1.2 เพื่อประเมินว่าคณะกรรมการ สง. และผู้บริหารระดับสูง ได้ปฏิบัติตามกฎเกณฑ์และประกาศหนังสือเวียนของ ธปท. อย่างถูกต้อง

1.3 เพื่อประเมินว่า กรรมการ สง.มีคุณสมบัติเหมาะสมกับตำแหน่ง และมีความรู้ความเข้าใจถึงภารกิจ บทบาทหน้าที่ และความรับผิดชอบในการกำกับดูแลด้านเทคโนโลยีสารสนเทศของ สง.

1.4 เพื่อประเมินว่า คณะกรรมการ สง. และผู้บริหารระดับสูงได้ให้ความสนใจ ติดตามและกำกับดูแลการดำเนินงานด้านเทคโนโลยีสารสนเทศของ สง. ให้สอดคล้องตามกลยุทธ์ นโยบายและวัตถุประสงค์ขององค์กร

1.5 เพื่อประเมินว่า คณะกรรมการ สง. และผู้บริหารระดับสูงได้ปฏิบัติหน้าที่และความรับผิดชอบอย่างมีประสิทธิภาพ

1.6 เพื่อประเมินว่า คณะกรรมการ สง. และผู้บริหารระดับสูงได้เอาใจใส่ต่อการแก้ไขปัญหาของ สง. และให้ความสนใจกับรายงานของผู้ตรวจสอบ ธปท. โดย ดำเนินการ หรือกำหนดมาตรการในการแก้ไขได้ทันท่วงที

2. ขอบเขตการตรวจสอบ

2.1 ประเมินคณะกรรมการ สง. และผู้บริหารระดับสูง รวมทั้ง คณะกรรมการชุดย่อยเฉพาะที่รับผิดชอบงานด้านเทคโนโลยีสารสนเทศ เช่น คณะกรรมการกลยุทธ์ด้านเทคโนโลยีสารสนเทศ (IT Strategy Committee) คณะกรรมการเทคโนโลยีสารสนเทศ (IT Steering Committee) และคณะกรรมการตรวจสอบ โดยพิจารณาหลักเกณฑ์การแต่งตั้ง คุณสมบัติ องค์ประกอบ บทบาทหน้าที่และความรับผิดชอบ

2.2 ประเมินคุณภาพการบริหารงานด้านเทคโนโลยีสารสนเทศของคณะกรรมการ สง. ผู้บริหารระดับสูงและคณะกรรมการชุดย่อย

3. กระบวนการตรวจสอบ

3.1 การประเมินระบบการกำกับดูแลด้านเทคโนโลยีสารสนเทศ โดยจะทำการตรวจสอบรายงานการประชุมของคณะกรรมการต่างๆ และเอกสารที่เกี่ยวข้องกับการดำเนินงานด้าน

เทคโนโลยีสารสนเทศ เพื่อประเมินระบบการกำกับดูแลการดำเนินงานด้านเทคโนโลยีสารสนเทศของสง. โดยการประเมินดังกล่าวเป็นส่วนหนึ่งของการประเมินระบบการกำกับดูแลกิจการด้านธรรมาภิบาลของ สง.

3.2 การตรวจสอบคณะกรรมการที่รับผิดชอบงานด้านเทคโนโลยีสารสนเทศ ผู้ตรวจสอบต้องคำนึงถึงเนื้อหาในการทำหน้าที่ของคณะกรรมการดังกล่าวว่า มีความเป็นอิสระเพียงพอ และครอบคลุมงานที่ต้องดำเนินการ มากกว่ารูปแบบ เนื่องจาก สง. บางแห่งไม่ได้จัดตั้งคณะกรรมการย่อยเพื่อรับผิดชอบงานด้านเทคโลยีสารสนเทศขึ้นมาเฉพาะ แต่ได้มอบหมายให้คณะกรรมการบริหาร/จัดการ ทำหน้าที่และรับผิดชอบด้วย

3.3 การสัมภาษณ์ ผู้บริหารและผู้ที่เกี่ยวข้อง เพื่อประเมินข้อเท็จจริง และประเมินว่าเจ้าหน้าที่ของสง. ได้ปฏิบัติตามระเบียบ/คำสั่ง/คู่มือปฏิบัติงาน และประกาศหนังสือเวียนที่ ธปท. กำหนด

3.4 หากตรวจสอบแล้วพบข้อสังเกต ให้ผู้ตรวจสอบค้นหาข้อเท็จจริงเพิ่มเติม และหารือกับผู้บังคับบัญชาตามลำดับชั้นเพื่อพิจารณาก่อนสรุปผลใน Exit meeting ต่อไป

3.5 หากมีข้อสังเกตที่เกี่ยวข้องกับผู้บริหารระดับสูง การสรุปผลในที่ประชุม Exit meeting ควรมีแต่ผู้ที่เกี่ยวข้องเท่านั้น

3.6 ประสานงานกับผู้ตรวจสอบด้านอื่นที่เกี่ยวข้อง หากมีรายละเอียดที่ต้องตรวจสอบเพิ่มเติม

4. แนวทางการเขียนรายงานการตรวจสอบ

การตรวจสอบธรรมาภิบาลด้านเทคโนโลยีสารสนเทศของสถาบันการเงินถือเป็นส่วนหนึ่งในการประเมินคุณภาพการจัดการ ดังนั้น หากมีประเด็นหรือข้อสังเกตที่พบจากการตรวจสอบ เช่น การปฏิบัติหน้าที่ของคณะกรรมการและผู้บริหารระดับสูงไม่สอดคล้องกับหลักธรรมาภิบาล คณะกรรมการขาดความเป็นอิสระ ขอให้ผู้ตรวจสอบเขียนประเด็นหรือข้อสังเกตดังกล่าวในรายงานตรวจสอบด้านเทคโนโลยีสารสนเทศ ภายใต้หัวข้อความเสี่ยงด้านการบริหารงานเทคโนโลยีสารสนเทศ

5. แนวทางการตรวจสอบ

ประเด็นการตรวจสอบ	วิธีการตรวจสอบ	เอกสารที่ใช้ประกอบการตรวจสอบ
1. การผสมผสานกลยุทธ์ด้านเทคโนโลยีสารสนเทศกับกลยุทธ์ทางธุรกิจของ สง. (Strategic Alignment) 1.1 ความสอดคล้องกันระหว่างกลยุทธ์ด้านเทคโนโลยีสารสนเทศกับกลยุทธ์ทางธุรกิจของ สง. <u>วัตถุประสงค์</u> เพื่อตรวจสอบว่า สง. ได้กำหนดกลยุทธ์และเป้าหมายด้านเทคโนโลยีสารสนเทศควบคู่กันไปกับกลยุทธ์และเป้าหมายทางธุรกิจ เพื่อให้กลยุทธ์และเป้าหมายทั้งสองด้านมีความสอดคล้องกัน	- ตรวจสอบรายงานการประชุมคณะกรรมการ สง. เพื่อประเมินว่า (1) คณะกรรมการ สง. ได้ประชุมหารือเกี่ยวกับการกำหนดกลยุทธ์ทางเทคโนโลยีสารสนเทศให้สอดคล้องกับกลยุทธ์ทางธุรกิจ (2) คณะกรรมการ สง. ได้มีส่วนร่วมในการกำหนดกลยุทธ์ด้านเทคโนโลยีสารสนเทศ โดยพิจารณาจากการเข้าร่วมประชุมและการให้ความเห็นของกรรมการ	- รายงานการประชุมคณะกรรมการ สง. - อื่น ๆ เช่น ข่าวหนังสือพิมพ์
	- ตรวจสอบรายงานการประชุมของการกำหนดแผนงานเทคโนโลยีสารสนเทศ และผู้เข้าร่วมประชุม เพื่อพิจารณากระบวนการกำหนดเป้าหมายขององค์กรและเป้าหมายทางเทคโนโลยีสารสนเทศ (1) มีการกำหนดเป้าหมายของ สง.ไว้อย่างชัดเจน เป็นลายลักษณ์อักษร (2) มีการกำหนดเป้าหมายทางเทคโนโลยีสารสนเทศ เพื่อสนับสนุนเป้าหมายของ สง. (3) ผู้บริหารระดับสูงทั้งหน่วยงานเทคโนโลยีสารสนเทศและสายงานธุรกิจร่วมกันพัฒนาแผนงานเทคโนโลยีสารสนเทศ	- รายงานการประชุมของการกำหนดแผนงานเทคโนโลยีสารสนเทศ - แผนงานเทคโนโลยีสารสนเทศ

ประเด็นการตรวจสอบ	วิธีการตรวจสอบ	เอกสารที่ใช้ประกอบการตรวจสอบ
1.2 กลยุทธ์การจัดการเทคโนโลยีสารสนเทศของคณะกรรมการ สง. และฝ่ายจัดการ <u>วัตถุประสงค์</u> เพื่อตรวจสอบว่าคณะกรรมการ สง. และฝ่ายจัดการได้ดำเนินกลยุทธ์เพื่อให้งานเทคโนโลยีสารสนเทศได้สนับสนุนเป้าหมายทางธุรกิจของ สง.	- ตรวจสอบกระบวนการและแนวคิดในการกำหนดและจัดทำกลยุทธ์การจัดการเทคโนโลยีสารสนเทศ ดังนี้ (1) มีการแต่งตั้งคณะกรรมการย่อยด้านกลยุทธ์เทคโนโลยีสารสนเทศเพื่อให้คำปรึกษา พิจารณากำหนดทิศทางของกลยุทธ์และทบทวนรายการลงทุนด้านเทคโนโลยีสารสนเทศที่เป็นรายการสำคัญ (2) พิจารณาองค์ประกอบของคณะกรรมการที่กำหนดกลยุทธ์ (3) หน่วยงานเทคโนโลยีสารสนเทศได้มีส่วนร่วมในการกำหนดทิศทางของกลยุทธ์ (4) ในการปฏิบัติงานเทคโนโลยีสารสนเทศ สง. จะปฏิบัติงานด้วยตนเองหรือใช้ผู้ให้บริการจากภายนอก (Outsourcing)	-รายงานการประชุมคณะกรรมการ สง. - คำสั่งแต่งตั้งคณะกรรมการที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ - คำสั่งการเพื่อมอบหมายหรือกำหนดผู้จัดทำแผนกลยุทธ์การจัดการเทคโนโลยีสารสนเทศ
	- ตรวจสอบรายงานการประเมินระบบงานและเจ้าหน้าที่ฝ่ายบริหารว่าในการพัฒนาหรือปรับเปลี่ยนกลยุทธ์ ได้มีการประเมินระบบสารสนเทศที่ใช้งานในปัจจุบัน เพื่อพิจารณาระดับของความสามารถในการรองรับความต้องการของหน่วยธุรกิจ โดยเน้นที่หน้าที่การทำงาน (Function) เสถียรภาพ ความซับซ้อน ต้นทุน จุดอ่อนของระบบงานและการประมวลผล	-รายงานการประเมินระบบงานและเอกสารที่เกี่ยวข้อง
	- ตรวจสอบเพื่อประเมินว่า สง. มีการสื่อสารให้ผู้ที่เกี่ยวข้องทราบถึงเป้าหมายและวัตถุประสงค์ของกลยุทธ์ด้านเทคโนโลยีสารสนเทศอย่างทั่วถึง - ตรวจสอบรายชื่อผู้เข้าร่วมการประชุมเพื่อชี้แจงเรื่องแผนงานของฝ่ายเทคโนโลยีสารสนเทศจากรายงานการประชุม	- รายงานการประชุมชี้แจงเรื่องแผนงานด้านเทคโนโลยีสารสนเทศ

ประเด็นการตรวจสอบ	วิธีการตรวจสอบ	เอกสารที่ใช้ประกอบการตรวจสอบ
	- ตรวจสอบโครงสร้างของหน่วยงานเทคโนโลยีสารสนเทศ เพื่อประเมินความเหมาะสมของการแบ่งแยกหน้าที่และความรับผิดชอบอย่างชัดเจน	- ผังโครงสร้างของหน่วยงานเทคโนโลยีสารสนเทศ - Job Description
	- ตรวจสอบแผนงานด้านเทคโนโลยีสารสนเทศและประเมินผู้บริหารระดับสูงด้านเทคโนโลยีสนเทศ (CIO) และผู้บริหารระดับสูงของหน่วยธุรกิจว่า มีการกำหนดลำดับความสำคัญของงานเทคโนโลยีสารสนเทศ ระยะเวลาแล้วเสร็จ ตลอดจนบุคคลผู้มีหน้าที่และความรับผิดชอบอย่างชัดเจน	- แผนงานเทคโนโลยีสารสนเทศ - Job Description
	- ประเมินผู้บริหารที่เกี่ยวข้อง และ/หรือ ตรวจสอบโปรแกรมการประเมินผลิตภัณฑ์ปัจจุบันหรือผลิตภัณฑ์ที่กำลังจะออกใหม่ เพื่อประเมินว่า ฝ่ายจัดการมีความรู้ความเข้าใจในลูกค้า ผลิตภัณฑ์ ตลาด และกระบวนการดำเนินงาน	- รายงานการประชุมคณะกรรมการ สง. - รายงานการประชุมคณะกรรมการบริหาร - รายงานการประเมินผลิตภัณฑ์ปัจจุบัน และผลิตภัณฑ์ใหม่
1.3 บทบาทของเทคโนโลยีสารสนเทศที่มีต่อฐานะและความก้าวหน้าขององค์กร <u>วัตถุประสงค์</u> เพื่อตรวจสอบว่าคณะกรรมการ สง. และผู้ที่เกี่ยวข้องได้ตระหนักถึงการนำเทคโนโลยีสารสนเทศมาใช้ในเชิงธุรกิจ โดยเฉพาะพัฒนาการล่าสุด	- ตรวจสอบรายงานการประชุมคณะกรรมการ สง. ว่า ในการประชุมคณะกรรมการ สง. ได้บรรจุประเด็นด้านเทคโนโลยีสารสนเทศเป็นวาระปกติ และมีการพิจารณาประเด็นเหล่านี้อย่างเป็นระบบ	- รายงานการประชุมคณะกรรมการ สง.
	- ตรวจสอบเอกสารที่เกี่ยวข้อง เพื่อประเมินว่า สง. ได้ทำการศึกษาเกี่ยวกับเทคโนโลยีและโอกาสทางธุรกิจ เพื่อใช้ในการกำหนดทิศทางของ สง.	- รายงานการศึกษาทางเทคโนโลยีสารสนเทศที่ สง. จัดทำ

ประเด็นการตรวจสอบ	วิธีการตรวจสอบ	เอกสารที่ใช้ประกอบการตรวจสอบ
	- ตรวจสอบแผนการจัดโครงสร้างของเทคโนโลยี (Technology Infrastructure) ซึ่งต้องมีการกำหนดมาตรฐานของเทคโนโลยีที่องค์กรใช้ และควรพิจารณารวมกับการวางสถาปัตยกรรมของระบบ (System Architecture) ทิศทางของเทคโนโลยี และการปรับเปลี่ยนกลยุทธ์	- แผนการจัดโครงสร้างของเทคโนโลยี (Technology Infrastructure)
2. การเพิ่มคุณค่าให้แก่องค์กร (Value Delivery) 2.1 บทบาทของเทคโนโลยีสารสนเทศในการเพิ่มคุณค่าให้แก่องค์กร วัตถุประสงค์ เพื่อตรวจสอบว่า สง. ได้ใช้เทคโนโลยีสารสนเทศเพื่อสร้างอรรถประโยชน์ให้แก่ผู้ที่เกี่ยวข้องกับ สง.	- ตรวจสอบรายงานวิเคราะห์ผลตอบแทนของโครงการด้านเทคโนโลยีสารสนเทศที่ดำเนินการจนเสร็จสิ้นแล้ว เพื่อประเมินว่าเทคโนโลยีสารสนเทศได้ช่วยเพิ่มผลตอบแทนให้ผู้ที่มีส่วนได้ส่วนเสียกับองค์กร	-รายงานวิเคราะห์ผลตอบแทนจากโครงการด้านเทคโนโลยีสารสนเทศ
	- ตรวจสอบกระบวนการหรือวิธีปฏิบัติในการรับทราบและการรายงานความคิดเห็นหรือผลการใช้เทคโนโลยีสารสนเทศจากหน่วยธุรกิจหรือผู้ใช้งานระบบ และเอกสารที่เกี่ยวข้อง	- ระเบียบหรือวิธีปฏิบัติและเอกสารที่เกี่ยวข้องกับการรายงานความคิดเห็นหรือผลการใช้เทคโนโลยีสารสนเทศจากผู้ใช้งาน
	- ตรวจสอบแบบสอบถามความพึงพอใจของผู้ใช้งาน และสังเกตการณ์เพื่อประเมินความพึงพอใจของผู้ใช้งาน (End Users) ในบริการด้านเทคโนโลยีสารสนเทศ	- แบบสอบถามความพึงพอใจของผู้ใช้งาน
2.2 ประโยชน์ที่องค์กรได้รับจากโครงการพัฒนาเทคโนโลยีสารสนเทศ วัตถุประสงค์ เพื่อตรวจสอบว่าโครงการลงทุนด้านเทคโนโลยีสารสนเทศได้สร้างคุณประโยชน์ตามที่ สง. ต้องการ	- ประเมินหลักเกณฑ์และขั้นตอนในการจัดทำข้อตกลงของระดับการให้บริการ (SLA : Service Level Agreements)	- หลักเกณฑ์และขั้นตอนในการจัดทำข้อตกลงของระดับการให้บริการ

ประเด็นการตรวจสอบ	วิธีการตรวจสอบ	เอกสารที่ใช้ประกอบการตรวจสอบ
	- ตรวจสอบการปฏิบัติตามกฎ ระเบียบข้อบังคับของ สง. และทางการ ตรวจสอบหน่วยงานที่ต้องใช้ข้อมูลสารสนเทศหรือใช้เทคโนโลยีสารสนเทศเพื่อประเมินว่าเทคโนโลยีสารสนเทศที่ลงทุนไปช่วยสนับสนุนข้อมูลให้องค์กร เพื่อให้สามารถปฏิบัติตามกฎระเบียบของทางการได้ดี และช่วยยกระดับการบริการ (Service Levels) ให้ดียิ่งขึ้น	- รายงานผลการปฏิบัติตามกฎ ระเบียบข้อบังคับของทางการ
	- ตรวจสอบแผนการลงทุนในเทคโนโลยีสารสนเทศเพื่อประเมินว่า โครงการทางเทคโนโลยีสารสนเทศมีความสอดคล้องกับกลยุทธ์ธุรกิจ และมีวิธีการวัดมูลค่าไว้อย่างชัดเจนให้เห็นว่าคุ้มค่าควรลงทุน	- แผนการลงทุนในเทคโนโลยีสารสนเทศ - รายงานการวิเคราะห์ความคุ้มค่าของการลงทุน
	- ตรวจสอบผลสำเร็จของงานโครงการเทคโนโลยีสารสนเทศเปรียบเทียบกับแผนเพื่อประเมินว่าสามารถส่งมอบงานได้ตามที่กำหนดไว้	- แผนงานโครงการเทคโนโลยีสารสนเทศ
	- มีการรายงานความคืบหน้าของโครงการที่สำคัญให้คณะกรรมการ สง. ได้รับทราบอย่างสม่ำเสมอ	- รายงานความคืบหน้าของงานตามโครงการ - รายงานการประชุมคณะกรรมการ สง.
3. การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk Management) 3.1 แนวทางปฏิบัติในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ วัตถุประสงค์ เพื่อตรวจสอบว่า สง. มีการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศที่มีประสิทธิภาพ	- ตรวจสอบเพื่อประเมินว่าหน่วยงานเทคโนโลยีสารสนเทศ คณะกรรมการบริหารความเสี่ยง และหน่วยงานอื่นที่เกี่ยวข้อง ได้ร่วมกันกำหนดแนวทางการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศแล้วนำเสนอให้คณะกรรมการ สง. / ฝ่ายจัดการอนุมัติในหลักการ	- นโยบายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ - ระเบียบวิธีปฏิบัติเกี่ยวกับการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

ประเด็นการตรวจสอบ	วิธีการตรวจสอบ	เอกสารที่ใช้ประกอบการตรวจสอบ
	- ตรวจสอบเพื่อประเมินวิธีปฏิบัติในการระบุ ประเมิน และจัดการความเสี่ยง รวมทั้งจัดให้มีการวิเคราะห์ความเสี่ยงด้านเทคโนโลยีสารสนเทศที่ สง. ประสบอยู่ เพื่อให้ทราบถึงจุดที่มีความเสี่ยง (Vulnerabilities) ภายในโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ และความเสียหายที่อาจเกิดขึ้น โดยมีการปรับปรุงวิธีการดังกล่าวเป็นระยะ	- รายงานการประเมินและวิเคราะห์ความเสี่ยง และเอกสารที่เกี่ยวข้อง ซึ่งควรมีคำอธิบายวิธีการประเมินความเสี่ยง ลักษณะของความเสี่ยงที่เกิดขึ้นและผลกระทบจากความเสี่ยงนั้น
	- ตรวจสอบแผนปฏิบัติงานด้านความเสี่ยง ซึ่งควรกำหนดรายละเอียดแนวทางและวิธีการจัดการความเสี่ยง ได้แก่ การหลีกเลี่ยง การลดหรือบรรเทา และการระบุระดับของความเสี่ยงที่เกิดขึ้นและยอมรับได้ ตลอดจนมาตรการรักษาความปลอดภัย - ตรวจสอบเพื่อประเมินว่า สง. มีการติดตามความคืบหน้าหรือมีความต่อเนื่องในการลดความเสี่ยง	- แผนปฏิบัติงานการบริหารความเสี่ยง และมาตรการรักษาความปลอดภัย
	- ตรวจสอบเพื่อประเมินว่า สง. ได้จัดให้มีการดำเนินการแก้ไขปัญหาทางเทคโนโลยีสารสนเทศอย่างเป็นระบบ เพื่อให้การปฏิบัติงานเป็นไปอย่างต่อเนื่อง ได้แก่ การจัดการปัญหา (Problem Management) การจัดการ การแก้ไขเปลี่ยนแปลงโปรแกรมระบบงานหลังจากนำออกใช้งานแล้ว (Change Management) และการจัดการบันทึกการกำหนดค่าต่าง ๆ ของคอมพิวเตอร์ (Configuration Management)	- นโยบายและระเบียบปฏิบัติเกี่ยวกับการบันทึกปัญหาและวิธีการแก้ไข - ระเบียบปฏิบัติในการแก้ไขโปรแกรมระบบงาน - ระเบียบปฏิบัติวิธีการพัฒนาระบบงาน (SDLC) - ระเบียบปฏิบัติในการจัดการบันทึกการกำหนดค่าต่าง ๆ ของคอมพิวเตอร์

ประเด็นการตรวจสอบ	วิธีการตรวจสอบ	เอกสารที่ใช้ประกอบการตรวจสอบ
	- ตรวจสอบว่า สง. มีการเปรียบเทียบความคุ้มค่าของผลตอบแทนที่ได้รับกับต้นทุนการจัดการกับความเสี่ยง	- รายงานการวิเคราะห์ความคุ้มทุนในการจัดหาเครื่องมือป้องกันความเสี่ยง
	- ตรวจสอบว่า คณะกรรมการ สง. ได้รับรายงานเกี่ยวกับความเสี่ยงด้านเทคโนโลยีสารสนเทศ รวมทั้งความเสี่ยงเกี่ยวกับการปฏิบัติงานให้เป็นไปตามกฎเกณฑ์ กฎหมาย และข้อบังคับต่างๆ เพื่อนำไปใช้ในการติดตามความเสี่ยง และลดความเสี่ยง	- รายงานความเสี่ยงที่เสนอคณะกรรมการ สง. - รายงานการประชุมคณะ กรรมการ สง.
	- ตรวจสอบเพื่อประเมินว่าฝ่ายจัดการกำหนดให้มีผู้รับผิดชอบที่ชัดเจนเพื่อควบคุมดูแล และบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ	- ระเบียบคำสั่งแต่งตั้งเกี่ยวกับหน้าที่และความรับผิดชอบของหน่วยงานบริหารความเสี่ยง
3.2 การตรวจสอบและการควบคุมภายในด้านเทคโนโลยีสารสนเทศ <u>วัตถุประสงค์</u> เพื่อตรวจสอบว่าคณะกรรมการ สง. ได้กำหนดให้มีการตรวจสอบและการควบคุมภายในด้านเทคโนโลยีสารสนเทศ	- ตรวจสอบว่าคณะกรรมการ สง. ได้แต่งตั้งและกำหนดแนวทางการปฏิบัติงานและความรับผิดชอบของคณะกรรมการตรวจสอบ ให้มีหน้าที่พิจารณาความเสี่ยงที่สำคัญ แต่งตั้งผู้ตรวจสอบภายในและจัดหาผู้ตรวจสอบภายนอกที่เป็นอิสระ และติดตามให้มีการปฏิบัติตามคำแนะนำของผู้ตรวจสอบ	- คำสั่งแต่งตั้งและอำนาจหน้าที่ของคณะกรรมการตรวจสอบ
	- ตรวจสอบเพื่อประเมินกระบวนการในการรายงาน การแก้ไขปัญหาที่เกิดขึ้น และความรวดเร็วของฝ่ายจัดการในการดำเนินการแก้ไข เมื่อการปฏิบัติงานด้านเทคโนโลยีสารสนเทศมีจุดอ่อนหรือมีปัญหาที่เกิดจากการควบคุมภายใน และเกิดผลเสียต่อองค์กร	- ระเบียบวิธีปฏิบัติในการรายงานและแก้ไขปัญหา - รายงานและการแก้ไขปัญหา
	- ตรวจสอบนโยบาย Outsourcing และสัญญาว่าจ้างต่างๆ เพื่อประเมินประสิทธิภาพในการจัดการสัญญาว่าจ้างผู้ให้บริการ	- นโยบาย Outsourcing และระเบียบคำสั่งเกี่ยวกับสัญญาว่าจ้างต่างๆ

ประเด็นการตรวจสอบ	วิธีการตรวจสอบ	เอกสารที่ใช้ประกอบการตรวจสอบ
	- ตรวจสอบนโยบายและแนวทางการปฏิบัติต่อผู้ขายและประเมินผู้บริหารระดับสูงว่ามีการบริหารความเสี่ยงจากผู้ขาย (Supplier Risk) ด้วยการจัดการความสัมพันธ์กับผู้ขาย การใช้ Escrow การจัดหาผู้ขายสำรอง หรือการถือหุ้นในกิจการของผู้ขาย	- นโยบายและแนวทางการปฏิบัติต่อผู้ขาย
4. การบริหารทรัพยากรด้านเทคโนโลยีสารสนเทศ (IT Resource Management) 4.1 ความสามารถในการบริหารจัดการเทคโนโลยีสารสนเทศของคณะกรรมการ สง. <u>วัตถุประสงค์</u> ตรวจสอบเพื่อประเมินว่าคณะกรรมการ สง. มีทักษะที่เพียงพอต่อการบริหารงานและโครงการเทคโนโลยีสารสนเทศ	- ตรวจสอบเพื่อประเมินความสามารถของคณะกรรมการ สง. ในการปฏิบัติตามหลักธรรมาภิบาลด้านเทคโนโลยีสารสนเทศ และการตัดสินใจในเรื่องเทคโนโลยีสารสนเทศที่สำคัญ	- รายงานการประชุมคณะกรรมการ สง.
4.2 ความสามารถในการบริหารจัดการเทคโนโลยีสารสนเทศของฝ่ายจัดการ <u>วัตถุประสงค์</u> ตรวจสอบเพื่อประเมินว่าฝ่ายจัดการมีทักษะที่เพียงพอต่อการบริหารงานและโครงการเทคโนโลยีสารสนเทศ ซึ่งรวมถึงการบริหารทรัพยากรและการลงทุนในเทคโนโลยีสารสนเทศ	- ตรวจสอบเพื่อประเมินว่าหน่วยงานเทคโนโลยีสารสนเทศมีทรัพยากรที่มีประสิทธิภาพ และมีจำนวนเพียงพอต่อการบรรลุวัตถุประสงค์ด้านกลยุทธ์ ดังนี้ (1) ตรวจสอบแผนการจัดเตรียมและจัดสรรทรัพยากรที่จำเป็นในระบบงานแต่ละระบบ ซึ่งทรัพยากรดังกล่าวได้แก่ - บุคลากร - ระบบงาน - โครงสร้างพื้นฐานด้านเทคโนโลยี - อุปกรณ์ เครื่องมือต่างๆ - ข้อมูล (2) ตรวจสอบรายงานสถิติเกี่ยวกับประสิทธิภาพของการใช้ทรัพยากร	- แผนการจัดเตรียมและจัดสรรทรัพยากรที่จำเป็นในระบบงานแต่ละระบบ - รายงานสถิติเกี่ยวกับประสิทธิภาพของการใช้ทรัพยากร - รายงานผู้ตรวจสอบภายในและผู้ตรวจสอบภายนอก

ประเด็นการตรวจสอบ	วิธีการตรวจสอบ	เอกสารที่ใช้ประกอบการตรวจสอบ
	(3) ศึกษาความเห็นของผู้ตรวจสอบภายในและภายนอก	
	- ตรวจสอบนโยบายการลงทุนและวิธีการทบทวนการลงทุน รวมทั้งการสัมภาษณ์ผู้ที่เกี่ยวข้อง เพื่อประเมินความคุ้มค่าของการลงทุนในเทคโนโลยีสารสนเทศขององค์กร เมื่อเปรียบเทียบกับ สง. อื่น ๆ	-นโยบายและวิธีการทบทวนการลงทุน - รายงานการวิเคราะห์ความคุ้มค่าของการลงทุน
	- ตรวจสอบกระบวนการจัดทำงบประมาณเพื่อประเมินว่า ฝ่ายจัดการมีการบริหารทรัพยากรที่มีประสิทธิภาพ โดยหน่วยงานธุรกิจและหน่วยงานเทคโนโลยีสารสนเทศร่วมกันกำหนดวิธีการพิจารณาประเภทของทรัพยากรที่ต้องใช้ และวิธีการจัดสรรทรัพยากร โดยพิจารณาจากลำดับความสำคัญก่อนหลังของงานหรือโครงการเทคโนโลยีสารสนเทศที่สนับสนุนหน่วยงานธุรกิจ	- ระเบียบคำสั่งหรือวิธีปฏิบัติเกี่ยวกับกระบวนการจัดทำงบประมาณ
	- ตรวจสอบแผนการลงทุนในเทคโนโลยีสารสนเทศเพื่อประเมินว่ามีการกำหนดรายละเอียดของแผนการลงทุนไว้อย่างชัดเจน	- แผนการลงทุนในเทคโนโลยีสารสนเทศ
	- ตรวจสอบการวิเคราะห์จำนวนเงินลงทุนในเทคโนโลยีสารสนเทศ เพื่อประเมินประสิทธิภาพในการลงทุน โดยพิจารณาจาก (1) จำนวนเงินที่ลงทุนในเทคโนโลยีสารสนเทศ เมื่อเปรียบเทียบกับ สง. อื่น (2) งบประมาณที่ใช้ในกิจกรรมเทคโนโลยีสารสนเทศ เมื่อคิดเป็นร้อยละของรายได้รวม (3) ค่าใช้จ่ายด้านเทคโนโลยีสารสนเทศ เมื่อคิดเป็นร้อยละของกำไรหรืองบประมาณของ สง.	- ระเบียบหรือวิธีปฏิบัติเกี่ยวกับการจัดทำงบประมาณ - แผนการลงทุนในเทคโนโลยีสารสนเทศ - รายงานค่าใช้จ่ายจริงเปรียบเทียบกับงบประมาณ

ประเด็นการตรวจสอบ	วิธีการตรวจสอบ	เอกสารที่ใช้ประกอบการตรวจสอบ
	(4) อัตราการเพิ่มขึ้นของงบประมาณหรือค่าใช้จ่ายในแต่ละปีและการเปรียบเทียบกับค่าเฉลี่ยของสถาบันการเงิน (5) ความแตกต่างระหว่างประมาณการและการใช้จ่ายที่เกิดขึ้นจริง (6) จำนวนโครงการเทคโนโลยีสารสนเทศที่ใช้เงินเกินงบประมาณเป็นจำนวนมากและบ่อยครั้ง	
4.3 การพัฒนาบุคลากรด้านเทคโนโลยีสารสนเทศ วัตถุประสงค์ ตรวจสอบเพื่อประเมินว่า สง. ได้จัดให้มีการพัฒนา ฝึกอบรม ให้ความรู้ และจัดหาอุปกรณ์ที่เหมาะสมต่อการพัฒนาการเรียนรู้ ให้แก่บุคลากรด้านเทคโนโลยีสารสนเทศอย่างเพียงพอ	- ตรวจทานแผนฝึกอบรมประจำปี ซึ่งควรเป็นส่วนหนึ่งของแผนพัฒนาบุคลากร - ตรวจสอบประวัติการฝึกอบรมเพื่อประเมินว่าพนักงานได้รับการฝึกอบรมให้ตรงตามหน้าที่และความรับผิดชอบอย่างเพียงพอ	- แผนฝึกอบรมด้านเทคโนโลยีสารสนเทศประจำปี
5. การประเมินประสิทธิภาพ (Performance Measurement) 5.1 การวัดประสิทธิภาพของงานเทคโนโลยีสารสนเทศ วัตถุประสงค์ ตรวจสอบเพื่อประเมินบทบาทของคณะกรรมการ สง. และฝ่ายจัดการในการกำหนดตัวชี้วัดประสิทธิภาพของงานเทคโนโลยีสารสนเทศ	- ตรวจสอบรายงานการประชุมคณะกรรมการ สง. เพื่อประเมินว่าคณะกรรมการ สง. มีส่วนร่วมในการกำหนดให้มีการวัดประสิทธิภาพของงานเทคโนโลยีสารสนเทศ	- รายงานการประชุมคณะกรรมการ สง.
	- ตรวจสอบและประเมินฝ่ายจัดการเกี่ยวกับการกำหนดให้มีเครื่องมือหรือวิธีการเพื่อใช้วัดประสิทธิภาพ ผลงาน และติดตามความคืบหน้าของกิจกรรมการปรับปรุงพัฒนางานโครงการด้านเทคโนโลยี	- รายงานประเมินประสิทธิภาพงานเทคโนโลยีสารสนเทศและเครื่องมือชี้วัดประสิทธิภาพ

ประเด็นการตรวจสอบ	วิธีการตรวจสอบ	เอกสารที่ใช้ประกอบการตรวจสอบ
5.2 การรายงาน วัตถุประสงค์ ตรวจสอบเพื่อประเมินว่าคณะกรรมการ สง. ได้รับรายงานที่แสดงถึงประสิทธิภาพของงานเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ	- ตรวจสอบว่า คณะกรรมการ สง. ได้รับรายงานด้านเทคโนโลยีสารสนเทศต่างๆ เช่น (1) รายงานแสดงความคืบหน้าของโครงการลงทุนในเทคโนโลยีสารสนเทศที่เป็นโครงการใหญ่ๆ (2) รายงานสรุปความเสี่ยงและปัญหาด้านเทคโนโลยีสารสนเทศที่เกิดขึ้น (3) รายงานสรุปผลการสำรวจความคิดเห็นของหน่วยงานธุรกิจหรือลูกค้า ถึงความพึงพอใจในการบริการด้านเทคโนโลยีสารสนเทศ	- รายงานการประชุมคณะ กรรมการ สง.