COSO[1] 2013 กรอบแนวคิดระบบควบคุมภายใน เพื่อประยุกต์ใช้กับมหาวิทยาลัยในกำกับของรัฐ

โดย สุวรรณา เจนสวัสดิ์พงศ์, CIA

ผู้อำนวยการศูนย์ตรวจสอบภายใน มหาวิทยาลัยมหิดล[2]

มหาวิทยาลัยในประเทศไทยได้เริ่มมีการเปลี่ยนสถานะจากส่วนราชการ เป็นมหาวิทยาลัยในกำกับของรัฐมาเป็นเวลากว่า 10 ปี เพื่อให้มีความคล่องตัวในการดำเนินงาน การคิดค้น การผลิตนวัตกรรมที่มากขึ้น ภารกิจของมหาวิทยาลัยจึงอาจมีความหลากหลายมากกว่าในอดีต ดังนั้น ขณะนี้จึงอาจเป็นเวลาที่เหมาะสมที่มหาวิทยาลัยจะพิจารณายกระดับระบบควบคุมภายใน โดยประยุกต์ใช้กรอบแนวคิดของระบบควบคุมภายในฉบับล่าสุด (COSO (2013)) ซึ่งถึงแม้ว่ากรอบแนวคิดนี้จะยังอยู่ภายใต้องค์ประกอบของการควบคุมภายใน 5 องค์ประกอบเดิมที่ COSO กำหนดไว้เมื่อปี 1992 แต่รายละเอียดในแต่ละองค์ประกอบมีความชัดเจนมากขึ้น จากการแบ่งหมวดหมู่หลักการ (Principle) เป็น 17 หลักการ เพื่อให้องค์กรมีรายละเอียดข้อมูลมากพอที่จะนำไปประยุกต์ใช้ได้ง่ายมากขึ้น

และในบทความนี้ได้นำเสนอแบบประเมินองค์ประกอบของระบบควบคุมภายในตามกรอบแนวคิด COSO 2013 ที่น่าจะเหมาะสมกับบริบทของมหาวิทยาลัย โดยประยุกต์จากแบบประเมินที่คณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (ก.ล.ต.) กำหนดให้บริษัทจดทะเบียนทั้งหมดทำการประเมินและนำส่งผลการประเมินต่อก.ล.ต. เป็นส่วนหนึ่งของรายงานประจำปี

❖ จากกรอบแนวคิดเมื่อปี 1992 สู่ปี 2013

โดยอ้างอิงบทความเรื่อง COSO 2013 ความเปลี่ยนแปลงจาก COSO 1992 ที่เขียนโดย อาจารย์ จิรพร สุเมธีประสิทธิ์ ที่ปรึกษาอิสระ ที่เผยแพร่ผ่าน https://chirapon.wordpress.com/2013/10/09/coso-2013-ความเปลี่ยนแปลงจาก-coso-1992-ป/ COSO 2013 มีการเปลี่ยนแปลงจากกรอบแนวคิดฉบับปี 1992 ดังนี้

การปรับตัวครั้งใหญ่ของแนวคิดการควบคุมภายในตามกรอบ COSO ได้ทำให้เกิดกรอบแนวทางตามแนวคิดของ COSO 2013 ที่ปรับปรุงจากแนวคิดพื้นฐานของ COSO 1992 ในสาระสำคัญหลายประการ

ประเด็นที่น่าจะอยู่เบื้องหลังการปรับกรอบแนวคิดครั้งใหม่ของ COSO 2013 Internal Control – Integrated Framework น่าจะมาจากการทบทวนบทบาทของระบบควบคุมภายในที่ใช้กันอยู่ในกิจการทุกกิจการและทุกประเภท อย่างน้อย 2 ประเด็น ได้แก่

---

[1] COSO - The Committee of Sponsoring Organizations of the Treadway Commission เป็นคณะกรรมการร่วมของสถาบันวิชาชีพ 5 แห่ง ได้แก่ สถาบันผู้สอบบัญชีรับอนุญาตแห่งสหรัฐอเมริกา (AICPA) สถาบันผู้ตรวจสอบภายในสากล (Institute of Internal Auditors หรือ IIA) สถาบันผู้บริหารการเงิน (Financial Executives Institute หรือ FEI) สมาคมนักบัญชีแห่งสหรัฐอเมริกา (American Accounting Association หรือ AAA) และสถาบันนักบัญชีเพื่อการบริหาร (Institute of Management Accountants หรือ IMA)

[2] ข้อเขียนในบทความนี้เป็นความเห็นเฉพาะตัวของผู้เขียน มิใช่ความเห็นในนามขององค์กรที่ผู้เขียนสังกัด และเมื่อผู้เขียนใช้ข้อมูลจากแหล่งอื่น ก็ได้มีการอ้างอิงที่มาของข้อมูลนั้นประกอบไว้ด้วยแล้ว

ประเด็นที่ 1 โครงสร้างของการควบคุมภายในที่อยู่ใน COSO 1992 เพียงพอที่จะบรรเทาหรือลดระดับความเสี่ยงจนทำให้การประกอบการของกิจการบรรลุตามวัตถุประสงค์แล้วหรือไม่

ประเด็นที่ 2 การเปลี่ยนแปลงของระบบควบคุมภายใน สามารถสะท้อนหรือควรจะสะท้อนว่าเป็นการเปลี่ยนแปลงที่สอดคล้องกับการเปลี่ยนแปลงทางธุรกิจด้วยหรือไม่

สิ่งที่เป็นความเชื่อของ COSO 2013 Internal Control – Integrated Framework คือ การเปลี่ยนแปลงของระบบควบคุมภายใน ควรจะสอดคล้องกับการเปลี่ยนแปลงเชิงโครงสร้างของธุรกิจ หรือการเปลี่ยนแปลงของเทคโนโลยีสารสนเทศ หรือการเปลี่ยนแปลงกระบวนการดำเนินงานจากที่เคยดำเนินการเองไปสู่การว่าจ้างผู้ให้บริการภายนอกดำเนินการแทนซึ่งทำให้ต้องขยายการกำกับควบคุมออกไปสู่บุคลากรของผู้ให้บริการภายนอกด้วย

การปรับกรอบแนวทางการควบคุมภายในจาก COSO 1992 สู่ COSO 2013 จึงน่าจะเป็นตัวกระตุ้นให้องค์กร

(1) ได้ทบทวนในระดับกลยุทธ์ว่า ควรมีการเปลี่ยนแปลงเพื่อเป็นการปรับปรุงประสิทธิภาพ หรือประสิทธิผลของระบบการควบคุมภายในหรือไม่

(2) มีโอกาสบูรณาการและเชื่อมโยงหน้าที่ด้านการค้นหาความเสี่ยงและการกำกับการปฏิบัติตามกฎเกณฑ์ (Compliance) ให้เป็นส่วนหนึ่งของขั้นตอนการดำเนินธุรกรรมขององค์กรให้ชัดเจนยิ่งขึ้น

(3) ดำเนินการให้มั่นใจได้ว่า ระบบการควบคุมภายในองค์กรนั้น มีอยู่ และ ปฏิบัติได้จริง

เรื่องที่เห็นได้ชัดเจนว่า COSO 2013 เพิ่มเติมจาก COSO 1992 ประกอบด้วย

ประการที่ 1 การเอาใจใส่ และให้ความสำคัญกับธรรมาภิบาล (Governance) ที่องค์กรไม่อาจหลีกเลี่ยงได้ และการต้องเพิ่มกิจกรรมที่ส่งเสริมธรรมาภิบาลในองค์กรด้วย

ประการที่ 2 การเพิ่มข้อพึงปฏิบัติที่ให้ความสำคัญ และการกำหนดให้ใช้เทคโนโลยีเพื่อการควบคุมด้วยกลไกอัตโนมัตินอกเหนือจากการพึ่งพาตัวบุคคล ทั้งในส่วนที่เป็นกระบวนการปฏิบัติงาน (Operation) และระบบการรายงาน (Reporting)

ประการที่ 3 การปรับระบบการควบคุมภายในให้เหมาะสมกับองค์กรโดยคำนึงถึงผลกระทบจากกระแสโลกาภิวัตน์ และการให้บริการตามพันธกิจซึ่งอาจต้องเปลี่ยนแปลงตาม

ประการที่ 4 การขยายขอบเขตของการจัดทำรายงานโดยเฉพาะด้านการเงิน โดยควรคำนึงให้สามารถใช้ประโยชน์ได้ทั้งภายในและภายนอกองค์กร

ประการที่ 5 การแยกความเสี่ยงจากการทุจริตออกมาพิจารณาต่างหากและเพิ่มหัวข้อในการพิจารณา ซึ่งความเสี่ยงนี้เป็นหลักการสำคัญหลักการหนึ่งใน 17 หลักการของ COSO 2013 ที่องค์กรต้องวางระบบควบคุมภายในให้สามารถป้องกันการทุจริตในลักษณะต่างๆ ได้ด้วย

ประการที่ 6 การเพิ่มความครอบคลุมของรายงานเกี่ยวกับผลการใช้ระบบควบคุมภายใน โดยไม่ได้จำกัดเฉพาะรายงานทางการเงิน หากแต่ครอบคลุมถึงรายงานลักษณะอื่น รวมทั้งรายงานด้านการปฏิบัติงานและการปฏิบัติให้เป็นไปตามกฎเกณฑ์ และรายงานที่สะท้อนความยั่งยืนขององค์กรด้วย

ประการที่ 7 การขยายกลุ่มผู้ที่เกี่ยวข้องในการจัดวางระบบการควบคุมเพื่อกำกับความเสี่ยงที่มีผลต่อการบรรลุแผนยุทธศาสตร์ขององค์กร โดยให้ครอบคลุมทั้ง ผู้ที่เกี่ยวข้องภายใน และ ผู้ที่เกี่ยวข้องภายนอก

ผู้ที่เกี่ยวข้องภายใน ครอบคลุมทั้ง 1) ผู้บริหารระดับสูง ซึ่งมีความรับผิดชอบทั้งการบริหารจัดการในฐานะผู้บริหาร และการกำหนดนโยบาย ออกคำสั่ง กฎเกณฑ์ ข้อบังคับ 2) หน่วยงานบริหารความเสี่ยง และ 3) คณะกรรมการบริษัทหรือคณะกรรมการตรวจสอบ ซึ่งมีความรับผิดชอบด้านการกำกับดูแลในองค์กร

ส่วนผู้ที่เกี่ยวข้องภายนอก COSO 2013 จะเน้นไปยัง ผู้ตรวจสอบภายนอก

ประการที่ 8 COSO 2013 กำหนดการบริหารจัดการความเสี่ยงที่ชัดเจนกว่า COSO 1992

ประการที่ 9 การเพิ่มความรับผิดชอบของเจ้าของภาระงาน/กระบวนการ (Process Owner) แต่ละเรื่องในการออกแบบให้กระบวนการมีระบบควบคุม ที่สอดคล้องกับวัตถุประสงค์ของการควบคุมภายในที่ตั้งไว้

บุคลากรที่เกี่ยวข้องครอบคลุมตั้งแต่คณะกรรมการขององค์กร (มหาวิทยาลัย เรียก สภามหาวิทยาลัย) ผู้บริหารระดับสูง และบุคลากรที่รับผิดชอบภาระงานหรือกระบวนการหนึ่งๆ ทั่วทั้งองค์กร

ประการที่ 10 การเพิ่มบทบาทของระบบควบคุมด้านเทคโนโลยีสารสนเทศ (IT Control) โดยเฉพาะความเสี่ยงของการรักษาความปลอดภัยของสารสนเทศ การใช้เทคโนโลยีสมัยใหม่ในการดำเนินงาน การเชื่อมโยงระบบงานข้ามสถานที่ตั้ง และการใช้คลาวด์ คอมพิวติ้ง ซึ่งเป็นสิ่งที่มีประโยชน์ต่อองค์กรแต่ก็จะทำให้องค์กรมีความเสี่ยงต่อการถูกโจมตีทางคอมพิวเตอร์ด้วย

ประการที่ 11 การยกระดับความสำคัญของความเสี่ยงจากการกำกับการปฏิบัติตามกฎเกณฑ์และความเสี่ยงด้านปฏิบัติการ (Compliance and Operational Objectives) ให้มีความเด่นชัดมากขึ้น และมีความสำคัญเทียบเท่าความเสี่ยงทางการเงินและการรายงานทางการเงิน ทั้งนี้ เพื่อให้องค์กรมีการวางระบบการควบคุมภายในเพื่อวัตถุประสงค์ในด้านนี้อย่างจริงจัง

ประการที่ 12 การแยกข้อพึงปฏิบัติในด้านการควบคุมการออกรายงานทางการเงินที่เปิดเผยแก่บุคคลภายนอกออกมาเป็นหลักการเฉพาะ ซึ่งแสดงถึงแนวคิดที่ขยายวงออกไปจากเดิมที่เน้นเฉพาะการควบคุมภายในองค์กร สู่ผู้ที่เกี่ยวข้องภายนอกองค์กรมากขึ้น

ประการที่ 13 การขยายกรอบแนวคิดด้านการควบคุม สู่ความสัมพันธ์ เชื่อมโยงระหว่างองค์กร เช่น

(ก) การทำความตกลงร่วมลงทุน
(ข) การพึ่งพาอาศัยซับพลายเออร์
(ค) การทำความตกลงกับคู่ค้า

โดย COSO 2013 ให้นำประเด็นเหล่านี้ ซึ่งอาจเป็นประเด็นระดับโลกมาค้นหาและประเมินความเสี่ยง และพัฒนางานควบคุมเพื่อกำกับความสำเร็จของงาน

ประการที่ 14 นอกเหนือจากการยึดองค์ประกอบหลัก 5 องค์ประกอบของการควบคุมภายในตามเดิมแล้ว COSO 2013 ยังพยายามก้าวสู่การพัฒนาประสิทธิผลของการใช้การควบคุมภายในเป็นกลไกในการกำกับขั้นตอนการดำเนินงานและผลการดำเนินการ ให้การควบคุมมีหน้าที่จริงในองค์กร ไม่ใช่เพียงการออกแบบหรือวางมาตรการการควบคุม

ประการที่ 15 มีการปรับปรุงองค์ประกอบของระบบควบคุม 5 องค์ประกอบให้ละเอียดมากขึ้น ได้แก่

- องค์ประกอบที่ 1 – สภาพแวดล้อมการควบคุม

โดยเน้นการกำหนดนโยบายจากระดับบนลงล่าง (Tone at the Top) ที่เป็นความรับผิดชอบของคณะกรรมการบริษัท ผู้บริหารระดับสูง และคณะกรรมการตรวจสอบ มากขึ้น

- องค์ประกอบที่ 2 – การค้นหาความเสี่ยง

โดยเน้นการนิยามเกณฑ์ความเสี่ยงที่ยอมรับได้ (Risk Appetite) และค่าเบี่ยงเบนความเสี่ยงที่เกิดจากผลของเหตุการณ์ความเสี่ยงต่อการบรรลุผลสำเร็จของการดำเนินงาน ที่อาจจะต้องทำให้องค์กรมีความยืดหยุ่นตามสภาพความเสี่ยงมากขึ้น

- องค์ประกอบที่ 3 – กิจกรรมการควบคุม

โดยเน้นการวางนโยบาย และกำหนดกิจกรรมควบคุมไว้ในขั้นตอนการปฏิบัติงานที่จะกำกับ ตลอดจนการวางระบบรายงานเพื่อทบทวนกิจกรรมการควบคุมที่เกิดจริงกับวัตถุประสงค์การควบคุมที่วางไว้

- องค์ประกอบที่ 4 – สารสนเทศและการสื่อสาร

โดยเน้นการไหลของสารสนเทศและกิจกรรมการสื่อสารที่ครอบคลุมตามความจำเป็น ตั้งแต่ระดับคณะกรรมการบริษัท ผู้บริหาร และเจ้าของกระบวนการทุกระดับในองค์กร

- องค์ประกอบที่ 5 – การกำกับติดตาม และประเมินผล

โดยเน้นการกำกับติดตามของเจ้าของกระบวนการ ทั้งในการปฏิบัติงานประจำวันและการประเมินผลโดยหน่วยงานอื่นที่เป็นอิสระ โดยการประเมินผลนี้จะต้องเชื่อมโยงกับวัตถุประสงค์ของกระบวนการ ความเสี่ยงที่เกี่ยวข้อง และกิจกรรมการควบคุมในกระบวนการ

❖ การประยุกต์แบบประเมินความเพียงพอของระบบควบคุมภายในของก.ล.ต. สู่มหาวิทยาลัย

การตอบแบบประเมินในแต่ละข้อ ควรอยู่บนพื้นฐานของการปฏิบัติจริง หากประเมินแล้วพบว่ายังขาดการควบคุมภายในที่เพียงพอในข้อใด (ไม่ว่าจะเป็นการไม่มีระบบในเรื่องนั้น หรือมีแล้วแต่ยังไม่เหมาะสม) ขอให้อธิบายเหตุผลและแนวทางแก้ไขประกอบไว้ด้วย

การควบคุมภายในองค์กร (Control Environment)

1. องค์กร[3]แสดงถึงความยึดมั่นในคุณค่าของความซื่อตรง (integrity) และจริยธรรม

คำถาม	ใช่	ไม่ใช่	คำอธิบาย
1.1 สภามหาวิทยาลัย[4]และผู้บริหารกำหนดแนวทาง และมีการปฏิบัติที่อยู่บนหลักความซื่อตรงและการรักษาจรรยาบรรณในการดำเนินงาน ที่ครอบคลุมถึง 1.1.1 การปฏิบัติหน้าที่ประจำวันและการตัดสินใจในเรื่องต่างๆ 1.1.2 การปฏิบัติต่อคู่ค้า ลูกค้า และบุคคลภายนอก			
1.2 มีข้อกำหนดที่เป็นลายลักษณ์อักษรให้ผู้บริหารและพนักงานปฏิบัติหน้าที่ด้วยความซื่อตรงและรักษาจรรยาบรรณ ที่ครอบคลุมถึง *(ในกรณีที่ส่วนงานประเมิน ให้หมายถึงข้อกำหนดของมหาวิทยาลัย หากส่วนงานมีข้อกำหนดเฉพาะ ให้ระบุไว้ด้วย)* 1.2.1 ข้อกำหนดเกี่ยวกับจริยธรรม (code of conduct) สำหรับผู้บริหารและพนักงาน ที่เหมาะสม 1.2.2 ข้อกำหนดห้ามผู้บริหารและพนักงานปฏิบัติตนในลักษณะที่อาจก่อให้เกิดความขัดแย้งทางผลประโยชน์กับองค์กร ซึ่งรวมถึงการห้ามคอร์รัปชันอันทำให้เกิดความเสียหายต่อองค์กร[5] 1.2.3 บทลงโทษที่เหมาะสมหากมีการฝ่าฝืนข้อกำหนดข้างต้น 1.2.4 การสื่อสารข้อกำหนดและบทลงโทษข้างต้นให้ผู้บริหารและพนักงานทุกคนรับทราบ เช่น รวมอยู่ในการปฐมนิเทศพนักงานใหม่ การให้พนักงานลงนามรับทราบข้อกำหนดและบทลงโทษเป็นประจำทุกปี รวมทั้งมีการเผยแพร่ code of conduct ให้แก่พนักงานและบุคคลภายนอกได้รับทราบ			

[3] องค์กร หมายถึง มหาวิทยาลัย หรือส่วนงาน แล้วแต่กรณี

[4] หากเป็นการประเมินในระดับส่วนงาน ให้หมายถึง คณะกรรมการประจำส่วนงาน

[5] มหาวิทยาลัยควรกำหนดการควบคุมภายในตามมาตรการต่อต้านคอร์รัปชันให้เหมาะสมกับความเสี่ยงของมหาวิทยาลัย

คำถาม	ใช่	ไม่ใช่	คำอธิบาย
1.3 มีกระบวนการติดตามและประเมินผลการปฏิบัติตาม Code of Conduct *(ส่วนงาน – ให้ประเมินเฉพาะเมื่อมี code ของส่วนงานเอง)* 1.3.1 การติดตามและประเมินผลโดยหน่วยงานตรวจสอบภายใน 1.3.2 การประเมินตนเองโดยผู้บริหารและพนักงาน 1.3.3 การประเมินโดยผู้เชี่ยวชาญที่เป็นอิสระจากภายนอกองค์กร			
1.4 มีการจัดการอย่างทันเวลา หากพบการไม่ปฏิบัติตามข้อกำหนดเกี่ยวกับความซื่อตรงและการรักษาจรรยาบรรณ 1.4.1 มีกระบวนการที่ทำให้สามารถตรวจพบการฝ่าฝืนได้ภายในเวลาที่เหมาะสม 1.4.2 มีกระบวนการที่ทำให้สามารถลงโทษหรือจัดการกับการฝ่าฝืนได้อย่างเหมาะสม และภายในเวลาอันควร 1.4.3 มีการแก้ไขการกระทำที่ขัดต่อหลักความซื่อตรงและการรักษาจรรยาบรรณอย่างเหมาะสม และภายในเวลาอันควร			

2. สภามหาวิทยาลัยมีความเป็นอิสระจากฝ่ายบริหาร และทำหน้าที่กำกับดูแล (Oversight) และพัฒนาการดำเนินการด้านการควบคุมภายใน *(ส่วนงานไม่ต้องกรอกหมวดนี้)*

คำถาม	ใช่	ไม่ใช่	คำอธิบาย
2.1 มีการกำหนดบทบาทหน้าที่ของสภามหาวิทยาลัยแยกจากฝ่ายบริหาร โดยได้สงวนสิทธิ์อำนาจเฉพาะของสภาฯ ไว้อย่างชัดเจน			
2.2 สภาฯ กำกับดูแลให้มีการกำหนดเป้าหมายการดำเนินงานตามพันธกิจของมหาวิทยาลัยที่ชัดเจนและวัดผลได้ เพื่อเป็นแนวทางในการปฏิบัติงานของผู้บริหารและพนักงาน			
2.3 สภาฯ กำกับดูแลให้มหาวิทยาลัยกำหนดบทบาทหน้าที่ของสภาฯ และผู้บริหารให้ถูกต้องตามพรบ. ของมหาวิทยาลัย ซึ่งครอบคลุมบทบาทที่สำคัญของคณะกรรมการตรวจสอบ ผู้สอบบัญชี ผู้ตรวจสอบภายใน และผู้รับผิดชอบต่อรายงานทางการเงิน			

คำถาม	ใช่	ไม่ใช่	คำอธิบาย
2.4 สภาฯ เป็นผู้มีความรู้เกี่ยวกับพันธกิจของมหาวิทยาลัย และมีความเชี่ยวชาญที่เป็นประโยชน์ต่อมหาวิทยาลัย หรือสามารถขอคำแนะนำจากผู้เชี่ยวชาญในเรื่องนั้นๆได้			
2.5 สภาฯ ประกอบด้วยกรรมการอิสระ (ผู้ทรงคุณวุฒิ) ที่มีความรู้ความสามารถน่าเชื่อถือ และมีความเป็นอิสระในการปฏิบัติหน้าที่อย่างแท้จริง เช่น ไม่มีความสัมพันธ์ทางธุรกิจกับมหาวิทยาลัย ไม่มีความสัมพันธ์อื่นใดอันอาจมีอิทธิพลต่อการใช้ดุลยพินิจและปฏิบัติหน้าที่อย่างเป็นอิสระ และผู้ทรงฯ มีจำนวนที่เหมาะสม และเพียงพอ			
2.6 สภาฯ กำกับดูแลการพัฒนาและปฏิบัติเรื่องการควบคุมภายในในมหาวิทยาลัย ซึ่งครอบคลุมทั้งการสร้างสภาพแวดล้อมการควบคุม การประเมินความเสี่ยง กิจกรรมการควบคุม ข้อมูลและการสื่อสาร และการติดตาม			

3. ฝ่ายบริหารได้จัดให้มีโครงสร้างสายการบังคับบัญชา การกำหนดอำนาจในการสั่งการและความรับผิดชอบที่เหมาะสมเพื่อให้องค์กรบรรลุวัตถุประสงค์ ภายใต้การกำกับดูแล (oversight) ของสภามหาวิทยาลัย

คำถาม	ใช่	ไม่ใช่	คำอธิบาย
3.1 ผู้บริหารระดับสูงกำหนดโครงสร้างองค์กรที่สนับสนุนการบรรลุวัตถุประสงค์ขององค์กร โดยพิจารณาถึงความเหมาะสมทั้งเพื่อการดำเนินพันธกิจและการดำเนินงานตามพรบ. ข้อบังคับ ประกาศ รวมถึงการจัดให้มีการควบคุมภายในอย่างมีประสิทธิภาพ เช่น แบ่งแยกหน้าที่ในส่วนงานที่สำคัญ ซึ่งทำให้เกิดการตรวจสอบถ่วงดุลระหว่างกัน มีงานตรวจสอบภายในที่ขึ้นตรงกับคณะกรรมการตรวจสอบ และมีสายการรายงานที่ชัดเจน เป็นต้น *(ส่วนงานไม่ต้องประเมินเกี่ยวกับงานตรวจสอบภายใน)*			
3.2 ผู้บริหารระดับสูงกำหนดสายการบังคับบัญชาในองค์กร โดยพิจารณาถึงความเหมาะสมเกี่ยวกับอำนาจหน้าที่ ความรับผิดชอบและการสื่อสารข้อมูล			

คำถาม	ใช่	ไม่ใช่	คำอธิบาย
3.3 มีการกำหนด มอบหมาย และจำกัดอำนาจหน้าที่และความรับผิดชอบอย่างเหมาะสมระหว่างสภามหาวิทยาลัย ผู้บริหารระดับสูง ผู้บริหาร และพนักงาน			

4. องค์กรแสดงถึงความมุ่งมั่นในการจูงใจ พัฒนาและรักษาบุคลากรที่มีความรู้ความสามารถ

คำถาม	ใช่	ไม่ใช่	คำอธิบาย
4.1 องค์กรมีนโยบายและวิธีการปฏิบัติเพื่อจัดหา พัฒนา และรักษาบุคลากรที่มีความรู้ ความสามารถที่เหมาะสม และมีกระบวนการสอบทานนโยบายและวิธีการปฏิบัตินั้นอย่างสม่ำเสมอ			
4.2 องค์กรมีกระบวนการประเมินผลการปฏิบัติงาน การให้แรงจูงใจหรือรางวัลต่อบุคลากรที่มีผลการปฏิบัติงานดี และการจัดการต่อบุคลากรที่มีผลงานไม่บรรลุเป้าหมาย รวมถึง การสื่อสารกระบวนการเหล่านี้ให้ผู้บริหารและพนักงานทราบ			
4.3 องค์กรมีกระบวนการแก้ไขปัญหาหรือเตรียมพร้อมสำหรับการขาดบุคลากรที่มีความรู้และความสามารถที่เหมาะสมอย่างทันเวลา			
4.4 องค์กรมีกระบวนการสรรหา พัฒนา และรักษาผู้บริหารและพนักงานทุกคน เช่น การจัดระบบที่ปรึกษา (mentoring) และการฝึกอบรม			
4.5 องค์กรมีแผนและกระบวนการสรรหาผู้สืบทอดตำแหน่ง (succession plan) ที่สำคัญ			

5. องค์กรกำหนดให้บุคลากรมีหน้าที่และความรับผิดชอบในการควบคุมภายใน เพื่อให้บรรลุตามวัตถุประสงค์ขององค์กร

คำถาม	ใช่	ไม่ใช่	คำอธิบาย
5.1 (สภาฯ และ)[6] ผู้บริหารมีกระบวนการและการสื่อสารเชิงบังคับให้บุคลากรทุกคนมีความรับผิดชอบต่อการควบคุมภายใน และจัดให้มีการปรับปรุงแก้ไขกระบวนการปฏิบัติในกรณีที่จำเป็น			

[6] ในกรณีส่วนงาน ให้ไม่ต้องใช้คำในวงเล็บ

คำถาม	ใช่	ไม่ใช่	คำอธิบาย
5.2 (สภาฯ และ) ผู้บริหารกำหนดตัวชี้วัดผลการปฏิบัติงาน การสร้างแรงจูงใจ และการให้รางวัล ที่เหมาะสม โดยพิจารณาทั้งเรื่องการปฏิบัติตาม Code of Conduct และวัตถุประสงค์ในระยะสั้นและระยะยาวขององค์กร			
5.3 (สภาฯ และ) ผู้บริหารประเมินแรงจูงใจและการให้รางวัลอย่างต่อเนื่อง โดยเน้นให้สามารถเชื่อมโยงกับความสำเร็จของหน้าที่ในการปฏิบัติตามการควบคุมภายในด้วย			
5.4 (สภาฯ และ) ผู้บริหารได้พิจารณาไม่ให้มีการสร้างแรงกดดันที่มากเกินไปในการปฏิบัติหน้าที่ของบุคลากรแต่ละคน			

การประเมินความเสี่ยง (Risk Assessment)

6. องค์กรกำหนดวัตถุประสงค์ไว้อย่างชัดเจนเพียงพอ เพื่อให้สามารถระบุและประเมินความเสี่ยงต่างๆ ที่เกี่ยวข้องกับการบรรลุวัตถุประสงค์ขององค์กร

คำถาม	ใช่	ไม่ใช่	คำอธิบาย
6.1 องค์กรสามารถปฏิบัติตามมาตรฐานการบัญชีที่รับรองโดยทั่วไปและเหมาะสมกับองค์กรในขณะนั้น โดยแสดงได้ว่ารายการในรายงานทางการเงินมีตัวตนจริง ครบถ้วน แสดงถึงสิทธิหรือภาระผูกพันขององค์กรได้ถูกต้อง มีมูลค่าเหมาะสม (เช่น รายการที่ต้องมีการประเมินมูลค่า หรือค่าเผื่อทางบัญชี) และเปิดเผยข้อมูลครบถ้วน ถูกต้อง			
6.2 องค์กรกำหนดสาระสำคัญของรายการทางการเงิน โดยพิจารณาถึงปัจจัยที่สำคัญ เช่น ผู้ใช้รายงานทางการเงิน ขนาดของรายการ แนวโน้มของบริการตามพันธกิจ			
6.3 รายงานทางการเงินขององค์กรสะท้อนถึงกิจกรรมการดำเนินงานขององค์กรอย่างแท้จริง			
6.4 สภาฯ หรือคณะกรรมการบริหารความเสี่ยง อนุมัติและสื่อสารนโยบายการบริหารความเสี่ยงให้ผู้บริหารและพนักงานทุกคนรับทราบและถือปฏิบัติ จนเป็นส่วนหนึ่งของวัฒนธรรมขององค์กร			

7. องค์กรระบุและวิเคราะห์ความเสี่ยงทุกประเภทที่อาจกระทบต่อการบรรลุวัตถุประสงค์ไว้อย่างครอบคลุมทั่วทั้งองค์กร

คำถาม	ใช่	ไม่ใช่	คำอธิบาย
7.1 องค์กรระบุความเสี่ยงทุกประเภทซึ่งอาจมีผลกระทบต่อการดำเนินงานตามพันธกิจทั้งระดับองค์กร ฝ่าย งาน หน่วย			
7.2 องค์กรวิเคราะห์ความเสี่ยงทุกประเภทที่อาจเกิดจากทั้งปัจจัยภายในและปัจจัยภายนอกองค์กร ซึ่งรวมถึงความเสี่ยงด้านกลยุทธ์ การดำเนินงาน การรายงาน การปฏิบัติตามกฎเกณฑ์ และด้านเทคโนโลยีสารสนเทศ			
7.3 ผู้บริหารทุกระดับมีส่วนร่วมในการบริหารความเสี่ยง			
7.4 องค์กรได้ประเมินความสำคัญของความเสี่ยง โดยพิจารณาทั้งโอกาสเกิดเหตุการณ์ และผลกระทบที่อาจเกิดขึ้น			
7.5 องค์กรมีมาตรการและแผนปฏิบัติงานเพื่อจัดการความเสี่ยง โดยอาจเป็นการยอมรับความเสี่ยงนั้น (acceptance) การลดความเสี่ยง (reduction) การหลีกเลี่ยงความเสี่ยง (avoidance) หรือการร่วมรับความเสี่ยง (sharing)			

8. องค์กรได้พิจารณาถึงโอกาสที่จะเกิดการทุจริต ในการประเมินความเสี่ยงที่จะบรรลุวัตถุประสงค์ขององค์กร

คำถาม	ใช่	ไม่ใช่	คำอธิบาย
8.1 องค์กรประเมินโอกาสที่จะเกิดการทุจริตขึ้น โดยครอบคลุมการทุจริตแบบต่างๆ เช่น การจัดทำรายงานทางการเงินเท็จ การทำให้สูญเสียทรัพย์สิน การคอร์รัปชัน การที่ผู้บริหารสามารถฝ่าฝืนระบบควบคุมภายใน (management override of internal controls) การเปลี่ยนแปลงข้อมูลในรายงานที่สำคัญ การได้มาหรือใช้ไปซึ่งทรัพย์สินโดยไม่ถูกต้อง เป็นต้น			
8.2 องค์กรได้ทบทวนเป้าหมายการปฏิบัติงานอย่างรอบคอบโดยพิจารณาความเป็นไปได้ของเป้าหมายที่กำหนดแล้ว รวมทั้งได้พิจารณาความสมเหตุสมผลของการให้สิ่งจูงใจหรือผลตอบแทนแก่พนักงานแล้วด้วยว่า ไม่มีลักษณะส่งเสริมให้พนักงานกระทำไม่			

คำถาม	ใช่	ไม่ใช่	คำอธิบาย
เหมาะสม เช่น ไม่ตั้งเป้าหมายการดำเนินงานไว้สูงเกินจริงจนทำให้เกิดแรงจูงใจในการตกแต่งตัวเลขเพื่อให้รายงานได้ว่าได้ผลตามเป้า เป็นต้น			
8.3 คณะกรรมการตรวจสอบได้พิจารณาและสอบถามผู้บริหารเกี่ยวกับโอกาสในการเกิดทุจริต และมาตรการที่องค์กรดำเนินการเพื่อป้องกันหรือแก้ไขการทุจริต *(ส่วนงานไม่ต้องประเมินข้อนี้)*			
8.4 องค์กรได้สื่อสารให้พนักงานทุกคนเข้าใจและปฏิบัติตามนโยบายและแนวปฏิบัติที่กำหนดไว้			

9. องค์กรสามารถระบุและประเมินความเปลี่ยนแปลงที่อาจมีผลกระทบต่อระบบการควบคุมภายใน

คำถาม	ใช่	ไม่ใช่	คำอธิบาย
9.1 องค์กรประเมินการเปลี่ยนแปลงจากปัจจัยภายนอก ที่อาจมีผลกระทบต่อการให้บริการ การควบคุมภายใน และการรายงานทางการเงิน ตลอดจนได้กำหนดมาตรการตอบสนองต่อการเปลี่ยนแปลงนั้นอย่างเพียงพอแล้ว			
9.2 องค์กรประเมินการเปลี่ยนแปลงรูปแบบการให้บริการ ที่อาจมีผลกระทบต่อการดำเนินงานตามพันธกิจ การควบคุมภายใน และการรายงานทางการเงิน ตลอดจนได้กำหนดมาตรการตอบสนองต่อการเปลี่ยนแปลงนั้นอย่างเพียงพอแล้ว			
9.3 องค์กรประเมินการเปลี่ยนแปลงผู้นำองค์กร ที่อาจมีผลกระทบต่อการดำเนินงาน การควบคุมภายใน และการรายงานทางการเงิน ตลอดจนได้กำหนดมาตรการตอบสนองต่อการเปลี่ยนแปลงนั้นอย่างเพียงพอแล้ว			

การควบคุมการปฏิบัติงาน (Control Activities)

10. องค์กรมีมาตรการควบคุมที่ช่วยลดความเสี่ยงที่จะไม่บรรลุวัตถุประสงค์ขององค์กร ให้อยู่ในระดับที่ยอมรับได้

คำถาม	ใช่	ไม่ใช่	คำอธิบาย
10.1 มาตรการควบคุมขององค์กรมีความเหมาะสมกับความเสี่ยงและลักษณะเฉพาะขององค์กร เช่น สภาพแวดล้อม ความซับซ้อนของงาน ลักษณะงาน ขอบเขตการดำเนินงาน รวมถึงลักษณะเฉพาะอื่น ๆ			
10.2 องค์กรมีมาตรการควบคุมภายในที่กำหนดเป็นลายลักษณ์อักษร และครอบคลุมกระบวนการต่างๆ อย่างเหมาะสม เช่น มีนโยบายและระเบียบวิธีปฏิบัติงานเกี่ยวกับการจัดเก็บค่าบริการ การรับและนำส่งเงิน การพัสดุ การบริหารงานบุคคล ตลอดจนกำหนดขอบเขต อำนาจหน้าที่ และลำดับชั้นการอนุมัติของผู้บริหารในแต่ละระดับไว้อย่างชัดเจน รัดกุม เพื่อให้สามารถป้องกันการทุจริตได้ เช่น มีการกำหนดขนาดวงเงินและอำนาจอนุมัติของผู้บริหารแต่ละระดับ ขั้นตอนในการอนุมัติโครงการลงทุน โครงการมูลค่าสูงอื่นๆ ขั้นตอนการจัดซื้อและวิธีการคัดเลือกผู้ขาย การบันทึกข้อมูลรายละเอียดการตัดสินใจจัดซื้อ ขั้นตอนการเบิกจ่ายวัสดุอุปกรณ์ หรือ การเบิกใช้เครื่องมือต่างๆ เป็นต้น โดยได้จัดให้มีกระบวนการสำหรับกรณีต่าง ๆ ดังนี้ 10.2.1 การเก็บรวบรวมข้อมูลเกี่ยวกับกรรมการสภาฯ ผู้บริหาร และผู้ที่เกี่ยวข้อง (Connected Person) กับบุคคลดังกล่าว *(เช่น ผู้ที่มีอำนาจต่อการตัดสินใจของกรรมการ และผู้บริหาร คู่สมรส รวมทั้งบุตรที่ยังไม่บรรลุนิติภาวะ)* รวมทั้งบุคคลที่เกี่ยวโยงกัน (Related Person) *(เช่น บิดา มารดา พี่ น้อง บุตร และคู่สมรส)* เพื่อประโยชน์ในการติดตามและสอบทานการทำรายการระหว่างกัน หรือรายการที่อาจมีความขัดแย้งทางผลประโยชน์ รวมทั้งมีการปรับปรุงข้อมูลให้เป็นปัจจุบันเสมอ 10.2.2 กรณีที่องค์กรอนุมัติธุรกรรมหรือทำสัญญากับผู้ที่เกี่ยวข้องในลักษณะที่มีผลผูกพันองค์กรในระยะยาวไปแล้ว องค์กรได้ติดตามให้มั่นใจได้ว่า มีการปฏิบัติตามเงื่อนไขที่ตกลงกันไว้ตลอดระยะเวลาที่มีผลผูกพันองค์กร หรือได้มีการทบทวนความเหมาะสมของสัญญาเป็นระยะๆ เป็นต้น			

คำถาม	ใช่	ไม่ใช่	คำอธิบาย
10.3 องค์กรกำหนดให้การควบคุมภายในมีความหลากหลายอย่างเหมาะสม เช่น การควบคุมแบบ manual และ automated หรือการควบคุมแบบป้องกันและติดตาม			
10.4 องค์กรกำหนดให้มีการควบคุมภายในในทุกระดับขององค์กร เช่น ระดับ cluster ส่วนงาน ฝ่าย กอง งาน หน่วย กระบวนการ			
10.5 องค์กรมีการแบ่งแยกหน้าที่ความรับผิดชอบในงาน 3 ด้านต่อไปนี้ ออกจากกันโดยเด็ดขาด เพื่อเป็นการตรวจสอบซึ่งกันและกัน กล่าวคือ (1) หน้าที่อนุมัติ (2) หน้าที่บันทึกรายการบัญชีและข้อมูลสารสนเทศ และ (3) หน้าที่ในการดูแลจัดเก็บทรัพย์สิน			

11. องค์กรเลือกและพัฒนากิจกรรมการควบคุมทั่วไปด้วยระบบเทคโนโลยี เพื่อช่วยสนับสนุนการบรรลุวัตถุประสงค์

คำถาม	ใช่	ไม่ใช่	คำอธิบาย
11.1 องค์กรกำหนดความเกี่ยวข้องกันระหว่างการใช้เทคโนโลยีสารสนเทศในกระบวนการปฏิบัติงาน และการควบคุมทั่วไปของระบบสารสนเทศ			
11.2 องค์กรกำหนดการควบคุมของโครงสร้างพื้นฐานของระบบเทคโนโลยีให้มีความเหมาะสม			
11.3 องค์กรกำหนดการควบคุมด้านความปลอดภัยของระบบเทคโนโลยีให้มีความเหมาะสม			
11.4 องค์กรกำหนดการควบคุมกระบวนการได้มา การพัฒนาและการบำรุงรักษาระบบเทคโนโลยีให้มีความเหมาะสม			

12. องค์กรจัดให้มีกิจกรรมการควบคุมผ่านทางนโยบาย ซึ่งได้กำหนดสิ่งที่คาดหวังและขั้นตอนการปฏิบัติ เพื่อให้นโยบายที่กำหนดไว้นั้นสามารถนำไปสู่การปฏิบัติได้

คำถาม	ใช่	ไม่ใช่	คำอธิบาย
12.1 องค์กรมีนโยบายที่รัดกุมเพื่อติดตามให้การทำธุรกรรมระหว่างองค์กรกับกรรมการสภาฯ ผู้บริหาร พนักงาน หรือผู้ที่เกี่ยวข้องกับบุคคลดังกล่าว ต้องผ่านขั้นตอนการอนุมัติที่กำหนด เช่น อาจอ้างอิงแนวปฏิบัติของปปช. เพื่อป้องกันการหาโอกาสหรือนำผลประโยชน์ขององค์กรไปใช้ส่วนตัว			
12.2 องค์กรมีนโยบายให้การพิจารณาอนุมัติธุรกรรม ต้องกระทำโดยผู้ที่ไม่มีส่วนได้เสียในธุรกรรมนั้น			
12.3 องค์กรมีนโยบายเพื่อให้การพิจารณาอนุมัติธุรกรรมกับกรรมการสภาฯ ผู้บริหาร พนักงาน หรือผู้ที่เกี่ยวข้องกับบุคคลดังกล่าว ต้องคำนึงถึงประโยชน์สูงสุดขององค์กรเป็นสำคัญ โดยเฉพาะราคา ต้องสามารถเปรียบเทียบกับราคาตลาดได้เสมือนเป็นรายการที่กระทำกับบุคคลภายนอกทั่วไป (at arms' length basis)			
12.4 องค์กรมีกระบวนการติดตามดูแลการดำเนินงานของส่วนงานย่อยขององค์กร รวมทั้งกำหนดแนวทางให้บุคคลที่องค์กรแต่งตั้งให้เป็นผู้บริหารนั้นถือปฏิบัติ *(หากไม่มี ให้เขียน N/A)*			
12.5 องค์กรกำหนดหน้าที่และความรับผิดชอบให้ผู้บริหารและพนักงานนำนโยบายและกระบวนการไปใช้ปฏิบัติ			
12.6 มีการถือปฏิบัติตามนโยบายและกระบวนการปฏิบัติงานขององค์กรอย่างเหมาะสม บุคลากรมีความสามารถ มีความเข้าใจ และกระบวนการปฏิบัติงานครอบคลุมถึงการแก้ไขข้อผิดพลาดที่อาจเกิดขึ้นในการปฏิบัติงาน			
12.7 องค์กรกำหนดให้ต้องมีการทบทวนนโยบายและกระบวนการปฏิบัติให้มีความเหมาะสมอยู่เสมอ			

ระบบสารสนเทศและการสื่อสารข้อมูล (Information & Communication)

13. องค์กรมีข้อมูลที่เกี่ยวข้องและมีคุณภาพ เพื่อสนับสนุนให้การควบคุมภายในสามารถดำเนินไปได้ตามที่กำหนดไว้

คำถาม	ใช่	ไม่ใช่	คำอธิบาย
13.1 องค์กรกำหนดข้อมูลที่ต้องการใช้ในการดำเนินงาน ทั้งข้อมูลจากภายในและภายนอกองค์กร ที่มีคุณภาพและเกี่ยวข้องต่องาน			
13.2 องค์กรพิจารณาทั้งต้นทุนและประโยชน์ที่จะได้รับ รวมถึงปริมาณและความถูกต้องของข้อมูล			
13.3 องค์กรดำเนินการเพื่อให้สภาฯ / คณะกรรมการประจำส่วนงาน มีข้อมูลที่สำคัญอย่างเพียงพอสำหรับใช้ประกอบการตัดสินใจ ตัวอย่างข้อมูลที่สำคัญ เช่น รายละเอียดของเรื่องที่เสนอ ให้พิจารณา เหตุผล ผลกระทบต่อองค์กร และทางเลือกต่าง ๆ			
13.4 องค์กรดำเนินการเพื่อให้กรรมการสภาฯ / คณะกรรมการประจำส่วนงาน ได้รับหนังสือนัดประชุมหรือเอกสารประกอบการประชุมที่ระบุข้อมูลที่จำเป็นและเพียงพอต่อการพิจารณาก่อนการประชุมล่วงหน้าก่อนการประชุมนานพอควร			
13.5 องค์กรดำเนินการเพื่อให้รายงานการประชุมสภาฯ / คณะกรรมการประจำส่วนงาน มีรายละเอียดตามควร เพื่อให้สามารถตรวจสอบย้อนหลังเกี่ยวกับความเหมาะสมในการปฏิบัติหน้าที่ของกรรมการแต่ละราย เช่น การบันทึกข้อซักถามของกรรมการ ความเห็นหรือข้อสังเกตของกรรมการในเรื่องที่พิจารณา ความเห็นของกรรมการรายที่ไม่เห็นด้วยกับเรื่องที่เสนอพร้อมเหตุผล เป็นต้น			
13.6 องค์กรมีการดำเนินการดังต่อไปนี้ 13.6.1 มีการจัดเก็บเอกสารสำคัญ ไว้อย่างครบถ้วนเป็นหมวดหมู่ 13.6.2 กรณีที่ได้รับแจ้งจากผู้สอบบัญชีหรือผู้ตรวจสอบภายในว่ามีข้อบกพร่องในการควบคุมภายใน องค์กรได้แก้ไขข้อบกพร่องนั้นอย่างครบถ้วนแล้ว			

14. องค์กรได้สื่อสารกับหน่วยงานภายใน ซึ่งรวมถึงวัตถุประสงค์และความรับผิดชอบต่อการควบคุมภายในที่จำเป็นต่อการสนับสนุนให้การควบคุมภายในสามารถดำเนินไปได้ตามที่วางไว้

คำถาม	ใช่	ไม่ใช่	คำอธิบาย
14.1 องค์กรมีกระบวนการสื่อสารข้อมูลภายในอย่างมีประสิทธิภาพ และมีช่องทางการสื่อสารที่เหมาะสม เพื่อสนับสนุนการควบคุมภายใน			

คำถาม	ใช่	ไม่ใช่	คำอธิบาย
14.2 องค์กรมีการรายงานข้อมูลที่สำคัญถึงสภาฯ / คณะกรรมการประจำส่วนงาน อย่างสม่ำเสมอ และกรรมการสามารถเข้าถึงแหล่งสารสนเทศที่จำเป็นต่อการปฏิบัติงาน หรือสอบทานรายการต่าง ๆ ตามที่ต้องการ เช่น การกำหนดบุคคลที่เป็นศูนย์ติดต่อเพื่อให้สามารถติดต่อขอข้อมูลอื่นนอกจากที่ได้รับจากผู้บริหาร รวมทั้งการติดต่อสอบถามข้อมูลจากผู้สอบบัญชี ผู้ตรวจสอบภายใน การจัดประชุมเพิ่มเติมระหว่างกรรมการและผู้บริหารตามที่สภาฯ / คณะกรรมการร้องขอเมื่อมีกรณีจำเป็น			
14.3 องค์กรจัดให้มีช่องทางการสื่อสาร เพื่อให้บุคคลากรภายในองค์กรสามารถแจ้งข้อมูลหรือเบาะแสเกี่ยวกับการฉ้อฉลหรือทุจริตภายในองค์กร (whistle-blower hotline) ได้อย่างปลอดภัย			

15. องค์กรได้สื่อสารกับหน่วยงานภายนอก เกี่ยวกับประเด็นที่อาจมีผลกระทบต่อการควบคุมภายใน

คำถาม	ใช่	ไม่ใช่	คำอธิบาย
15.1 องค์กรมีกระบวนการสื่อสารข้อมูลกับผู้มีส่วนได้ส่วนเสียภายนอกอย่างมีประสิทธิภาพ เพื่อสนับสนุนการควบคุมภายใน เช่น การจัดให้มีศูนย์รับเรื่องร้องเรียน ร้องทุกข์			
15.2 องค์กรจัดให้มีช่องทางการสื่อสารทั้งทางปกติ และทางลับ เพื่อให้ผู้มีส่วนได้ส่วนเสียภายนอกสามารถแจ้งข้อมูลหรือเบาะแสเกี่ยวกับการฉ้อฉลหรือทุจริต (whistle-blower hotline) แก่องค์กรได้อย่างปลอดภัย			

ระบบการติดตาม (Monitoring Activities)

16. องค์กรติดตามและประเมินผลการควบคุมภายใน เพื่อให้มั่นใจได้ว่าการควบคุมภายในยังดำเนินไปอย่างครบถ้วน เหมาะสม

คำถาม	ใช่	ไม่ใช่	คำอธิบาย
16.1 องค์กรจัดให้มีกระบวนการติดตามการปฏิบัติตามจริยธรรมองค์กรและข้อกำหนดห้ามฝ่ายบริหารและพนักงานปฏิบัติตนใน			

คำถาม	ใช่	ไม่ใช่	คำอธิบาย
ลักษณะที่อาจก่อให้เกิดความขัดแย้งทางผลประโยชน์ เช่น กำหนดให้แต่ละส่วนงานติดตามการปฏิบัติและรายงานผู้บังคับบัญชา หรือมอบหมายให้หน่วยงานตรวจสอบภายในติดตามการปฏิบัติและรายงานต่อคณะกรรมการตรวจสอบ เป็นต้น			
16.2 องค์กรจัดให้มีการตรวจสอบการปฏิบัติตามระบบการควบคุมภายในที่วางไว้โดยการประเมินตนเอง และ/หรือการประเมินอิสระโดยผู้ตรวจสอบภายใน			
16.3 ความถี่ในการติดตามและประเมินผลมีความเหมาะสมกับการเปลี่ยนแปลงขององค์กร			
16.4 ผู้ที่ทำการติดตามและประเมินผลระบบการควบคุมภายใน เป็นผู้มีความรู้และความสามารถ			
16.5 องค์กรกำหนดแนวทางการรายงานผลการตรวจสอบภายในให้ขึ้นตรงต่อคณะกรรมการตรวจสอบ			
16.6 องค์กรส่งเสริมให้ผู้ตรวจสอบภายในปฏิบัติหน้าที่ตามมาตรฐานสากลการปฏิบัติงานวิชาชีพการตรวจสอบภายใน (International Standards for the Professional Practice of Internal Auditing, IIA)			

17. องค์กรประเมินและสื่อสารข้อบกพร่องของการควบคุมภายในอย่างทันเวลาต่อบุคคลที่รับผิดชอบ ซึ่งรวมถึงผู้บริหารระดับสูง และสภาฯ / คณะกรรมการประจำส่วนงานตามความเหมาะสม

คำถาม	ใช่	ไม่ใช่	คำอธิบาย
17.1 องค์กรประเมินผลและสื่อสารข้อบกพร่องของการควบคุมภายในและดำเนินการเพื่อติดตามแก้ไขอย่างทันท่วงที หากการดำเนินงานที่เกิดขึ้นแตกต่างจากเป้าหมายหรือแนวทางที่กำหนดไว้อย่างมีนัยสำคัญ			
17.2 องค์กรมีนโยบายการรายงาน ดังนี้ 17.2.1 ฝ่ายบริหารต้องรายงานต่อสภาฯ / คณะกรรมการประจำส่วนงานโดยพลันในกรณีที่เกิดเหตุการณ์หรือข้อสงสัยว่ามีเหตุการณ์ทุจริตอย่างร้ายแรง มีการปฏิบัติที่ฝ่าฝืนกฎหมาย หรือมีการกระทำที่			

คำถาม	ใช่	ไม่ใช่	คำอธิบาย
ผิดปกติอื่น ซึ่งอาจกระทบต่อชื่อเสียงและฐานะการเงินขององค์กรอย่างมีนัยสำคัญ 17.2.2 รายงานข้อบกพร่องที่เป็นสาระสำคัญ พร้อมแนวทางการแก้ไขปัญหา (แม้ว่าจะได้เริ่มดำเนินการจัดการแล้ว) ต่อสภาฯ หรือคณะกรรมการตรวจสอบ เพื่อพิจารณาภายในระยะเวลาอันควร 17.2.3 รายงานความคืบหน้าในการปรับปรุงข้อบกพร่องที่เป็นสาระสำคัญต่อสภาฯ หรือคณะกรรมการตรวจสอบ จนแก้ไขข้อบกพร่องได้แล้วเสร็จ			

การนำไปใช้

องค์กรควรใช้แบบประเมินนี้เป็นแนวทางในการประเมินหรือทบทวนความเพียงพอของระบบควบคุมภายในอย่างน้อยปีละครั้ง และอาจมีการทบทวนเพิ่มเติมหากเกิดเหตุการณ์ที่อาจส่งผลกระทบต่อการดำเนินงานขององค์กรอย่างมีนัยสำคัญ

การประเมินดังกล่าวควรผ่านการพิจารณาของคณะกรรมการตรวจสอบและสภามหาวิทยาลัยด้วย เพื่อให้เกิดการแลกเปลี่ยนความเห็น มีความเข้าใจตรงกัน และสามารถกำหนดแนวทางปฏิบัติที่เหมาะสมกับมหาวิทยาลัยได้

18 เมษายน 2560

.....

ข้อมูลอ้างอิง

- บทความ COSO 2013 ความเปลี่ยนแปลงจาก COSO 1992 (https://chirapon.wordpress.com/2013/10/09/coso-2013-ความเปลี่ยนแปลงจาก-coso-1992-1/) เขียนโดย อาจารย์ จิรพร สุเมธีประสิทธิ์ ที่ปรึกษาอิสระ ประเภท A เลขทะเบียนสมาชิก 4276 ศูนย์ข้อมูลที่ปรึกษาไทย กระทรวงการคลัง

- แบบประเมินความเพียงพอของระบบควบคุมภายใน ของก.ล.ต. ตามแนวคิดของ COSO ที่ได้ปรับปรุง framework ใหม่ เมื่อเดือนพฤษภาคม 2556 และนำมาปรับให้เข้าใจง่ายขึ้น