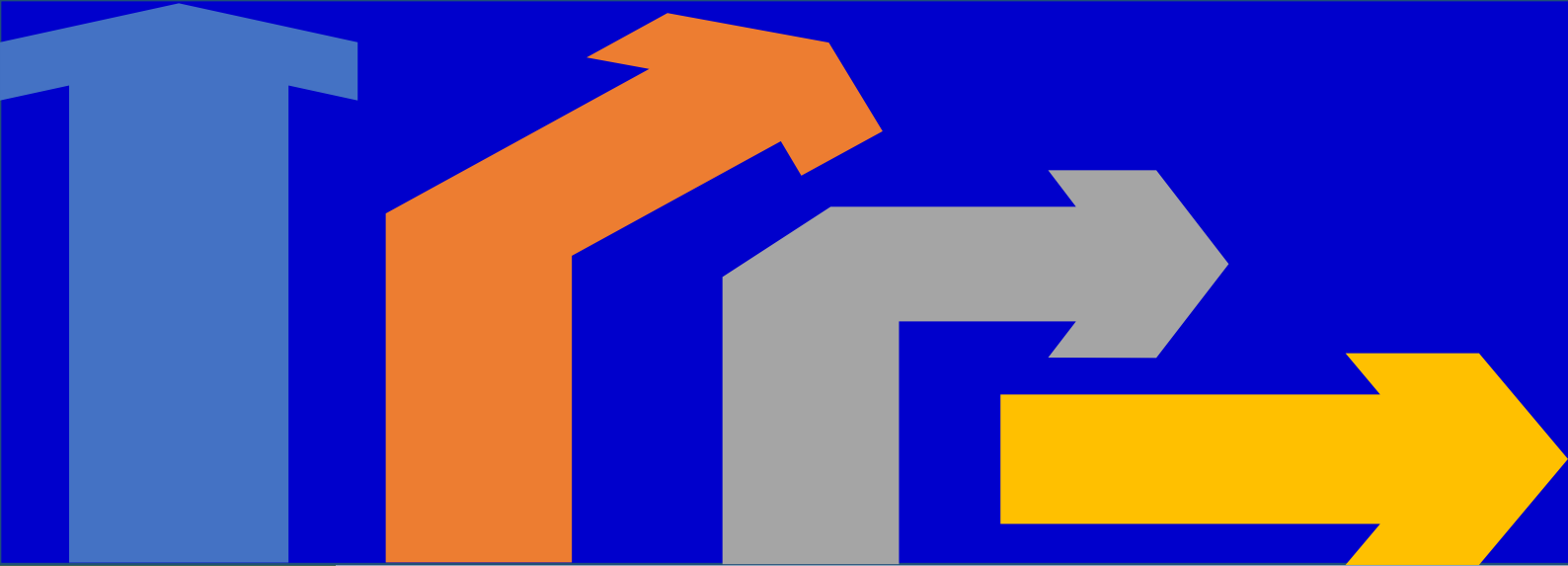




COMPLIANCE NEW GUIDEBOOK

แนวคิดและกระบวนการจัดวางอย่างครบวงจร
รองรับเศรษฐกิจกระแสใหม่

เล่มที่ 1

การปรับใช้ตามมาตรฐานสากล 4 ฉบับ

อาจารย์ จิรพร สุ่มะธีประสิทธิ์

COMPLIANCE NEW GUIDEBOOK

แนวคิดและกระบวนการจัดวางอย่างครบวงจร

รองรับเศรษฐกิจกระแสใหม่

เล่มที่ 1 การปรับใช้ตามมาตรฐานสากล 4 ฉบับ

อาจารย์ จิรพร สุเมธีประสิทธิ์

ข้อมูลทางบรรณานุกรมของสำนักหอสมุดแห่งชาติ

National Library of Thailand Cataloging in Publication Data

อาจารย์ จิรพร สุเมธีประสิทธิ์

COMPLIANCE NEW GUIDEBOOK

แนวคิดและกระบวนการจัดวางอย่างครบวงจรรองรับเศรษฐกิจกระแสใหม่

เล่มที่ 1 การปรับใช้ตามมาตรฐานสากล 4 ฉบับ

191 หน้า

ISBN (E-Book) 978-616-612-143-8

สงวนสิทธิ์ ตามพระราชบัญญัติลิขสิทธิ์ (ฉบับเพิ่มเติม) พ.ศ. 2558

พิมพ์ครั้งที่ 1 : พ.ศ. 2567

จำหน่ายในรูปแบบ : E-Book

ราคา : 179 บาท

จัดทำโดย : อาจารย์ จิรพร สุเมธีประสิทธิ์

ออกแบบปก : อาจารย์ จิรพร สุเมธีประสิทธิ์

สั่งซื้อได้ที่ : ศูนย์หนังสือแห่งจุฬาลงกรณ์มหาวิทยาลัย

ถนนพญาไท เขตปทุมวัน กรุงเทพฯ 10330

<http://www.chulabook.com>

โทร.086-323-3703-4

customer@cubook.chula.ac.th, info@cubook.chula.ac.th

Apps: CU-eBook Store

คำนำ

หนังสือ COMPLIANCE NEW GUIDEBOOK แนวคิดและกระบวนการจัดวางอย่างเป็นระบบรองรับเศรษฐกิจกระแสใหม่ เล่มที่ 1 การปรับใช้ตามมาตรฐานสากล 4 ฉบับ เป็นหนึ่งในชุดของ COMPLIANCE NEW GUIDEBOOK ที่ต้องแยกจัดทำออกเป็น 4 เล่มย่อย เพื่อให้มีรายละเอียดที่เพียงพอในการนำไปใช้ สำหรับเจ้าหน้าที่กำกับการปฏิบัติตามกฎเกณฑ์ซึ่งถือเป็นวิชาชีพใหม่ที่นับวันจะมีความสำคัญต่อทุกองค์กรและกิจกรรมทุกประเภทมากขึ้นอย่างรวดเร็ว จนไม่สามารถให้บุคลากรที่มีคุณสมบัติด้านความรู้ความเข้าใจที่ไม่ลึกซึ้งและกว้างขวางเพียงพอมาปฏิบัติงานในด้านนี้ได้

แรงบันดาลใจที่ทำให้ผู้เขียน ตัดสินใจออกหนังสือ COMPLIANCE NEW GUIDEBOOK ในรูปแบบของการอ่านแบบ e-BOOK มาจากปัจจัยหลายประการ นับตั้งแต่ประสบการณ์ในการเป็นวิทยากรบรรยาย หลักสูตร การกำกับการปฏิบัติตามกฎเกณฑ์มาเป็นระยะเวลานาน ได้มีโอกาสและได้รับความไว้วางใจจากองค์กรทั้งภาครัฐและเอกชนให้เป็นที่ปรึกษาเพื่อช่วยชี้แนะการพัฒนาระบบกำกับการปฏิบัติตามกฎเกณฑ์ ที่เป็นวัตถุประสงค์หลักประการหนึ่งของระบบการควบคุมภายใน การเรียกร้องจากลูกค้าลูกหาที่ได้มีโอกาสให้การอบรมขอให้นำเอาสิ่งที่ได้บรรยายและประสบการณ์จริงรวบรวมเป็นตำราเพื่อใช้อ้างอิงในการปฏิบัติงานเชิงวิชาชีพ ซึ่งสอดคล้องกับความตั้งใจของผู้เขียนเองที่จะถ่ายทอดประสบการณ์ที่เกิดขึ้นจริง ทั้งไว้ให้ได้ใช้ประโยชน์ในแวดวงวิชาการ

อย่างไรก็ดี กว่าจะได้เป็นต้นฉบับสุดท้ายของ COMPLIANCE NEW GUIDEBOOK เล่มที่ 1 ฉบับที่ได้มีโอกาสปรากฏต่อท่านในที่นี่ ต้องมีการเปลี่ยนแปลงเนื้อหาให้เป็นปัจจุบันมากขึ้นอยู่หลายครั้งเนื่องจากขอบเขตของกฎเกณฑ์ที่อยู่ในข่ายต้องให้ความสำคัญในการกำกับการปฏิบัติ ขยายพรมแดนจากด้านของกฎหมายโดยตรงออกไปสู่กฎเกณฑ์ที่กำกับองค์กร ให้มีการดำเนินธุรกิจบนหลักความรับผิดชอบต่อสังคมและสิ่งแวดล้อม หรือที่รู้จักกันในชื่อของ ESG หรือ SDGs ด้วย

ผู้เขียนหวังอย่างยิ่งว่า หลังจากที่ท่านได้มีโอกาสได้อ่านเนื้อหาในรายละเอียดของ COMPLIANCE NEW GUIDEBOOK เล่มที่ 1 ที่เน้นเรื่องของมาตรฐานสากล ที่สนับสนุนและผลักดันให้เกิดกลไกและระบบการกำกับการปฏิบัติตามกฎเกณฑ์แล้ว ท่านจะติดตามผลงานในเล่มต่อไปอีก 3 เล่ม เพื่อให้สามารถนำไปใช้เป็นคู่มือสำหรับเจ้าหน้าที่กำกับการปฏิบัติตามกฎเกณฑ์ได้อย่างเพียงพอและครบถ้วน

อาจารย์ จิรพร สุเมธีประสิทธิ์

ผู้เขียน



สารบัญ

	หน้า
บทนำ	1
มาตรฐานสากลที่เกี่ยวข้องกับการกำกับการปฏิบัติตามกฎเกณฑ์	
1. ความเป็นมา	1
2. กำกับด้วย 4 มาตรฐานสากลที่สำคัญ	2
มาตรฐาน COSO 2013	2
มาตรฐาน COSO ERM 2017	3
มาตรฐาน GRC ของ OCEG	3
มาตรฐาน ISO 37301 : 2021	4
3. การใช้ 2 แนวปฏิบัติที่ดีเพื่อสนับสนุนเพิ่มเติม	5
แนวปฏิบัติที่ดีในการแบ่งความรับผิดชอบตาม Four Lines of Defense และ Five Lines of Defense	6
แนวปฏิบัติที่ดีด้าน Compliance ขององค์กร OECD	7
4. บทสรุปที่สำคัญ	9
5. พัฒนาการงานกำกับการปฏิบัติตามกฎเกณฑ์	10
บทที่ 1	13
นิยามการกำกับการปฏิบัติตามกฎเกณฑ์และความเสี่ยงที่เกี่ยวข้อง	
1. นิยามและความหมายของการกำกับการปฏิบัติตามกฎเกณฑ์	13
2. วงจรของการกำกับการปฏิบัติตามกฎเกณฑ์	15
3. นิยามและรูปแบบของความเสี่ยงด้านการกำกับการปฏิบัติตามกฎเกณฑ์	22
4. สาเหตุของความเสี่ยงด้านการกำกับการปฏิบัติตามกฎเกณฑ์	26
5. หลักการและเงื่อนไขการวิเคราะห์และประเมินความเสี่ยงด้านการกำกับการปฏิบัติตามกฎเกณฑ์	29



	หน้า
6. ความท้าทายของการกำหนดขอบเขตและการแบ่งแยกงานบริหาร COMPLIANCE	30
บทที่ 2	33
มาตรฐานสากล 1: COSO 2013: Integrated Internal Control Framework	
1. องค์ประกอบที่สำคัญตามมาตรฐาน COSO 2013	34
ส่วนที่ 1 วัตถุประสงค์ของการควบคุมภายใน (Control Objectives)	34
ส่วนที่ 2 ระดับการควบคุมภายในขององค์กร (Control level)	36
ส่วนที่ 3 ประเภทของความเสี่ยงที่องค์กรต้องมีการจัดการ	38
2. การนำเอา COSO 2013 มาปรับใช้ในงาน Compliance	42
ส่วนที่ 1 การปรับใช้ในตารางหรือเมทริกซ์อำนาจการอนุมัติ (Table or Matrix of Authority)	42
ส่วนที่ 2 การปรับใช้การกำกับการปฏิบัติตามกฎเกณฑ์แทรกในระดับกระบวนการ (Process-level of Compliance) เพื่อกำกับตนเอง	52
3. หลักเกณฑ์การพิจารณาเพิ่มบทบาท Compliance ในระดับกระบวนการ	55
หลักการมีบทบาทของการกำกับการปฏิบัติตามกฎเกณฑ์	56
บทที่ 3	59
มาตรฐานสากล 2: COSO ERM 2017	
1. หลักการ เหตุผล ความเป็นมา	59
2. กฎหมาย SOX Act กำกับการบริหารความเสี่ยงด้านกำกับการปฏิบัติตามกฎเกณฑ์	60
หลักการที่ 1 การควบคุมภายในต้องทำรายงานและเปิดเผยสาธารณะ	61



	หน้า
หลักการที่ 2 หน่วยงาน COMPLIANCE UNIT ต้องดูแลทั่วทั้งองค์กร	61
หลักการที่ 3 Compliance Unit เป็นกฤษฎีกาภายในองค์กร	62
3. การบริหารความเสี่ยงการกำกับการปฏิบัติตามกฎเกณฑ์ภายใต้กรอบ COSO ERM	64
1) องค์ประกอบของ Framework for Effective Compliance and Ethics Programs	65
2) การกำกับดูแล ผู้มีอำนาจกระทำการ และสถานะภาพในองค์กรรวม (Oversight) ขององค์กร	70
3) บทบาทของหน่วยงานกำกับการปฏิบัติตามกฎเกณฑ์ในระดับองค์กร หรือ Compliance function	71
4) ผู้บริหารระดับสูงมีหน้าที่ความรับผิดชอบในการบริหารจัดการ	71
5) องค์กรอาจจะจัดตั้งผู้รับผิดชอบโครงการ	72
6) บทบาทด้านการสำรวจแบบ Due Diligence และการกระจายอำนาจที่เหมาะสม	72
7) การสื่อสารการฝึกอบรมและทำให้เกิดความรู้ความเข้าใจในช่องทางอื่น	73
8) กลไกติดตามผล การตรวจสอบ และระบบการรายงานผล	74
9) การสร้างแรงจูงใจและการสร้างกติกากการบังคับใช้	76
10) การตอบโต้กับการกระทำที่ฝ่าฝืน การกำกับการปฏิบัติตามกฎเกณฑ์	76
11) การวิเคราะห์และประเมินความเสี่ยงเพื่อปรับปรุงแผนงานให้ดีขึ้น	77
4. มุมมองของ COSO ERM ต่อการบริหารความเสี่ยงการกำกับการปฏิบัติตามกฎเกณฑ์ 5 องค์ประกอบ	78
องค์ประกอบที่ 1 GOVERNANCE & CULTURE สำหรับ COMPLIANCE RISK	79



	หน้า
หลักการที่ 1 การกำกับภาพในองค์กรรวมของคณะกรรมการ (Exercise Board Risk Oversight)	79
หลักการที่ 2 การจัดวางโครงสร้างการดำเนินงานที่มีประสิทธิภาพ (Establishes Operating Structures)	80
หลักการที่ 3 การกำหนดวัฒนธรรมพฤติกรรม การตื่นตัวที่พึง ประสงค์	82
หลักการที่ 4 แสดงให้เห็นถึงความยึดมั่นมุ่งมั่นต่อคุณค่าหลักองค์กร (Demonstrates Commitment To Core Value)	84
หลักการที่ 5 กำหนดแรงจูงใจ กลไกพัฒนา และดำรงรักษาศักยภาพ รายบุคคล	85 86
สรุปสิ่งที่ต้องดำเนินการตามองค์ประกอบที่ 1	
องค์ประกอบที่ 2 กลยุทธ์และวัตถุประสงค์ Compliance Risk	86
หลักการที่ 6 การวิเคราะห์บริบทธุรกิจเพื่อกำหนดกลยุทธ์และ เป้าประสงค์	86
หลักการที่ 7 กำหนดเกณฑ์ความเสี่ยงที่ยอมรับได้ (Define Risk Appetite)	88
หลักการที่ 8 ประเมินทางเลือกในการใช้กลยุทธ์ตามเกณฑ์ที่ ยอมรับได้	88
หลักการที่ 9 จัดวางวัตถุประสงค์ความเสี่ยงที่รองรับธุรกิจ	89
สรุปสิ่งที่ต้องดำเนินการตามองค์ประกอบที่ 2	90
องค์ประกอบที่ 3 ผลดำเนินงานด้านการบริหาร Compliance Risk	91
หลักการที่ 10 การระบุความเสี่ยงการบริหารแผนงาน/โครงการ C&E	91
หลักการที่ 11 เรียงลำดับความรุนแรงของความเสี่ยงเพื่อบริหาร แผนงาน/โครงการ C&E	92



	หน้า
หลักการที่ 12 เรียงลำดับความเสี่ยงในการบริหารแผนงาน/โครงการ C&E	95
หลักการที่ 13 ขออนุมัติเพื่อทำแผนตอบโต้ บรรเทาความเสี่ยง	97
หลักการที่ 14 พัฒนาสถานะภาพรวม Portfolio View Of Compliance Risk	99
สรุปสิ่งที่ต้องดำเนินการตามองค์ประกอบที่ 3	100
องค์ประกอบที่ 4 ทบทวนและปรับปรุง Compliance Risk และการจัดการ	101
หลักการที่ 15 การวิเคราะห์และประเมินการเปลี่ยนแปลงที่มีนัยสำคัญ	101
หลักการที่ 16 ทบทวนความเสี่ยงและผลดำเนินงาน	102
หลักการที่ 17 ผลักดันสู่การปรับปรุงการบริหารความเสี่ยงทั่วทั้งองค์กร	103
สรุปสิ่งที่ต้องดำเนินการตามองค์ประกอบที่ 4	105
องค์ประกอบที่ 5 ข้อมูลสารสนเทศ การสื่อสาร และการรายงานสำหรับ Compliance Risk	105
หลักการที่ 18 การยกระดับข้อมูลสารสนเทศและเทคโนโลยี	105
หลักการที่ 19 การสื่อสารข้อมูลความเสี่ยง	107
หลักการที่ 20 การรายงานความเสี่ยง วัฒนธรรม และผลดำเนินงาน	108
สรุปสิ่งที่ต้องดำเนินการตามองค์ประกอบที่ 5	109
บทที่ 4	110
มาตรฐานสากล 3: GRC ของ OCEG	
1. หลักการ เหตุผล ความเป็นมา	110



	หน้า
2. กรอบแนวคิดของมาตรฐาน	114
องค์ประกอบที่ 1: Governance	114
องค์ประกอบที่ 2 : Risk Management	115
องค์ประกอบที่ 3 : Compliance	116
การยกระดับมาตรฐาน GRC ตามเศรษฐกิจกระแสใหม่ของโลก	116
3. ขอบเขตของการบริหารความเสี่ยงตามกรอบแนวคิด GRC	120
4. ผลลัพธ์ร่วมกัน (UNIVERSAL OUTCOMES) ตามมาตรฐาน GRC	126
บทสรุปของมาตรฐาน GRC	129
บทที่ 5	131
มาตรฐาน ISO 37301: 2021 Compliance Management System	
- Requirements with guidance for use	
1. หลักการ เหตุผล และความเป็นมา	131
2. ระบบบริหารการกำกับการปฏิบัติตามกฎเกณฑ์ตาม ISO 37301	139
1) ประโยชน์ที่สำคัญของ ISO 37301	139
2) ประเด็นการเปลี่ยนแปลงที่สำคัญ	139
3) แนวทางการนำมาตรฐาน ISO 37301 มาใช้ภายในองค์กร	141
3. บทสรุปมาตรฐาน ISO 37301 ด้านการกำกับการปฏิบัติตามกฎเกณฑ์	143
บทที่ 6	145
The Three Lines of Defense สนับสนุนการกำกับการความเสี่ยง	
Compliance Risk	
1. หลักการ เหตุผล และความเป็นมา	145
2. การเกิดของแนวคิด The Three Lines of Defense	146
3. บทบาทของผู้บริหารระดับสูงและคณะกรรมการ	147
4. การจัดวางกลุ่มงานตาม The Three Lines of Defense	149



	หน้า
บทบาทของ 1st Line	149
บทบาทของ 2nd Line	150
บทบาทของ 3rd Line	152
5. บทบาทของหน่วยงานภายนอกองค์กร	153
กลุ่มที่ 1 บทบาทของผู้สอบบัญชีภายนอก	153
กลุ่มที่ 2 บทบาทของหน่วยงานรัฐภายนอก	154
6. การบูรณาการ เชื่อมโยง ส่งต่อการจัดการความเสี่ยงด้านการกำกับ การปฏิบัติตามกฎเกณฑ์ผ่าน The Three Lines of Defense	156
7. OECD GOVERNANCE ต่อการกำกับข้ามอาณาเขต	158
1) แนวปฏิบัติที่ดีสำหรับหน่วยงานที่กำกับกฎเกณฑ์ตามกฎหมาย	159
2) ตัวอย่างกฎเกณฑ์สำคัญที่ใช้กำกับข้ามอาณาเขต	162
8. บทบาทการกำกับ การดำเนินธุรกิจบนหลักความรับผิดชอบต่อสังคม และสิ่งแวดล้อมและกฎเกณฑ์ข้ามอาณาเขต	164
1) การกำกับ การดำเนินธุรกิจบนหลักความรับผิดชอบต่อสังคมและ สิ่งแวดล้อม	164
2) เจ้าหน้าที่กำกับการปฏิบัติตามกฎเกณฑ์ข้ามอาณาเขตในฐานะ วิชาชีพ	165
บทที่ 7	168
บทสรุปเพื่อการพัฒนาการกำกับการปฏิบัติตามกฎเกณฑ์	
1. ขั้นตอนการพัฒนากลไกการกำกับการปฏิบัติตามกฎเกณฑ์	168
2. กิจกรรมหลักของการพัฒนา	172

บทนำ

มาตรฐานสากลที่เกี่ยวข้องกับ การกำกับการปฏิบัติตามกฎเกณฑ์



1. ความเป็นมา

การกำกับการปฏิบัติตามกฎเกณฑ์ (Compliance Management) เป็นหนึ่งในระบบงานบริหารจัดการที่มีพัฒนาการมายาวนานหลายสิบปีแล้ว ตามแนวนโยบายของหน่วยงานกำกับดูแล โดยเฉพาะการบังคับใช้กับบริษัทมหาชนในตลาดหลักทรัพย์ ซึ่งเท่ากับเป็นบริษัทขนาดใหญ่ เพื่อให้เป็นต้นแบบของระบบการบริหารจัดการ (Management System) ที่ดี แม้ว่าจนถึงขณะนี้ ผู้บริหารองค์กรทั้งในไทยและหลายประเทศทั่วโลกจะยังรู้สึกว่าเป็นเรื่องนี้เป็นแนวคิดใหม่ที่ไม่คุ้นเคยสักที

การทำความเข้าใจกับการบริหารจัดการด้านการกำกับการปฏิบัติตามกฎเกณฑ์จึงต้องเริ่มจากการทำการศึกษา ทำความเข้าใจ ในสาระสำคัญและในองค์ประกอบของแต่ละ

มาตรฐานสากลที่อ้างอิงและกล่าวถึงคำว่า “การกำกับการปฏิบัติตามกฎเกณฑ์” หรือ Compliance ทำให้คำนี้ถูกนำมาใช้และพูดถึงกันในวงการบริหารจัดการขององค์กรต่างๆ

2. กำกับด้วย 4 มาตรฐานสากลที่สำคัญ

มาตรฐานสากลที่สำคัญในส่วนของการกำกับการปฏิบัติตามกฎเกณฑ์ ประกอบด้วย
มาตรฐานสากลที่เกี่ยวข้องกับการกำกับการปฏิบัติตามกฎเกณฑ์ ประกอบด้วย

มาตรฐานสากล 1	COSO 2013: Integrated Internal Control Framework
มาตรฐานสากล 2	COSO ERM 2017 – Compliance Management
มาตรฐานสากล 3	GRC ของ OCEG
มาตรฐานสากล 4	ISO 37301: 2021 Compliance Management System

ความแตกต่างของ 4 มาตรฐาน COMPLIANCE กับการใช้



จากแผนภาพดังกล่าวข้างต้นสามารถสรุปได้ว่า การกำกับการปฏิบัติตามกฎเกณฑ์เมื่อนำมาปรับใช้โดยพิจารณาตามแนวปฏิบัติของมาตรฐานสากล สามารถแยกการประยุกต์ใช้ได้ดังนี้

มาตรฐาน COSO 2013

เป็นมาตรฐานที่นำการกำกับ การปฏิบัติตามกฎเกณฑ์ไปแทรกไว้ในกระบวนการควบคุมภายในจึงเหมาะสมในการกำกับ มิให้กระบวนการควบคุมการปฏิบัติงานประจำวันที่ต้องใช้การกำกับ การปฏิบัติตามกฎเกณฑ์อยู่ตลอดเวลา ทำให้ผู้รับผิดชอบภาระงานที่เป็นผู้ปฏิบัติงานสามารถควบคุมการกำกับ การปฏิบัติตามกฎเกณฑ์ในระหว่างปฏิบัติงานได้โดยทันที ไม่เกิดความล่าช้า สามารถใช้ซ้ำได้ และสามารถปรับเปลี่ยนได้เมื่อมีความจำเป็น

มาตรฐาน COSO ERM 2017

เป็นมาตรฐานที่จัดทำแนวปฏิบัติที่ดี แยกการวิเคราะห์และประเมินความเสี่ยงของการกำกับ การปฏิบัติตามกฎเกณฑ์ ออกมาต่างหากจากการวิเคราะห์และประเมินความเสี่ยงในระดับกลยุทธ์และแผนงาน/โครงการเชิงกลยุทธ์ขององค์กร เนื่องจากเห็นว่า มีความจำเป็นต้องใช้ผู้เชี่ยวชาญ มีทักษะ องค์ความรู้เกี่ยวข้องกับกฎเกณฑ์ต่างๆ รอบด้าน

มาตรฐานนี้กำหนดให้การกำกับ การปฏิบัติตามกฎเกณฑ์เป็นความเสี่ยงที่องค์กรต้องให้ความสำคัญ ในระดับของการบริหารความสำเร็จเชิงวัตถุประสงค์และผลดำเนินงาน ฝ่ายบริหารหรือฝ่ายจัดการจำเป็นต้องทำให้มั่นใจว่า ได้กำหนดแผนงาน บริหารความเสี่ยงที่จะรับมือและตอบโต้กับความเสี่ยงด้านการกำกับ การปฏิบัติตามกฎเกณฑ์อย่างเพียงพอพร้อมกับการตัดสินใจในเชิงธุรกิจ

มาตรฐาน GRC ของ OCEG

มาตรฐานนี้เกิดจากองค์กรไม่แสวงหากำไร ชื่อ OCEG หรือชื่อเดิมคือ The Open Compliance

and Ethics Group มีบทบาทสำคัญตั้งแต่ปี 2002 ภายหลังจากการล้มละลายมาจากการบริหารจัดการองค์กรที่มีจรรยาบรรณวิบัติของ บริษัทมหาชนที่จดทะเบียนในตลาดหลักทรัพย์ ของอเมริกาชื่อ Enron ทำให้เกิดการถอดบทเรียนเพื่อแสวงหาแนวทางการกำกับดูแล องค์กรที่ดีที่เรียกคืนความมั่นใจต่อบริษัทจดทะเบียนของนักลงทุนในตลาดหลักทรัพย์

มาตรฐานนี้ให้ความสำคัญกับบทบาทในส่วนของ คณะกรรมการในฐานะขององค์กรคณะที่ทำหน้าที่ กำกับดูแลในภาพรวมของฝ่ายบริหารหรือฝ่าย จัดการ โดยเสนอให้มีการจัดตั้งคณะกรรมการ องค์กร คณะ หรือคณะอนุกรรมการพิเศษขึ้นเพื่อ กำกับดูแล ติดตามและประเมินผลการดำเนินงาน ด้านการบริหารและจัดการกับความเสี่ยงการ กำกับ การปฏิบัติตามกฎเกณฑ์โดยเฉพาะเจาะจง โดยเฉพาะส่วนที่เกี่ยวข้องกับหน่วยงานกำกับ ทางกฎหมายภายนอกองค์กร และทำให้มั่นใจว่า ฝ่ายบริหารหรือฝ่ายจัดการมีกิจกรรมในการ ขับเคลื่อนองค์กร โดยเฝ้าระวังและหลีกเลี่ยงการ ผ่าฝืนการกำกับ การปฏิบัติตามกฎเกณฑ์ได้อย่าง เพียงพอและมีประสิทธิภาพ ควบคู่กับ คณะกรรมการกำกับดูแลองค์กรที่ดี และ คณะกรรมการบริหารความเสี่ยง

มาตรฐานนี้กำหนดขึ้นเพื่อแก้ปัญหาการกำกับ ดูแลองค์กรที่ไม่เหมาะสมและไม่เพียงพอของ บริษัทมหาชนที่จดทะเบียนในตลาดหลักทรัพย์ หรือบริษัทที่มีความรับผิดชอบต่อสาธารณะ เช่น หน่วยงานภาครัฐ เนื่องจากเป็นมาตรฐานที่ให้

ความสำคัญกับผู้มีส่วนได้ส่วนเสียจากภายนอก นอกเหนือจากคำนึงถึงวัตถุประสงค์ทางธุรกิจ และเป้าหมายการดำเนินงานภายในขององค์กรเอง

มาตรฐาน ISO 37301 : 2021

เป็นมาตรฐานที่กำหนดขึ้นโดยองค์กร ISO โดยมองว่า การกำกับ การปฏิบัติตามกฎเกณฑ์เป็นระบบบริหารหนึ่งขององค์กรที่สำคัญและจำเป็น แต่ละองค์กรที่มีลักษณะของการดำเนินงาน รูปแบบธุรกิจ บริบทของการดำเนินงานที่แตกต่างกัน ควรจะวางระบบมาตรฐานการปฏิบัติงาน ในส่วนของการกำกับการปฏิบัติตามกฎเกณฑ์ได้ใกล้เคียงกัน

ระบบการบริหารงานกำกับการปฏิบัติการ กฎเกณฑ์ที่ดีต้องดำเนินงานตามวงจรคุณภาพ หรือที่เรียกว่า PDCA : Plan – Do – Check – Act ซึ่งหาก สามารถดำเนินการได้อย่างครบถ้วน ราบเรียบจะได้รับรับรอง หลังจากผ่านเกณฑ์การตรวจประเมินของ ISO

มาตรฐานสากลทั้ง 4 มาตรฐานล้วนแต่มีความสำคัญ และมีได้มีแนวคิดที่ขัดแย้งกัน แต่ละมาตรฐานมีจุดเด่น ที่น่าสนใจ และประโยชน์ที่ได้จากการนำมาใช้ที่แตกต่างกัน องค์กรจึงไม่จำเป็นต้องเลือกมาตรฐานใดมาตรฐานหนึ่ง แต่สามารถวางแผนที่นำทางให้องค์กรได้ใช้ประโยชน์จากทุกมาตรฐานดังกล่าวข้างต้น เพื่อให้เกิดประสิทธิภาพและประสิทธิผลสูงสุดแก่องค์กร

3. การใช้ 2 แนวปฏิบัติที่ดีเพื่อสนับสนุนเพิ่มเติม

นอกเหนือจากมาตรฐานสากลพร้อมแนวปฏิบัติที่ดีที่ออกประกาศใช้พร้อมกันกลับ มาตรฐานดังกล่าวข้างต้นแล้วยังมีแนวปฏิบัติที่ดีที่องค์กรควรพิจารณานำมาสนับสนุนการพัฒนาการกำกับการปฏิบัติตามกฎเกณฑ์ เพื่อช่วยให้ระบบการจัดวางงานในส่วนนี้ประสบความสำเร็จ ประกอบด้วย

- 1) แนวปฏิบัติที่ดีในการแบ่งความรับผิดชอบตาม Four Lines of Defense และ Five Lines of Defense
- 2) แนวปฏิบัติที่ดีด้าน Compliance ขององค์กร OECD
 - (1) Compliance for Regulator
 - (2) Compliance for Public Sector

ซึ่งตามแนวคิดโดยภาพรวมของแนวปฏิบัติที่ดีดังกล่าวข้างต้นสามารถสรุปประเด็นที่สำคัญได้ดังนี้

**แนวปฏิบัติที่ดีในการแบ่งความ
รับผิดชอบตาม Four Lines of
Defense และ Five Lines of
Defense**

เป็นแนวปฏิบัติที่ดีของกลุ่ม COSO ที่ออกมาเพิ่มเติมเพื่อรองรับการกำหนดบทบาทและหน้าที่ความรับผิดชอบในการบริหารและจัดการความเสี่ยงภายในองค์กรให้เป็นไปอย่างเหมาะสม ตั้งแต่บทบาทหน้าที่และความรับผิดชอบ ของภาระงานหรือเจ้าของกระบวนการโดยตรงไปจนถึงบทบาทของหน่วยงานที่ทำหน้าที่กำกับในภาพรวมขององค์กรหรือที่เรียกว่าหน่วยงานสนับสนุนและบทบาทของงานตรวจสอบภายใน ในฐานะผู้ให้ความเชื่อมั่นอย่างอิสระ

สำหรับกรณีการกำกับการปฏิบัติตามกฎเกณฑ์ จำเป็นต้องคำนึงถึงและรวมเอาหน่วยงานกำกับดูแลภายนอก ที่ทำหน้าที่ในการกำกับการดำเนินงานขององค์กรอย่างใกล้ชิด รวมทั้งการตรวจประเมินการปฏิบัติตามกฎเกณฑ์หรือตามเงื่อนไขของใบอนุญาตประกอบการ การวินิจฉัยตามอำนาจทางปกครองเป็นรายกรณี โดยบางครั้งไม่ต้องผ่านกระบวนการทางศาล เพราะมีการแต่งตั้งคณะกรรมการเฉพาะ

กิจขึ้นมาเพื่อการนั้นๆโดยเฉพาะ ทำให้ความรับผิดชอบด้านการกำกับ การปฏิบัติตามกฎเกณฑ์ ต้องใช้แนวคิดของ Four Lines of Defense ถือว่าหน่วยงานกำกับทางกฎหมายภายนอกเป็น 4th Line

ส่วนบทบาทและหน้าที่ความรับผิดชอบของหน่วยงานภายในองค์กรในส่วนของการกำกับการปฏิบัติตามกฎเกณฑ์ โดยเฉพาะ เป็นการกำกับในระดับขององค์กรหรือระดับนิติบุคคล จึงต้องใช้แนวคิดของการกำกับถึง 5 ชั้น ที่เริ่มจากคณะกรรมการ ผู้บริหารระดับสูง งานตรวจสอบภายใน หน่วยงานกำกับองค์กรในภาพรวม และผู้ปฏิบัติงานที่เป็นเจ้าของภาระงานหรือเจ้าของกระบวนการ

แนวปฏิบัติที่ดีด้าน Compliance ขององค์กร OECD

องค์กร OECD เป็นองค์กรความร่วมมือระหว่างประเทศที่ครอบคลุมในระดับของรัฐบาลของหลายประเทศที่พัฒนาแล้ว ครอบคลุมภูมิภาคต่างๆของโลกในฐานะรัฐบาลที่เป็นผู้กำหนดระดับนโยบาย ก็ไปก็แบบว่าและการมอบหมายสั่งการผ่านหน่วยงานรัฐ ทำให้ผลกระทบของแนวปฏิบัติที่ดีตามประกาศหรือข้อตกลงขององค์กรระหว่างประเทศแห่งนี้มีลักษณะเป็นกฎหมายประเภทหนึ่งของโลกที่ใช้บังคับในลักษณะเดียวกันสำหรับประเทศสมาชิก รวมทั้งประเทศอื่นที่มีการติดต่อความสัมพันธ์ทางการค้าและทางธุรกิจกับประเทศสมาชิกของ OECD

นอกเหนือจาก OECD เป็นผู้ที่มิมีบทบาทสำคัญในการประกาศใช้แนวปฏิบัติที่ออกมาบังคับใช้กับประเทศสมาชิกแล้ว OECD ยังทำหน้าที่ในการสำรวจ การวิจัย ตลอดจนการติดตามประเมินผลการดำเนินงานจริงในการกำกับการปฏิบัติตามกฎเกณฑ์ของแต่ละประเทศ เพื่อให้คำแนะนำ ความคิดเห็นในการแก้ไขปรับปรุง และพัฒนา อย่างต่อเนื่องเป็นประจำทุกปี การนำเอากรอบแนวปฏิบัติที่ดีขององค์กรนี้มาใช้จึงมีกรณีศึกษาและบทเรียนให้เรียนรู้จากประเทศต่างๆ ทั่วโลก ทำให้ประเทศที่นำมาใช้ปฏิบัติสามารถนำไปประยุกต์และปรับใช้ได้ง่าย

OECD พิจารณาว่าการกำกับการปฏิบัติตามกฎเกณฑ์ถือเป็นส่วนหนึ่งของการกำกับดูแลที่ดี ตั้งแต่ระดับของหน่วยงานกำกับดูแลที่เป็นผู้บังคับใช้กฎหมาย หน่วยงานภาครัฐที่เป็นผู้มีอำนาจตามกฎหมายควบคุมเกี่ยวกับการให้บริการต่อประชาชน ไปจนถึงผู้ประกอบการภาคเอกชนโดยเฉพาะนิติบุคคลที่เป็นบริษัทมหาชน ทำให้แนวปฏิบัติด้านการกำกับการปฏิบัติตามกฎเกณฑ์มีความครอบคลุมในหน่วยงานทุกระดับขององค์กร

แนวปฏิบัติที่ดีที่สำคัญ ประกอบด้วย

- (1) Compliance for Regulator
- (2) Compliance for Public Sector