

Organizational Behavior

Topical Requirement

User Guide

พฤติกรรมองค์กร

ข้อกำหนดเฉพาะ

คู่มือผู้ใช้



The Institute of
Internal Auditors

สารบัญ (Contents)

ภาพรวมของข้อกำหนดเฉพาะ.....	3
การบังคับใช้ ความเสี่ยง และดุลยพินิจทางวิชาชีพ.....	4
หมวดย่อย (Sections)	9
ข้อควรพิจารณา.....	11
ภาคผนวก A. ตัวอย่างการประยุกต์ใช้ในทางปฏิบัติ.....	30
ภาคผนวก B. กรณีศึกษาการตรวจสอบเฉพาะ.....	34
ภาคผนวก C. เครื่องมือในการจัดทำเอกสารที่เลือกใช้ได้.....	41
ภาคผนวก D. การเทียบเคียงกับกรอบการควบคุมภายในและการบริหารความเสี่ยงของ COSO....	46
ภาคผนวก E. กิจกรรมการตรวจสอบและการให้ความเชื่อมั่นที่เกี่ยวข้องกับพฤติกรรม	53



ภาพรวมของข้อกำหนดเฉพาะ (Overview of Topical Requirements)

ข้อกำหนดเฉพาะ (Topical Requirements) เป็นองค์ประกอบสำคัญของกรอบการปฏิบัติงานทางวิชาชีพสากล (International Professional Practices Framework® - IPPF) ควบคู่ไปกับมาตรฐานการตรวจสอบภายในสากล (Global Internal Audit Standards™) และแนวปฏิบัติสากล (Global Guidance) สมาคมผู้ตรวจสอบภายใน (The IIA) กำหนดให้ใช้ข้อกำหนดเฉพาะร่วมกับมาตรฐานการตรวจสอบภายในสากลซึ่งถือเป็นเกณฑ์ที่ได้รับการยอมรับอย่างเป็นทางการของวิธีปฏิบัติที่กำหนดไว้ โดยมีการอ้างอิงถึงมาตรฐานต่างๆ ไว้ในคู่มือฉบับนี้เพื่อเป็นแหล่งข้อมูลเชิงลึกที่มีรายละเอียดมากขึ้น

ข้อกำหนดเฉพาะกำหนดรูปแบบที่เป็นทางการเพื่อให้ผู้ตรวจสอบภายในจัดการกับพื้นที่ที่มีความเสี่ยงสูง เพื่อส่งเสริมคุณภาพและความสอดคล้องของวิชาชีพ ทั้งนี้ อำนาจหน้าที่ของหน่วยงานตรวจสอบภายใน (Internal Audit Mandate) ต้องกำหนดนิยามของขอบเขตและประเภทของบริการที่หน่วยงานตรวจสอบภายในดำเนินการให้ชัดเจน ซึ่งจะรวมถึงการนำข้อกำหนดเฉพาะมาพิจารณาประกอบด้วย (มาตรฐาน 6.1 อำนาจหน้าที่ของหน่วยงานตรวจสอบภายใน) ข้อกำหนดเฉพาะจัดทำขึ้นเพื่อเป็นเกณฑ์พื้นฐานและกำหนดเกณฑ์ในการประเมินที่เกี่ยวข้องสำหรับการให้บริการให้ความเชื่อมั่น (Assurance Services) ในหัวข้อที่เกี่ยวข้องกับข้อกำหนดเฉพาะนั้นๆ (มาตรฐาน 13.4 เกณฑ์ในการประเมิน) การปฏิบัติตามข้อกำหนดเฉพาะถือเป็นภาคบังคับ (Mandatory) สำหรับงานตรวจสอบเพื่อให้ความเชื่อมั่นและเป็นข้อแนะนำให้ใช้ในการประเมินระหว่างการให้บริการให้คำปรึกษา (Advisory Services) ทั้งนี้ ข้อกำหนดเฉพาะไม่ได้มุ่งหมายที่จะครอบคลุมทุกแง่มุมที่อาจต้องพิจารณาเมื่อปฏิบัติงานให้ความเชื่อมั่น แต่มีเจตนาที่จะให้ข้อกำหนดขั้นต่ำเพื่อช่วยให้สามารถประเมินหัวข้อนั้นๆ ได้อย่างสอดคล้องและน่าเชื่อถือ

ข้อกำหนดเฉพาะมีความเชื่อมโยงอย่างชัดเจนกับโมเดลแนวป้องกันสามด้าน (Three Lines Model) ของ IIA และมาตรฐานการตรวจสอบภายในสากล โดยมีองค์ประกอบหลักคือ กระบวนการกำกับดูแล การบริหารความ

เสี่ยง และการควบคุม ซึ่งสอดคล้องกับมาตรฐาน 9.1 การทำความเข้าใจกระบวนการกำกับดูแล การบริหาร ความเสี่ยง และการควบคุม ในการอ้างอิงถึงโมเดลแนวป้องกันสามด้านนั้น การกำกับดูแล (Governance) เชื่อมโยงกับคณะกรรมการ/องค์คณะผู้กำกับดูแล (Board/Governing Body) การบริหารความเสี่ยง (Risk Management) เชื่อมโยงกับแนวป้องกันด้านที่สอง (Second Line) และวิธีการควบคุม (Controls) หรือ กระบวนการควบคุม (Control Processes) เชื่อมโยงกับแนวป้องกันด้านที่หนึ่ง (First Line) ในขณะที่ฝ่าย บริหาร (Management) ปรากฏอยู่ในทั้งแนวป้องกันด้านที่หนึ่งและสอง หน่วยงานตรวจสอบภายในจะอยู่ใน แนวป้องกันด้านที่สาม (Third Line) ในฐานะผู้ให้บริการให้ความเชื่อมั่นที่เป็นอิสระและเที่ยงธรรม โดยรายงาน ตรงต่อคณะกรรมการ/องค์การกำกับดูแล (หลักการที่ 8 ควบคุมดูแลโดยคณะกรรมการ)

การบังคับใช้ ความเสี่ยง และดุลยพินิจทางวิชาชีพ (Applicability, Risk, and Professional Judgment)

หน่วยงานตรวจสอบภายในต้องปฏิบัติตามข้อกำหนดเฉพาะ (Topical Requirements) เมื่อปฏิบัติงานให้ความ เชื่อมั่น (Assurance Engagements) ในหัวข้อที่มีข้อกำหนดเฉพาะนั้นรองรับอยู่ หรือเมื่อมีการระบุแง่มุมของ ข้อกำหนดเฉพาะนั้นปรากฏขึ้นภายในงานตรวจสอบอื่นๆ

ตามที่ระบุไว้ในมาตรฐานการตรวจสอบฯ การประเมินความเสี่ยงถือเป็นส่วนสำคัญในการวางแผนของหัวหน้า หน่วยงานตรวจสอบภายใน (Chief Audit Executive - CAE) การตัดสินใจเลือกที่จะรวมงานตรวจสอบใดไว้ ในแผนการตรวจสอบภายในนั้น จำเป็นต้องมีการประเมินกลยุทธ์ วัตถุประสงค์ และความเสี่ยงขององค์กร อย่างน้อยปีละครั้ง (มาตรฐาน 9.4 แผนการตรวจสอบภายใน) และเมื่อมีการวางแผนงานตรวจสอบแต่ละ โครงการ ผู้ตรวจสอบภายในต้องประเมินความเสี่ยงที่เกี่ยวข้องกับโครงการนั้นๆ (มาตรฐาน 13.2 การประเมิน ความเสี่ยงของงานที่ได้รับมอบหมาย)

เมื่อหัวข้อของข้อกำหนดเฉพาะได้ถูกระบุในระหว่างกระบวนการวางแผนการตรวจสอบภายในโดยอิงความ เสี่ยง (Risk based Planning) และถูกบรรจุไว้ในแผนการตรวจสอบแล้ว ต้องนำข้อกำหนดที่ระบุไว้ใน ข้อกำหนดเฉพาะมาใช้เพื่อประเมินหัวข้อดังกล่าวในงานตรวจสอบนั้น นอกจากนี้ เมื่อผู้ตรวจสอบภายใน ปฏิบัติงานตรวจสอบใดๆ (ไม่ว่าจะถูกบรรจุอยู่ในแผนการตรวจสอบหรือไม่ก็ตาม) และพบว่ามียอดประกอบ ของข้อกำหนดเฉพาะปรากฏขึ้น ต้องประเมินการบังคับใช้ข้อกำหนดเฉพาะนั้นโดยเป็นส่วนหนึ่งของงาน



ตรวจสอบ สุดท้ายนี้ หากมีการร้องของานตรวจสอบที่ไม่ได้อยู่ในแผนตั้งแต่แรกและงานนั้นครอบคลุมหัวข้อดังกล่าว ต้องประเมินการบังคับใช้ข้อกำหนดเฉพาะด้วยเช่นกัน

ดุลยพินิจทางวิชาชีพ (Professional Judgment) มีบทบาทสำคัญอย่างยิ่งในการนำข้อกำหนดเฉพาะมาใช้ในการประเมินความเสี่ยงเป็นตัวขับเคลื่อนการตัดสินใจของหัวหน้าหน่วยงานตรวจสอบภายในว่าจะรวมงานตรวจสอบใดไว้ในแผนการตรวจสอบภายใน (มาตรฐาน 9.4 แผนการตรวจสอบภายใน) นอกจากนี้ ผู้ตรวจสอบภายในยังใช้ดุลยพินิจทางวิชาชีพในการกำหนดแง่มุมที่จะครอบคลุมในแต่ละงานที่ได้รับมอบหมาย (มาตรฐาน 13.3 วัตถุประสงค์และขอบเขตของงานที่ได้รับมอบหมาย มาตรฐาน 13.4 เกณฑ์ในการประเมิน และมาตรฐาน 13.6 แนวทางปฏิบัติงาน) ตลอดจนการระบุทรัพยากรที่จำเป็นเพื่อให้บรรลุวัตถุประสงค์ของงานตรวจสอบ (มาตรฐาน 13.5 ทรัพยากรสำหรับงานที่ได้รับมอบหมาย)

ต้องเก็บรักษาหลักฐานที่แสดงว่าได้มีการประเมินการบังคับใช้ข้อกำหนดแต่ละข้อในข้อกำหนดเฉพาะแล้ว รวมถึงต้องระบุเหตุผลประกอบในกรณีที่มีการยกเว้นข้อกำหนดใดๆ การปฏิบัติตามข้อกำหนดเฉพาะต้องจัดทำเป็นเอกสารโดยใช้ดุลยพินิจทางวิชาชีพของผู้ตรวจสอบตามที่ระบุไว้ในมาตรฐาน 14.6 การจัดทำเอกสารสำหรับงานที่ได้รับมอบหมาย

ขณะที่ข้อกำหนดเฉพาะจะกำหนดเกณฑ์พื้นฐานของกระบวนการควบคุมที่ควรพิจารณา แต่สำหรับองค์กรที่ประเมินว่าความเสี่ยงของประเด็นนั้นอยู่ในระดับสูงมาก อาจจำเป็นต้องประเมินแง่มุมอื่นเพิ่มเติม

หากหัวหน้าหน่วยงานตรวจสอบภายใน พิจารณาแล้วเห็นว่าหน่วยงานตรวจสอบภายในไม่มีความรู้ความชำนาญที่จำเป็นในการปฏิบัติงานตรวจสอบในหัวข้อของข้อกำหนดเฉพาะอาจพิจารณาจัดจ้างผู้ให้บริการภายนอกเพื่อปฏิบัติงานนั้น (มาตรฐาน 3.1 ความสามารถในหน้าที่ มาตรฐาน 7.2 คุณสมบัติของหัวหน้าหน่วยงานตรวจสอบภายใน และมาตรฐาน 10.2 การบริหารทรัพยากรบุคคล) มาตรฐานมีผลบังคับใช้กับบุคคลหรือหน่วยงานใดๆ ที่ให้บริการตรวจสอบภายในไม่ว่าองค์กรจะจ้างผู้ตรวจสอบภายในโดยตรง หรือจัดจ้างผ่านผู้ให้บริการภายนอก หรือทั้งสองอย่าง โดยหัวหน้าหน่วยงานตรวจสอบภายในยังคงเป็นผู้รับผิดชอบสูงสุดในการดูแลให้มีการปฏิบัติตามมาตรฐาน นอกจากนี้ หากหัวหน้าหน่วยงานตรวจสอบภายในพิจารณาว่าทรัพยากรตรวจสอบภายในไม่เพียงพอต้องแจ้งให้คณะกรรมการทราบถึงผลกระทบของทรัพยากรที่ไม่เพียงพอและแนวทางการแก้ไขปัญหาการขาดแคลนทรัพยากรดังกล่าว (มาตรฐาน 8.2 ทรัพยากร)



การปฏิบัติงาน การจัดทำเอกสาร และการรายงาน (Performance, Documentation, and Reporting)

เมื่อนำข้อกำหนดเฉพาะมาใช้ผู้ตรวจสอบภายในต้องปฏิบัติตามมาตรฐานการตรวจสอบฯ โดยดำเนินงานให้สอดคล้องกับโดเมนที่ 5: การให้บริการตรวจสอบภายใน (Domain V: Performing Internal Audit Services) ซึ่งบรรยายถึงการวางแผนงานตรวจสอบที่ได้รับมอบหมาย (หลักการที่ 13 การวางแผนงานที่ได้รับมอบหมายอย่างมีประสิทธิภาพ) การปฏิบัติงานตรวจสอบ (หลักการที่ 14 ปฏิบัติงานที่ได้รับมอบหมาย) และการสื่อสารผลการตรวจสอบ (หลักการที่ 15 สื่อสารผลของงานที่ได้รับมอบหมายและการติดตามแผนดำเนินการ)

ข้อกำหนดเฉพาะถูกออกแบบมาเพื่อสนับสนุนวิธีปฏิบัติของการตรวจสอบภายในที่สม่ำเสมอและมีคุณภาพสูง โดยต้องนำไปใช้ควบคู่กับกฎหมายในท้องถิ่น ระเบียบข้อบังคับ ความคาดหวังของหน่วยงานกำกับดูแล และกรอบการปฏิบัติงานทางวิชาชีพซึ่งเป็นที่ยอมรับอื่นๆ ซึ่งอาจมีการกำหนดข้อกำหนดเพิ่มเติมหรือข้อกำหนดที่เฉพาะเจาะจงยิ่งขึ้น ข้อกำหนดเพิ่มเติมหรือข้อกำหนดที่เฉพาะเจาะจงยิ่งขึ้น ผู้ตรวจสอบภายในอาจจัดทำแนวการปฏิบัติงาน (Work Programs) และวิธีการทดสอบต่างๆ โดยอาศัยกฎระเบียบและกรอบการปฏิบัติงานเหล่านี้เป็นพื้นฐาน ทั้งนี้ ผู้ตรวจสอบภายในควรเปรียบเทียบระหว่างการทดสอบการควบคุมด้านพฤติกรรมองค์กรที่กำหนดไว้กับการทดสอบที่เชื่อถือได้ใดๆ ที่จัดทำโดยผู้ให้บริการให้ความเชื่อมั่นภายในและภายนอก รายอื่น และปรับให้สอดคล้องกัน (มาตรฐาน 9.5 การประสานงานและการพึ่งพาผลงานของผู้อื่น) เพื่อให้มั่นใจว่าครอบคลุมข้อกำหนดเฉพาะอย่างเพียงพอ

การประเมินความครอบคลุมของข้อกำหนดเฉพาะสามารถจัดทำเป็นเอกสารไว้ในแผนการตรวจสอบภายใน หรือในแนวการปฏิบัติงานของแต่ละงานตรวจสอบที่ได้รับมอบหมายขึ้นอยู่กับดุลยพินิจทางวิชาชีพของผู้ตรวจสอบ งานที่ได้รับมอบหมายหนึ่งงานหรือมากกว่าอาจครอบคลุมข้อกำหนดต่างๆ นอกจากนี้ ไม่ใช่ข้อกำหนดทั้งหมดที่อาจสามารถนำมาปรับใช้ได้ จึงต้องเก็บรักษาหลักฐานการประเมินการบังคับใช้ข้อกำหนดเฉพาะนั้นว่าสามารถนำมาใช้ได้หรือไม่ รวมถึงต้องอธิบายเหตุผลกรณีที่มีการยกเว้นข้อกำหนดใดๆ

การประกันคุณภาพ (Quality Assurance)

มาตรฐานการตรวจสอบฯ กำหนดให้หัวหน้าหน่วยงานตรวจสอบภายในต้องพัฒนา นำไปปฏิบัติ และดำรงรักษาโครงการประกันคุณภาพและปรับปรุงงาน (Quality Assurance and Improvement Program - QAIP) ที่ครอบคลุมทุกแง่มุมของหน่วยงานตรวจสอบภายใน (มาตรฐาน 8.3 คุณภาพ) โดยต้องสื่อสารผลลัพธ์ต่อ



คณะกรรมการและผู้บริหารระดับสูง ในการสื่อสารต้องรายงานถึงการปฏิบัติตามข้อกำหนดของ หน่วยงานตรวจสอบภายใน และการบรรลุวัตถุประสงค์ด้านผลการปฏิบัติงาน

การปฏิบัติตามข้อกำหนดกับข้อกำหนดเฉพาะควรได้รับการพิจารณาในกิจกรรมการควบคุมดูแลในระดับงาน ตรวจสอบที่ได้รับมอบหมาย (มาตรฐาน 12.3 การควบคุมดูแลและปรับปรุงการปฏิบัติงานที่ได้รับมอบหมาย) และประเด็นดังกล่าวจะถูกประเมินในการประเมินคุณภาพ (Quality Assessments) ทั้งภายในและภายนอก

พฤติกรรมองค์กร (Organizational Behavior)

การปรับมุมมองการตรวจสอบวัฒนธรรม

(Reframing the Auditing of Culture)

การเปลี่ยนผ่านจากการมองว่าการตรวจสอบ "วัฒนธรรม" เป็นเรื่องนามธรรมและคลุมเครือ ไปสู่การประเมินพฤติกรรมองค์กร (Organizational Behavior) ที่มีโครงสร้างและแม่นยำ ถือเป็นวิวัฒนาการที่จำเป็นและเหมาะสมแก่เวลาสำหรับวิชาชีพตรวจสอบภายใน แม้จะเป็นที่ยอมรับกันอย่างกว้างขวางว่าความบกพร่องทางวัฒนธรรมมักเป็นสาเหตุพื้นฐานของความล้มเหลวของการควบคุมที่มีนัยสำคัญ แต่ประเด็นนี้กลับยังไม่ได้รับการความสนใจในวิธี

ปฏิบัติของการตรวจสอบภายในเท่าที่ควร การปรับมุมมองใหม่จาก

การตรวจสอบ "วัฒนธรรม" เป็นการตรวจสอบ “พฤติกรรมองค์กรที่ไม่สอดคล้องกับวัตถุประสงค์ขององค์กร” จะก่อให้เกิดพื้นฐานที่ชัดเจน มีโครงสร้างมากขึ้น แม่นยำ และตรวจสอบได้ เช่นเดียวกับความเสี่ยงอื่นๆ องค์กรสามารถจัดการสิ่งนี้ได้โดยการออกแบบวิธีการควบคุมที่เหมาะสมและนำไปปฏิบัติอย่างมีประสิทธิภาพ

หมายเหตุ

ข้อกำหนดเฉพาะใช้คำศัพท์ทั่วไปของการตรวจสอบภายในตามที่กำหนดไว้ในมาตรฐานการตรวจสอบภายในสากล (Global Internal Audit Standards) ผู้อ่านควรศึกษาอ้างอิงคำศัพท์และคำจำกัดความต่างๆ ในอภิธานศัพท์ (Glossary) ของมาตรฐาน



ข้อกำหนดเฉพาะเรื่องพฤติกรรมองค์กร (Organizational Behavior Topical Requirement) ได้ยอมรับแนวคิดนี้ โดยกำหนดข้อกำหนดขั้นต่ำที่เป็นภาคบังคับ (Minimum Mandatory Requirements) เพื่อประเมินพฤติกรรมเมื่อผลการประเมินความเสี่ยงระบุว่าอยู่ในขอบเขตของการสอบทาน ข้อกำหนดเหล่านี้สามารถเข้ากันได้เป็นอย่างดีกับแนวทางการตรวจสอบซึ่งอิงตามความเสี่ยง (Risk-based Audit Approach) แบบดั้งเดิม และสามารถนำไปปรับใช้กับหน่วยงานตรวจสอบทุกหน่วยงานโดยมีการปรับเปลี่ยนเพียงเล็กน้อย คู่มือผู้ใช้นี้ได้ให้ตัวอย่างในทางปฏิบัติเกี่ยวกับวิธีการผนวกแนวทางนี้เข้ากับงานตรวจสอบที่ได้รับมอบหมายทั่วไป ตลอดจนคำแนะนำในการสอบทานกรอบพฤติกรรมองค์กรในภาพกว้างหรือองค์ประกอบย่อยแต่ละส่วน หัวข้อนี้มีอิทธิพลที่มีนัยสำคัญต่อวัตถุประสงค์ขององค์กร จึงจำเป็นต้องได้รับการพิจารณาและนำไปใช้ในเชิงรุก

คำจำกัดความของคำศัพท์หลักต่อไปนี้มีผลต่อการทำความเข้าใจและการประยุกต์ใช้ข้อกำหนดเฉพาะ เนื่องจากหัวข้อนี้ยังอยู่ในช่วงเริ่มต้นของการพัฒนา องค์กรต่างๆ อาจใช้คำศัพท์เหล่านี้ไม่สอดคล้องกัน คำจำกัดความที่ให้ไว้ควรช่วยให้ผู้ใช้สามารถปรับคำศัพท์ขององค์กรตนเองให้สอดคล้องกับคำศัพท์ที่ใช้ในข้อกำหนดเฉพาะและในคู่มือผู้ใช้นี้

- **สิ่งจูงใจที่มีผลต่อพฤติกรรม (behavioral incentives)** – สิ่งใดๆ ก็ตามที่สามารถมอบให้เพื่อสร้างแรงจูงใจที่มีผลต่อพฤติกรรม ซึ่งรวมถึงสิ่งจูงใจที่เป็นตัวเงิน เช่น การขึ้นเงินเดือน โบนัส หรือสิทธิในการซื้อหุ้น หรือสิ่งจูงใจที่ไม่ใช่ตัวเงิน เช่น คำ ชมเชย การมอบหมายงานที่พึงพอใจ หรือวันหยุด
- **รูปแบบพฤติกรรม (behavioral patterns)** – รูปแบบของพฤติกรรมที่เกิดขึ้นซ้ำๆ หรือบ่อยครั้ง โดยรูปแบบได้ถูกระบุในภาพรวมว่าเป็น "วิถีที่สิ่งต่างๆ ถูกปฏิบัติ" ซึ่งจะตรงข้ามกับสถานการณ์ที่เกิดขึ้นเพียงครั้งเดียว
- **ความเสี่ยงด้านพฤติกรรม (behavioral risk)** – ความเสี่ยงที่พฤติกรรมไม่สอดคล้องกับวัตถุประสงค์ขององค์กร
- **ตัวชี้วัดความเสี่ยงด้านพฤติกรรม (behavioral risk indicators)** – ข้อมูลเพื่อบริหารจัดการที่สามารถนำไปปฏิบัติได้จริงเกี่ยวกับพฤติกรรม
- **คณะกรรมการ (board)** – องค์กรคณะระดับสูงสุดที่รับผิดชอบในการกำกับดูแล
- **ความประพฤติ (conduct)** – พฤติกรรมที่เกี่ยวข้องกับข้อกำหนดและความคาดหวังของหน่วยงานทางการที่กำกับดูแล



- **วัฒนธรรม (culture)** – การตัดสินใจเลือกของพนักงานในการปฏิบัติหน้าที่และวิธีการทำงานร่วมกับผู้อื่นพร้อมกับปัจจัยที่ขับเคลื่อนพฤติกรรมองค์กรเหล่านั้น ปัจจัยขับเคลื่อนรวมถึงกลไกที่เป็นทางการ เช่น สิ่งจูงใจและเป้าหมาย และกลไกที่ไม่เป็นทางการ เช่น ค่านิยมและความเชื่อร่วมกัน
- **พฤติกรรมองค์กร (organizational behavior)** – การตัดสินใจเลือกของพนักงานที่สังเกตเห็นได้ในการปฏิบัติงานและวิธีการทำงานร่วมกับผู้อื่น พฤติกรรมนี้มีอิทธิพลต่อผลการปฏิบัติงานและการบรรลุวัตถุประสงค์ขององค์กร พูดย่างๆ คือ พฤติกรรมองค์กรคือ "วิถีที่เราทำสิ่งต่างๆ" และถือเป็นส่วนย่อยของวัฒนธรรม
- **การสอบทานผลการปฏิบัติงาน (performance reviews)** – การประเมินผลรายบุคคลหรือกลุ่มเกี่ยวกับความเพียงพอของงานที่บุคคลหรือกลุ่มปฏิบัติ
- **ผู้มีส่วนได้เสีย (stakeholder)** – กลุ่มผู้ที่มีผลประโยชน์ทางตรงหรือทางอ้อมในกิจกรรมและผลประกอบการขององค์กร ผู้มีส่วนได้เสียอาจรวมถึงคณะกรรมการ ผู้บริหาร พนักงาน ลูกค้า ผู้ขาย ผู้ถือหุ้น หน่วยงานทางการที่กำกับดูแล สถาบันการเงิน ผู้ตรวจสอบภายนอก สาธารณชน และอื่นๆ
- **ค่านิยม (values)** – หลักการที่เป็นแนวทางว่าบุคคลพึงประพฤติปฏิบัติอย่างไร

หมวดย่อย (Sections)

ข้อกำหนดที่เป็นข้อบังคับในข้อกำหนดเฉพาะเรื่องพฤติกรรมองค์กร และข้อควรพิจารณาที่ไม่เป็นข้อบังคับในคู่มือผู้ใช้นี้ แบ่งออกเป็น 3 หมวดย่อย:

- **การกำกับดูแล (Governance)** – การกำหนดวัตถุประสงค์พื้นฐานและกลยุทธ์ด้านพฤติกรรมองค์กรที่ชัดเจน เพื่อสนับสนุนเป้าหมาย นโยบาย และวิธีการปฏิบัติงานขององค์กร
- **การบริหารความเสี่ยง (Risk management)** – กระบวนการในการระบุ วิเคราะห์ จัดการ และติดตามความเสี่ยงที่เกี่ยวข้องกับพฤติกรรมองค์กร รวมถึงกระบวนการยกระดับการรายงานต่อผู้บริหารระดับที่สูงขึ้น (Escalation) อย่างทันท่วงที
- **การควบคุม (Controls)** – กระบวนการควบคุมที่กำหนดโดยฝ่ายบริหารและมีการประเมินผลเป็นระยะ เพื่อบรรเทาความเสี่ยงที่เกี่ยวข้องกับพฤติกรรมองค์กร



นอกจากข้อกำหนดเฉพาะและคู่มือผู้ใช้นี้แล้ว ผู้ตรวจสอบภายในอาจศึกษาแนวปฏิบัติทางวิชาชีพเกี่ยวกับพฤติกรรมองค์กรเพิ่มเติม เช่น แนวปฏิบัติสากล (Global Guidance) ของ IPPF และแหล่งข้อมูลเฉพาะด้านอื่นๆ ในอุตสาหกรรม



ข้อควรพิจารณา (Considerations)

ผู้ตรวจสอบภายในอาจใช้ข้อควรพิจารณาต่อไปนี้เพื่อช่วยในการประเมินข้อกำหนดในข้อกำหนดเฉพาะเรื่องพฤติกรรมองค์กร ตัวอักษรที่กำกับข้อควรพิจารณาแต่ละข้อข้างล่างนี้จะถูกอ้างอิงโยง (Cross-referenced) กับข้อกำหนดที่สอดคล้องกันในข้อกำหนดเฉพาะ ข้อควรพิจารณาเหล่านี้เป็นเพียงการยกตัวอย่างประกอบแต่ไม่ใช่ภาคบังคับ ผู้ตรวจสอบภายในควรใช้ดุลยพินิจทางวิชาชีพในการตัดสินใจเลือกประเด็นที่จะรวมไว้ในการประเมิน

สำหรับงานตรวจสอบภายในภาครัฐ ข้อจำกัดอันเนื่องมาจากกฎหมาย โครงสร้างรัฐบาล หรือสภาพแวดล้อมทางการเมืองถือเป็นอุปสรรคที่อาจเกิดขึ้นในการจัดการบางแง่มุมของงานนั้น ผู้ตรวจสอบภายในภาครัฐควรจัดทำเอกสารระบุข้อจำกัดเกี่ยวกับขอบเขตของงานดังกล่าวไว้เป็นส่วนหนึ่งของกระบวนการประเมินความเสี่ยง และใช้ดุลยพินิจทางวิชาชีพเพื่อกำหนดและสื่อสารขอบเขตการสอบทานที่ปรับให้เหมาะสมแล้วอย่างชัดเจน

ข้อควรพิจารณาด้านการกำกับดูแล (Governance Considerations)

ในการประเมินการนำกระบวนการด้านการกำกับดูแลมาประยุกต์ใช้กับพฤติกรรมองค์กร ผู้ตรวจสอบภายในอาจสอบทานประเด็นดังต่อไปนี้:

A. โครงสร้างบทบาทและความรับผิดชอบ เพื่อให้มั่นใจว่าคณะกรรมการยังคงความสามารถติดตามและมีอิทธิพลต่อมิติทางพฤติกรรมขององค์กร หลักฐานอาจรวมถึง:

- คณะกรรมการกำกับดูแล (governance committee):
 - จัดตั้งและรักษาคณะกรรมการหรือคณะอนุกรรมการเฉพาะด้านที่มุ่งเน้นเรื่องพฤติกรรมองค์กร โดยมีอำนาจหน้าที่ ที่ชัดเจนในการเชื่อมโยงการควบคุมดูแลพฤติกรรมองค์กรเข้ากับการขับเคลื่อนกลยุทธ์



- ทบทวนตัวชี้วัดความเสี่ยงด้านพฤติกรรม (behavioral risk indicators) ที่สอดคล้องกับเป้าหมายธุรกิจระยะยาวอย่างสม่ำเสมอ โดยตัวชี้วัดความเสี่ยงด้านพฤติกรรมเป็นมาตรวัดสำหรับพิจารณาว่าจำเป็นต้องดำเนินการใดๆ หรือไม่ เพื่อให้มั่นใจว่าพฤติกรรมยังคงสอดคล้องกับวัตถุประสงค์ ค่านิยมที่เกี่ยวข้อง และจุดมุ่งหมายขององค์กร
- รวมเอาวัตถุประสงค์ด้านพฤติกรรมเข้าไว้ในกระบวนการประเมินผลการปฏิบัติงานและค่าตอบแทนของผู้บริหาร
- กรอบการรายงานต่อคณะกรรมการ (Board reporting frameworks):
 - ให้ข้อมูลเชิงลึกเกี่ยวกับตัวชี้วัดความเสี่ยงด้านพฤติกรรม โดยการใช้แดชบอร์ด (Dashboards) ที่มีโครงสร้างชัดเจน (เช่น ความผูกพันของพนักงาน แนวโน้ม เหตุการณ์ ความพึงพอใจของลูกค้า การยกย่องพนักงานตามค่านิยม)
 - การนำมาตรวัดด้านวัฒนธรรมที่เกี่ยวข้องมาบูรณาการเข้ากับการรายงานผลการดำเนินงานเชิงกลยุทธ์ในระดับคณะกรรมการ
- กลไกการรับฟังความคิดเห็นของผู้มีส่วนได้เสีย (Stakeholder feedback) เช่น การสำรวจ ช่วยให้:
 - คณะกรรมการได้รับความเห็นโดยตรงเกี่ยวกับการปรับปรุงพฤติกรรมให้สอดคล้องกับค่านิยมและกลยุทธ์จากพนักงาน ลูกค้า และผู้มีส่วนได้เสียอื่นๆ
 - ความคิดเห็นดังกล่าวถูกนำไปใช้ในการกำหนดทิศทางเชิงกลยุทธ์และการกำหนดมาตรการจัดการด้านพฤติกรรม

B. การจัดการพฤติกรรมองค์กรที่มีประสิทธิผลเกิดขึ้นได้จากการกำหนดความรับผิดชอบที่ชัดเจนทั่วทั้งองค์กร คณะกรรมการเป็นผู้รับผิดชอบสูงสุดในการทำให้มั่นใจว่าองค์กรส่งเสริมพฤติกรรมที่สอดคล้องกับวัตถุประสงค์ ซึ่งรวมถึงการกำหนดความคาดหวังที่ชัดเจนด้านความประพฤติ การควบคุมดูแล การรายงานความเสี่ยง และการตั้งคำถามต่อฝ่ายบริหารเมื่อมีการตรวจพบความไม่สอดคล้อง หลักฐานอาจรวมถึง:

- คณะกรรมการ:
 - อนุมัติระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) ด้านพฤติกรรมและวัตถุประสงค์หลักด้านวัฒนธรรม
 - กำหนดให้มีการรายงานตัวชี้วัดความเสี่ยงด้านพฤติกรรมอย่างสม่ำเสมอ (ตัวอย่างเช่น แนวโน้ม รูปแบบเหตุการณ์ ประเด็นจากการแจ้งเบาะแส)



- กำหนดให้ฝ่ายบริหารระดับสูงต้องรับผิดชอบต่อผลงานด้านวัฒนธรรมโดยผ่านกลไกต่างๆ เช่น โครงสร้างสิ่งจูงใจและ "แบบอย่างของผู้นำ (Tone at the Top)"
 - ประชุมร่วมกับหน่วยงานในแนวป้องกันด้านที่สองและสาม ในประเด็นที่เกี่ยวข้องกับการยกระดับการรายงานความเสี่ยงด้านพฤติกรรม ช่องว่างในการควบคุมดูแล และความเพียงพอของแผนการแก้ไขปัญหา
- หน่วยธุรกิจและฝ่ายบริหารระดับปฏิบัติการนำความคาดหวังด้านพฤติกรรมไปฝังไว้ในการทำงานประจำวัน เพื่อให้มั่นใจว่าการตัดสินใจ การสื่อสาร และการทำงานร่วมกันของทีม (Team Dynamic) สะท้อนค่านิยมขององค์กรที่กำหนดไว้ ซึ่งอาจรวมถึงความรับผิดชอบอย่างเต็มที่ในด้าน:
 - การเป็นแบบอย่างของพฤติกรรมที่พึงประสงค์และการรักษาสภาพแวดล้อมที่ปลอดภัยทางจิตใจ (Psychologically safe environment)
 - การนำวิธีการควบคุมที่มีอิทธิพลต่อพฤติกรรมไปใช้ปฏิบัติ เช่น การสรรหานักเลง การให้รางวัล การสื่อสาร และกิจวัตรของผู้นำ
 - การระบุและส่งรายงานความเสี่ยงด้านพฤติกรรมขึ้นไปตามลำดับชั้นแบบเชิงรุกเมื่อความเหล่านั้เกิดขึ้นในสภาพแวดล้อมการทำงาน
 - มาตรการบรรเทาความเสี่ยงด้านพฤติกรรมซึ่งเป็นผลมาจากพฤติกรรมที่ไม่สอดคล้องกันภายในทีม และความจำเป็นที่ต้องมีวิธีการควบคุม (ทั้งที่เป็นทางการและไม่เป็นทางการ)
 - หน่วยงานด้านความเสี่ยง ด้านการปฏิบัติตามกฎเกณฑ์ ด้านทรัพยากรบุคคล และหน่วยงานควบคุมดูแลที่เกี่ยวข้อง ออกแบบและดูแลรักษากรอบความเสี่ยงด้านพฤติกรรมขององค์กร ซึ่งรวมถึง:
 - กำหนดบทบาทและหน้าที่ในการควบคุมดูแลด้านพฤติกรรม
 - กำหนดช่องทางการยกระดับการรายงาน และกระบวนการวิเคราะห์ข้อมูล
 - จัดทำแดชบอร์ด การวิเคราะห์เฉพาะเรื่อง (Thematic analyses) และการประเมินเป็นระยะ เพื่อให้ข้อมูลเชิงลึกในลักษณะมองไปข้างหน้าเกี่ยวกับสภาวะด้านพฤติกรรมทั่วทั้งองค์กร
 - มีความสามารถในการตั้งคำถามเกี่ยวกับวิธีปฏิบัติที่สิ่งจูงใจ การสื่อสาร หรือพฤติกรรมผู้นำ เบี่ยงเบนไปจากเป้าหมายที่กำหนด



- ให้คำปรึกษาเกี่ยวกับการเปลี่ยนแปลงที่สำคัญในวิธีการควบคุมที่เกี่ยวข้องกับคน กรอบการกำกับดูแล หรือโครงการริเริ่มเพื่อการเปลี่ยนแปลงเชิงกลยุทธ์ที่อาจมีอิทธิพลต่อวัฒนธรรม
- ทบทวนแนวโน้มที่กำลังเกิดขึ้นใหม่จากรายงานเหตุการณ์ ข้อตรวจพบจากการตรวจสอบ และกลไกการให้ความเชื่อมั่นอื่นๆ ที่ระบุถึงประเด็นด้านพฤติกรรม

C. กระบวนการกำกับดูแลที่มั่นใจว่ามีการควบคุมดูแลด้านพฤติกรรม การติดตาม การประเมินผล และความสอดคล้องกันระหว่างรูปแบบพฤติกรรมและวัตถุประสงค์องค์กรอย่างสม่ำเสมอ กระบวนการอาจรวมถึง:

- การใช้แดชบอร์ด เพื่อแสดงข้อมูลสำคัญจากแหล่งต่างๆ เช่น ผลสำรวจความพึงพอใจและวัฒนธรรมของพนักงาน อัตราการลดลงและการขาดงานของพนักงาน เนื้อหาจากช่องทางการแสดงความคิดเห็น ข้อมูลเหตุการณ์ และมาตรวัดผลการปฏิบัติงานและนวัตกรรม ลักษณะของแดชบอร์ดที่มีประสิทธิภาพประกอบด้วย:
 - มีการกำหนดค่าเกณฑ์ (Threshold values) เพื่อระบุโอกาสในการปรับปรุงพฤติกรรม
 - มีการแยกข้อมูลพฤติกรรม (เช่น ข้อมูลจากช่องทางการแสดงความคิดเห็น) ออกจากข้อมูลปัจจัยขับเคลื่อน (เช่น ความชัดเจนของบทบาทหน้าที่) และข้อมูลผลลัพธ์ (เช่น ข้อร้องเรียนของลูกค้า)
 - มีการผนวกข้อมูลเชิงปริมาณ (เช่น จากการสำรวจ) เข้ากับข้อมูลเชิงคุณภาพ (เช่น จากการสนทนาเฉพาะกลุ่มเป้าหมาย (focus groups) และข้อมูลจากช่องทางการแสดงความคิดเห็น)
- การที่คณะกรรมการทำความเข้าใจเกี่ยวกับแง่มุมต่างๆ ของพฤติกรรมองค์กรในปัจจุบันเพื่อนำมาปรับใช้และแก้ไข ในอันที่จะเสริมสร้างประสิทธิผลและผลการดำเนินงานขององค์กร แง่มุมเหล่านี้ประกอบด้วย:
 - การตัดสินใจ ซึ่งรวมถึงการแสวงหามุมมองที่แตกต่างและการท้าทาย
 - การสื่อสารระหว่างพนักงาน ซึ่งรวมถึงการแสดงข้อกังวลและความคาดหวังต่างๆ
 - พนักงานทำงานร่วมกัน ซึ่งรวมถึงการทำงานข้ามทีมและเมื่อมีการจัดการความขัดแย้ง
 - พนักงานตอบสนองต่อความล้มเหลว ตัวอย่างเช่น การเรียนรู้จากความผิดพลาด หรือการตอบสนองด้วยการตำหนิหรือปฏิเสธ



- พฤติกรรมของผู้ในระดับกลางและระดับสูงส่งผลกระทบต่อพฤติกรรมด้านอื่นๆ อย่างไร (ตัวอย่างเช่น ผู้นำตอบสนองต่อข้อผิดพลาดอย่างไร และเปิดรับการโต้แย้งหรือทักท้วงในการตัดสินใจเพียงใด)
- กลยุทธ์และรูปแบบธุรกิจขับเคลื่อนการตัดสินใจ ประมวลผลความประพฤติ (Code of Conduct) และการบริหารผลการปฏิบัติงานด้านสิ่งจูงใจ/มาตรการยับยั้งอย่างไร
- คณะกรรมการกำหนดให้มีระบบการเรียนรู้อย่างต่อเนื่องที่ระบุโอกาสในการปรับปรุงและจัดการอย่างจริงจังและวัดผลได้ โดย:
 - การใช้ข้อมูลเชิงลึกโดยอิงหลักฐาน (Evidence-based insights) จากพฤติกรรมจริงของพนักงาน
 - มุ่งเน้นไปที่สิ่งที่รับรู้ว่าจะเกิดขึ้นจริงภายในองค์กรมากกว่าสิ่งที่ตั้งใจหรือปรารถนาให้เป็น
 - ประเมินข้อมูลเชิงคุณภาพและเชิงปริมาณผสมผสานกัน ซึ่งมักจะได้มาจากการสำรวจช่องทางรายงานเหตุการณ์ บทสนทนาที่เป็นความลับ และการสนทนาเฉพาะกลุ่มเป้าหมาย
 - นำข้อมูลเชิงลึกมาใช้เพื่อกำหนดสิ่งที่ต้องกระทำเพื่อเสริมสร้างและจัดการกับแง่มุมนั้นๆ ของพฤติกรรมองค์กร
 - รวมแผนปฏิบัติการเพื่อผนวกมาตรการแทรกแซงที่ตรงจุดในประเด็นวิกฤต (ตัวอย่างเช่น กลยุทธ์การสื่อสาร การฝึกอบรม การพัฒนาภาวะผู้นำ การหารือในระดับทีม)

D. นโยบายและวิธีการปฏิบัติงานที่เกี่ยวข้องกับระเบียบวิธีการจัดการความเสี่ยงด้านพฤติกรรมได้รับการจัดตั้ง ทบทวนเป็นระยะ สื่อสารอย่างมีประสิทธิภาพ และมีบูรณาการเข้ากับการดำเนินงานทางธุรกิจและการตัดสินใจ นโยบายและวิธีการปฏิบัติงานที่ครอบคลุมด้านจริยธรรม ทรัพยากรบุคคล การปฏิบัติตามกฎเกณฑ์ ความเสี่ยง การปฏิบัติงาน และอำนาจในการตัดสินใจ เพื่อให้มั่นใจว่า:

- ความคาดหวังด้านพฤติกรรมถูกระบุไว้อย่างเป็นทางการในนโยบายที่เกี่ยวข้อง (เช่น ประมวลผลความประพฤติและ/หรือนโยบายจริยธรรม (Policy on Ethics) ทรัพยากรบุคคล สิ่งจูงใจ และการมอบอำนาจ) นโยบายดังกล่าวควรระบุพฤติกรรมที่ยอมรับได้และยอมรับไม่ได้พร้อมตัวอย่างในทางปฏิบัติที่ชัดเจน และสอดคล้องกับระดับความเสี่ยงที่ยอมรับได้ขององค์กร
- หน่วยงานบริหารความเสี่ยงเปรียบเทียบความคาดหวังด้านพฤติกรรมกับกระบวนการปฏิบัติงานหลักๆ (เช่น การจ้างงาน การประเมินผลงาน การประชุมพิเศษ และการบริหารจัดการลูกค้า) โดยมั่นใจว่า



พฤติกรรมเหล่านั้นสะท้อนอยู่ในการตัดสินใจประจำวัน งานตรวจสอบให้เชื่อมั่นควรทดสอบว่า ความคาดหวังเหล่านี้มีอิทธิพลต่อพฤติกรรมจริงอย่างไรและรายงานให้คณะกรรมการทราบตามลำดับ

- คณะกรรมการแสวงหาและได้รับความเชื่อมั่นว่านโยบายองค์กรเข้าถึงได้ง่ายและมีการสื่อสารอย่างชัดเจนผ่านหลายช่องทาง (ตัวอย่างเช่น อินทราเน็ต การฝึกอบรม การประชุมพนักงานทั้งองค์กร (town hall)) การนำกรณีศึกษาและแผนภาพต้นไม้เพื่อการตัดสินใจ (decision tree) มาผนวกไว้จะช่วยให้เข้าใจบริบทเกี่ยวกับความคาดหวังด้านพฤติกรรมได้ชัดเจนยิ่งขึ้น แดชบอร์ดสามารถใช้ติดตามระดับความเข้าใจและมาตรการการใช้งานได้
- นโยบายและวิธีปฏิบัติงานด้านพฤติกรรมทั้งหมดมีรอบการทบทวนตามกำหนดการและปรับปรุงตามเหตุการณ์ที่เกิดขึ้น ผลสำรวจ หรือ การเปลี่ยนแปลงกฎระเบียบของทางการ หน่วยงานในแนวป้องกันด้านที่สองควรจัดทำทะเบียนการถอดบทเรียน (Lessons-learned register) เพื่อระบุช่องว่างระหว่างพฤติกรรมและวัตถุประสงค์องค์กรที่กำลังเกิดขึ้น
- คณะกรรมการได้รับข้อมูลที่เป็นปัจจุบันอย่างสม่ำเสมอเกี่ยวกับความครอบคลุม ความชัดเจน และประสิทธิผลของนโยบาย หน่วยงานในแนวป้องกันด้านที่สองควรวิเคราะห์การละเมิด ผลกระทบของนโยบาย และความสอดคล้องกับพฤติกรรมที่พึงประสงค์ โดยควรมีการทบทวนประสิทธิผลของนโยบาย โดยผ่านความคิดเห็นตอบกลับเชิงคุณภาพและตัวชี้วัดความเสี่ยงด้านพฤติกรรม

ข้อควรพิจารณาด้านการบริหารความเสี่ยง (Risk Management Considerations)

เพื่อประเมินว่ากระบวนการบริหารความเสี่ยงได้ถูกนำไปใช้กับพฤติกรรมองค์กรอย่างไร ผู้ตรวจสอบภายในอาจสอบถามว่า:

A. กระบวนการบริหารความเสี่ยงด้านพฤติกรรมได้มีการกำหนดไว้อย่างชัดเจน และครอบคลุมถึงลักษณะทางพฤติกรรมที่มีความสำคัญต่อการบรรลุวัตถุประสงค์ขององค์กร ลักษณะของการบริหารความเสี่ยงอาจรวมถึง:

- บทบาทและหน้าที่สอดคล้องกับกรอบการบริหารความเสี่ยงองค์กร และกรอบการกำกับดูแล โดยมีสายการรายงานที่เอื้อต่อความเป็นอิสระและส่งผลต่อการตัดสินใจ
- มีอำนาจในการโต้แย้งหรือทักท้วงการตัดสินใจ และยกระดับการรายงานประเด็นความเสี่ยงด้านพฤติกรรม โดยไม่ต้องเกรงกลัวต่อการถูกตอบโต้หรือการลดทอนความสำคัญลง



- มีความเป็นอิสระจากฝ่ายบริหารระดับปฏิบัติการ โดยสามารถเข้าถึงผู้บริหารระดับสูงและคณะกรรมการได้โดยตรง
- มีสิทธิเข้าถึงข้อมูลความเสี่ยงด้านพฤติกรรมจากหลายแหล่งที่มีความเกี่ยวข้อง ภายในเวลาที่เหมาะสม และมีการตรวจสอบความสอดคล้องของข้อมูลจากหลายแหล่ง ข้อมูลนี้รวมถึงข้อมูลที่มีโครงสร้าง (เช่น ผลจากการสำรวจ การฝ่าฝืนนโยบาย) และข้อมูลที่ไม่มีโครงสร้าง (ตัวอย่างเช่น รายงานการแจ้งข้อกังวล ข้อมูลเชิงลึกจากการสนทนาเฉพาะกลุ่มเป้าหมาย) แหล่งข้อมูลประกอบด้วยทรัพยากรบุคคล (เช่น อัตราการลดลงของพนักงาน การรักษาพนักงาน และข้อมูลจากการสำรวจ) การแจ้งเบาะแส ข้อร้องเรียนจากลูกค้า และข้อตรวจพบจากการตรวจสอบ
- มีการใช้การวิเคราะห์ข้อมูล (Data Analytics) เพื่อระบุแนวโน้ม สิ่งผิดปกติ และความเสี่ยงที่กำลังเกิดขึ้น
- มีการใช้แดชบอร์ด และตัวชี้วัดความเสี่ยงเพื่อรายงานต่อฝ่ายบริหารและคณะกรรมการ
- มีการใช้ตัวชี้วัดความเสี่ยงด้านพฤติกรรม ที่เชื่อมโยงกับวัตถุประสงค์ขององค์กร
- มีการสอบถามด้วยตนเองหรือว่าจ้างผู้ให้บริการจากภายนอกเพื่อหาสาเหตุที่แท้จริง ของความล้มเหลวในการปฏิบัติตามประมวลความประพฤติ และวัฒนธรรมที่ไม่สอดคล้องกัน
- มีความคุ้นเคยกับปัจจัยขับเคลื่อนพฤติกรรมทั้งที่เป็นทางการและไม่เป็นทางการ (ตัวอย่างเช่น สิ่งจูงใจ ความปลอดภัยทางจิตใจ และท่าทีของผู้นำ)
- ความน่าเชื่อถือและความไว้วางใจที่ผู้บริหารระดับสูงมีต่อทีมปฏิบัติการผนวกกับความสามารถในการมีอิทธิพลต่อการตัดสินใจได้ในขณะที่เกิดเหตุการณ์
- การมีส่วนร่วมอย่างแข็งขันในการออกแบบและวิธีการควบคุมที่เกี่ยวข้องกับทรัพยากรบุคคล (เช่น สิ่งจูงใจ การจ้างงาน และการฝึกอบรม)
- บทบาทที่ปรึกษาในโครงการเปลี่ยนแปลงเชิงกลยุทธ์และความริเริ่มเพื่อการปฏิรูปองค์กร
- การสร้างความผูกพันกับผู้นำทางธุรกิจเพื่อหล่อหลอมวัฒนธรรมผ่านการใช้อิทธิพลโน้มน้าวจิตใจ ไม่ใช่เพียงแค่การบังคับ
- การจัดเก็บและวิเคราะห์ข้อมูลอย่างต่อเนื่อง ซึ่งอาจรวมถึง:
 - แบบสำรวจความผูกพันและความเป็นอยู่ที่ดีของพนักงาน
 - ข้อมูลการยกย่องและให้รางวัลสำหรับพฤติกรรมที่ขับเคลื่อนค่านิยมองค์กร



- รายงานการแจ้งเบาะแสและข้อร้องเรียนต่างๆ
- คำติชมของลูกค้าที่เน้นให้เห็นทั้งความพึงพอใจและไม่พึงพอใจ
- การประเมินผลการปฏิบัติงานที่สะท้อนถึงความร่วมมือ ความซื่อสัตย์สุจริต และนวัตกรรม
- การใช้วิธีการวิเคราะห์ข้อมูลเพื่อระบุจุดเปราะบางและตรวจจับแนวโน้มต่าง ๆ
- กระบวนการที่กำหนดไว้อย่างชัดเจนในการยกระดับการรายงานเรื่องความเสี่ยง และพฤติกรรมที่ไม่สอดคล้องกับวัตถุประสงค์ขององค์กรอย่างทันท่วงที
- การควบคุมดูแลการกำหนดและการดำเนินการตามแผนปฏิบัติการของฝ่ายบริหาร เพื่อจัดการความเสี่ยงและส่งเสริมพฤติกรรมที่จำเป็น

B. กระบวนการติดตามพฤติกรรมองค์กรในเวลาที่เหมาะสม รวมถึงการรายงานผลให้ผู้มีส่วนได้เสียทราบ ตัวอย่างของตัวชี้วัดความเสี่ยงในหมวดพฤติกรรม บัณฑิตขับเคลื่อน และประเภทของผลลัพธ์ และข้อบกพร่องที่ควรรายงาน รวมถึง:

- การตัดสินใจ: การขาดการโต้แย้งหรือทักท้วงที่มีประสิทธิผล หรือการไม่เปิดรับมุมมองที่แตกต่างอย่างเพียงพอ
- การสื่อสาร: การให้ความสนใจต่อประเด็นที่ได้รับรายงานจากพนักงานอย่างไม่เพียงพอ
- การทำงานร่วมกัน: สภาพแวดล้อมการทำงานที่แยกส่วน ซึ่งพนักงานมุ่งเน้นแต่งานของตนเองเท่านั้น
- การตอบสนองต่อข้อบกพร่อง: การกล่าวโทษและลงโทษสำหรับความผิดพลาดที่ไม่ได้ตั้งใจ
- บัณฑิตขับเคลื่อนที่เป็นทางการ: บทบาทและหน้าที่ที่ไม่ชัดเจน หรือเป้าหมายที่ขัดแย้งกัน
- บัณฑิตขับเคลื่อนที่ไม่เป็นทางการ: ความปลอดภัยทางจิตใจต่ำ หรือการทำงานร่วมกันที่ไม่มีประสิทธิผลระหว่างแนวป้องกันทั้งสามด้าน (Three Lines)
- ข้อมูลผลการปฏิบัติงาน: ข้อร้องเรียนของลูกค้าที่มากเกินไป หรือนวัตกรรม หรือการเปลี่ยนผ่านสู่ดิจิทัลที่หยุดชะงัก
- ข้อมูลทรัพยากรบุคคล: อัตราการลดลงและการขาดงานของพนักงานที่สูง และผลสำรวจความพึงพอใจในการทำงานอยู่ในระดับที่ต่ำ
- ข้อมูลความเสี่ยงและกฎหมาย: การสืบสวน การฝ่าฝืนนโยบาย หรือการแจ้งเตือนภัยจำนวนมาก รวมถึงสถานการณ์ที่ก่อให้เกิดความเสียหายแต่สามารถหลีกเลี่ยงได้



C. กระบวนการเพื่อให้มั่นใจว่าความเปี่ยงเบนระหว่างพฤติกรรมที่คาดหวังและที่สังเกตได้ได้รับการระบุและสื่อสารไปยังผู้ที่มีอำนาจและมีความสามารถในการลงมือดำเนินการ ผู้ตรวจสอบภายในอาจสอบถามว่า:

- การสื่อสารที่มีประสิทธิผลต้องภายในเวลาที่เหมาะสม โดยอิงตามหลักฐาน และสนับสนุนด้วยการวิเคราะห์ปัจจัยพื้นฐานและสาเหตุที่แท้จริง
- การออกแบบและประสิทธิผลในการดำเนินการความพยายามในการสื่อสารจะช่วยหลีกเลี่ยงการแก้ไขปัญหาลักษณะซ้ำ ความเสียหายต่อชื่อเสียง หรือความล้มเหลวซ้ำซาก
- ข้อมูลถูกรวบรวมและสังเคราะห์จากหลายแหล่ง ซึ่งรวมถึงความคิดเห็นของพนักงาน รายงานการแจ้งเบาะแส ข้อตรวจพบจากการตรวจสอบ และการสอบถามเหตุการณ์ที่เกิดขึ้น
- เทคนิคการวิเคราะห์อย่างเป็นระบบ (เช่น การสอบถามเฉพาะเรื่อง (Thematic reviews) แบบจำลองพฤติกรรมศาสตร์ และกรอบการวิเคราะห์สาเหตุที่แท้จริง) ช่วยให้การวิเคราะห์ไม่หยุดอยู่เพียงอาการที่ปรากฏภายนอกเพื่อระบุปัจจัยขับเคลื่อนที่อยู่เบื้องหลังความไม่สอดคล้องได้ (ตัวอย่างเช่น สิ่งจูงใจที่ไม่ชัดเจน ความปลอดภัยทางจิตใจต่ำ หรือแบบอย่างของผู้นำที่ไม่มีประสิทธิผล)
- การนำเสนอช่องว่างไม่ใช่แค่การฝ่าฝืนกฎเกณฑ์หรือเหตุการณ์ที่เกิดขึ้นเฉพาะกรณี แต่เป็นเหตุการณ์ที่มีสาเหตุที่แท้จริงมาจากพฤติกรรม ซึ่งสะท้อนถึงปัญหาทางวัฒนธรรม ปัญหาเชิงระบบ และ/หรือปัญหาด้านภาวะผู้นำ
- การสื่อสารชี้ให้เห็นถึงสิ่งที่เกิดขึ้นและเพราะเหตุใดถึงเกิด โดยอาศัยข้อมูลเชิงปริมาณและเชิงคุณภาพมาสนับสนุนข้อสรุป
- องค์การมีการแยกระหว่างรูปแบบพฤติกรรม จุดอ่อนที่เกิดจากปัจจัยขับเคลื่อน พฤติกรรม และผลลัพธ์ขององค์กร (ตัวอย่างเช่น ผลกระทบต่อผลการปฏิบัติงาน ความเชื่อมั่นของผู้มีส่วนได้เสีย) ออกจากกันเพื่อให้สามารถจัดการกับพฤติกรรมและปัจจัยขับเคลื่อนพฤติกรรมเหล่านั้นได้ ข้อตรวจพบต้องถูกสื่อสารไปยังกลุ่มเป้าหมายที่ต้องในระดับรายละเอียดที่เหมาะสม:
 - ผู้จัดการระดับปฏิบัติการ: เพื่อการแก้ไขกระบวนการในทันที
 - ฝ่ายบริหารระดับสูง: เพื่อจัดสรรทรัพยากร การกำหนดสารที่จะสื่อสาร และการวางตัวที่เป็นแบบอย่าง
 - คณะกรรมการหรือคณะกรรมการที่เกี่ยวข้อง: เพื่อการควบคุมดูแลและพิจารณาผลกระทบเชิงกลยุทธ์



- มีการใช้เครื่องมือในการแสดงผลที่เป็นภาพและคำบรรยาย เช่น แดชบอร์ด แผนภูมิความเสี่ยง (Heat maps) หรือบทสรุปกรณีศึกษาที่อธิบายข้อตรวจพบ และสนับสนุนข้อเสนอแนะและ/หรือแผนปฏิบัติการ
- ผลกระทบต่อระดับความเสี่ยงที่องค์กรเผชิญอยู่ (Risk exposure) และความสามารถในการฟื้นตัวของสภาพแวดล้อมการควบคุมได้ถูกรวมไว้ในการสอบทานกระบวนการ
- การสื่อสารถึงช่องว่างต้องเชื่อมโยงกับมาตรการแก้ไขและมีการติดตามจนกว่าจะแล้วเสร็จ
- ผลลัพธ์ของการดำเนินการแทรกแซง (Interventions) จะได้รับการประเมินและแบ่งปันเพื่อให้องค์กรเรียนรู้ครบสมบูรณ์
- การสื่อสารต้องปราศจากอิทธิพลที่ไม่เหมาะสม และสอดคล้องกับระเบียบวิธีการยกระดับการรายงาน (Escalation protocols) ที่กำหนดไว้ เพื่อรักษาความเป็นอิสระและความน่าเชื่อถือของการประเมิน

D. ช่องว่างระหว่างพฤติกรรมที่คาดหวังและพฤติกรรมจริงได้รับการแก้ไข ในลักษณะที่มีโครงสร้างและการมีส่วนร่วม เพื่อให้มั่นใจว่าการแก้ไขนั้นมีรากฐานมาจากความเข้าใจและมุมมองของผู้มีส่วนได้เสียมีการติดตามจนเสร็จสิ้น และได้รับการประเมินประสิทธิผล ผู้ตรวจสอบภายในอาจสอบถามว่า:

- กระบวนการแก้ไขปัญหาดำเนินการโดยผู้มีส่วนได้เสียใกล้ชิดกับประเด็นปัญหาเข้ามามีส่วนร่วมอย่างมีความหมาย เช่น ผู้จัดการ ระดับปฏิบัติการ ทรัพยากรบุคคล พันธมิตรทางธุรกิจ ตัวแทนพนักงาน ที่ปรึกษาด้านการปฏิบัติตามกฎเกณฑ์ และบุคคลหรือทีมที่ได้รับผลกระทบ ข้อมูลจากบุคคลเหล่านี้จะช่วยให้อ้างอิงว่าการดำเนินการนั้น:
 - อิงตามบริบทจริง: ใส่ใจต่อความเป็นจริงในการปฏิบัติงานและบรรทัดฐานที่ไม่เป็นทางการซึ่งอาจเป็นสาเหตุของช่องว่างดังกล่าว
 - มีความน่าเชื่อถือและได้รับการยอมรับ: มีแนวโน้มที่จะได้รับการสนับสนุนและนำไปปฏิบัติจริงในองค์กรหากการดำเนินการนั้นถูกหล่อหลอมโดยผู้ที่มีส่วนเกี่ยวข้องโดยตรง
 - ตั้งคำถามอย่างสร้างสรรค์: เปิดโอกาสให้มีการสะท้อนความคิดเห็นอย่างตรงไปตรงมาเกี่ยวกับพฤติกรรมของผู้หน้าที่ส่งผลกระทบต่อผลลัพธ์ จุดอ่อนในการออกแบบการควบคุม หรือการทำงานร่วมกันของกลุ่ม

- มีการนำความคิดเห็นจากผู้มีส่วนได้เสียมาสังเคราะห์ และผนวกเข้าไว้ในแผนปฏิบัติการ โดยกลไกการรับฟังความคิดเห็นอาจรวมถึง การสัมภาษณ์ กลุ่มเป้าหมาย การวินิจฉัยด้วยแบบสำรวจ และวิธีการอื่นๆ
- มาตรการแก้ไขได้รับการจัดทำเป็นเอกสาร โดยกำหนดผู้รับผิดชอบ กรอบเวลา และเกณฑ์ความสำเร็จ:
 - การดำเนินการต่างๆ ได้สัดส่วนกับความรุนแรงของประเด็นปัญหา
 - ในกรณีที่จำเป็น การดำเนินการต่างๆ จะมุ่งเป้าไปที่ปัจจัยขับเคลื่อนที่เป็นทางการ (ตัวอย่างเช่น นโยบาย สิ่งจูงใจ) และปัจจัยขับเคลื่อนที่ไม่เป็นทางการ (ตัวอย่างเช่น วัฒนธรรม ทัศนคติ การทำงานร่วมกันของทีม)
 - ในกรณีที่มีหลายหน่วยงานเข้ามาเกี่ยวข้อง (ตัวอย่างเช่น ทรัพยากรบุคคลสำหรับการฝึกอบรม ฝ่ายบริหารความเสี่ยงสำหรับวิธีการควบคุม) มีการประสานงานและกำหนดความรับผิดชอบของการส่งมอบงานข้ามสายงานให้ชัดเจน
- มีการติดตามความคืบหน้าจนเสร็จสมบูรณ์ เพื่อให้มั่นใจว่าข้อตกลงได้รับการปฏิบัติตามและคงอยู่ต่อไป ซึ่งรวมถึง
 - การจัดทำทะเบียนรายการประเด็น/มาตรการแก้ไขด้านพฤติกรรม (Behavioral issue/action register) หรือกลไกที่เทียบเท่า
 - การติดตามผลเป็นประจำกับผู้รับผิดชอบมาตรการแก้ไขเพื่อยืนยันสถานะ
 - การยกระดับการรายงานเรื่องที่มีความล่าช้า การแก้ไขที่ไม่ครบถ้วน หรือการต่อต้านการเปลี่ยนแปลงไปที่ช่องทางการกำกับดูแลที่เหมาะสม
- มีการประเมินประสิทธิผลของวิธีการแก้ไขในการปิดช่องว่างและลดความเสี่ยงด้านพฤติกรรม ซึ่งอาจเกี่ยวข้องกับ:
 - การประเมินตัวชี้วัดความเสี่ยงด้านพฤติกรรมอีกครั้งภายหลังจากการนำมาตรการไปปฏิบัติ
 - การเก็บรวบรวมความคิดเห็นจากผู้มีส่วนได้เสียที่ได้รับผลกระทบจากการเปลี่ยนแปลงที่สังเกตได้
 - การทดสอบการเปลี่ยนแปลงพฤติกรรมผ่านการสังเกต การสำรวจ หรือเทคนิคการตรวจสอบ
 - การปรับเปลี่ยนมาตรการหรือเพิ่มกลไกสนับสนุนในส่วนที่ผลลัพธ์ยังมีจุดอ่อนหรือไม่ชัดเจน



ข้อควรพิจารณาด้านกระบวนการควบคุม (Control Process Considerations)

เพื่อประเมินว่ามีการนำกระบวนการควบคุมไปใช้เพื่อบรรเทาความเสี่ยงที่พฤติกรรมองค์กรจะไม่สอดคล้องกับวัตถุประสงค์ขององค์กรอย่างไร ผู้ตรวจสอบภายในอาจสอบถามประเด็นดังต่อไปนี้:

A. การสอบถามความเสี่ยงด้านพฤติกรรม เพื่อทำความเข้าใจความเสี่ยงที่ขับเคลื่อนโดยพฤติกรรมองค์กรในปัจจุบัน (นั่นคือ ผลกระทบที่ไม่ได้ตั้งใจซึ่งอาจเกิดขึ้นจาก "วิธีที่เราทำสิ่งต่างๆ") ตัวอย่างของการสอบถามดังกล่าว ได้แก่ การประเมินโครงการภายหลังดำเนินการเสร็จสิ้น การวิเคราะห์สาเหตุที่แท้จริง และการสอบถามรายละเอียดการปฏิบัติงานในสถานการณ์จริง

B. กระบวนการรับฟังความคิดเห็นที่มีโครงสร้าง เพื่อทำความเข้าใจว่าฝ่ายบริหารใช้กลไกใดในการสื่อสารความคาดหวังด้านพฤติกรรม (ตัวอย่างเช่น การประชุมพนักงานทั้งองค์กร อีเมล และการประชุมระหว่างบุคคลกับหัวหน้างาน) และประสิทธิผลของท่าทีจากผู้บริหาร (Management tone) ที่มีต่อพฤติกรรมภายในองค์กร ซึ่งสามารถทำได้โดยการประเมินกระบวนการที่รวบรวมและวิเคราะห์การรับรู้และความเข้าใจของพนักงานต่อสารจากคณะกรรมการและผู้บริหารระดับสูง ผู้ตรวจสอบภายในสามารถช่วยองค์กรปรับปรุงกลไกการสื่อสารอย่างต่อเนื่องและช่วยให้มั่นใจว่า แบบอย่างจากผู้นำได้รับการตอบสนองอย่างมีประสิทธิภาพในทุกระดับ โดยการสอบถามการควบคุมที่สำคัญ เช่น:

- การสำรวจ การสัมภาษณ์ และการสนทนาเฉพาะกลุ่มเป้าหมาย กับพนักงานเป็นประจำ โดยสอบถามเกี่ยวกับความชัดเจน ความสม่ำเสมอ และผลกระทบจากการสื่อสารของผู้นำ ซึ่งจะได้รับข้อมูลทั้งเชิงปริมาณและเชิงคุณภาพว่าสารต่างๆ ได้รับการตอบรับและเข้าใจได้ดีเพียงใดในระดับต่างๆ ขององค์กร
- เปิดช่องทางสำหรับการรับข้อเสนอแนะแบบไม่เปิดเผยตัวตนเพื่อให้พนักงานสามารถให้ความคิดเห็นอย่างตรงไปตรงมาโดยไม่ต้องกลัวการถูกตอบโต้ ช่องทางเหล่านี้ควรได้รับการสนับสนุนผ่านแพลตฟอร์มดิจิทัลที่สามารถรับข้อมูลและความคิดเห็นได้แบบทันที โดยควรนำข้อมูลจากช่องทางเหล่านี้มาวิเคราะห์เพื่อตรวจสอบว่า แบบอย่างจากผู้นำเป็นที่เข้าใจดีในหมู่พนักงานทุกระดับหรือไม่
- ความคิดเห็นจากการประชุมผู้บริหารระดับสูงที่รวบรวมผ่านการสำรวจ การสัมภาษณ์ การสนทนาเฉพาะกลุ่มเป้าหมาย รายงานการประชุม และช่องทางแบบไม่เปิดเผยตัวตน เพื่อให้มั่นใจว่าผู้บริหารระดับสูงตระหนักถึงการสื่อสารที่ไม่มีประสิทธิภาพ ความเข้าใจผิด หรือส่วนที่ต้องปรับปรุง ทั้งนี้ผู้บริหารระดับสูงแสดงให้เห็นว่าความคิดเห็นของพนักงานมีคุณค่าโดยการตอบสนองและดำเนินการ



ตามข้อเสนอแนะอย่างจริงจัง หากสิ่งนี้ไม่เกิดขึ้น พนักงานอาจมีแนวโน้มที่จะให้ข้อเสนอแนะน้อยลง เนื่องจากรู้สึกถึงถึงให้คำแนะนำต่างๆ ไปก็ไม่มีอะไรเปลี่ยนแปลง

- ข้อคิดเห็นเกี่ยวกับผลการปฏิบัติงานของผู้บริหารระดับสูงถูกนำไปรวมกับการทบทวนผลการปฏิบัติงานของพวกเขา เพื่อติดตามการรับรู้ต่อคำสั่งของผู้เป็นอย่างต่อเนื่อง สิ่งนี้เน้นย้ำความสำคัญของสารจากผู้นำและทำให้มั่นใจว่าสิ่งเหล่านี้สะท้อนอยู่ในการปฏิบัติงานประจำวัน

C. การยกระดับการรายงานภายในองค์กรได้รับการสนับสนุนให้การระบุและลดความเสี่ยงในระยะแรกเริ่ม และเพื่อสร้างสภาพแวดล้อมที่ปลอดภัยทางจิตใจที่พนักงานรู้สึกสบายใจที่จะรายงานปัญหาโดยไม่ต้องกลัวการถูกตอบโต้ ผู้ตรวจสอบภายในสามารถสอบถามวิธีการควบคุมที่สำคัญเพื่อช่วยเพิ่มประสิทธิภาพการจัดการความเสี่ยง เช่น:

- กลไกการรับฟังความคิดเห็นที่ใช้งานได้ง่าย ซึ่งรวมถึงการรายงานโดยตรงและทางเลือกแบบไม่เปิดเผยตัวตน หรือสายด่วนแจ้งเบาะแสการทุจริต (Whistleblower hotlines) ภายในและภายนอก การสำรวจ กล้องรับความคิดเห็น และแพลตฟอร์มดิจิทัลเพื่อให้สามารถรายงานที่เป็นความลับและบันทึกปัญหาที่บุคคลอาจลังเลที่จะรายงานอย่างเปิดเผย
- กระบวนการรายงานปัญหากำหนดไว้อย่างดีและเข้าใจง่าย พร้อมช่องทางที่หลากหลายทั้งช่องทางตรงและไม่เปิดเผยตัวตนทั้งภายในและภายนอก ตลอดจนความพยายามในการส่งเสริมความตระหนักรู้ของพนักงาน ลักษณะของช่องทางการรายงานควรประกอบด้วย:
 - การให้ความเชื่อมั่นในการรักษาความลับ (Confidentiality) เพื่อปกป้องตัวตนของผู้รายงานปัญหา
 - นโยบายห้ามการตอบโต้ (No-retaliation policies) ที่เคร่งครัด สื่อสารอย่างชัดเจน และบังคับใช้อย่างสม่ำเสมอเพื่อคุ้มครองบุคคลที่รายงานปัญหา
 - การสื่อสารกลับไปยังบุคคลที่รายงานปัญหาที่ระบุชื่อ โดยไม่คำนึงว่าเหตุผลหรือผลลัพธ์จะเป็นอย่างไร
 - การสรุปประเด็นปัญหาที่เคยมีการรายงานและผลลัพธ์ของการดำเนินการแก้ไขทั่วทั้งองค์กรเป็นประจำ เพื่อแสดงให้เห็นว่ามีการรายงานประเด็นปัญหา และมีการดำเนินการไปแล้วจริง และเพื่อให้มั่นใจได้ในเรื่องความโปร่งใสของการดำเนินการตามข้อเสนอแนะ



- การสื่อสารเป็นประจำจากฝ่ายบริหารที่เน้นย้ำความสำคัญของการสื่อสารที่เปิดเผยและการรายงานปัญหา พร้อมทั้งแสดงให้เห็นว่าฝ่ายบริหารเองเป็นแบบอย่างของพฤติกรรมดังกล่าว
- การฝึกอบรมเป็นประจำที่เน้นความสำคัญของความปลอดภัยทางจิตใจ ส่งเสริมให้บุคคลรายงานปัญหา และให้คำแนะนำเกี่ยวกับวิธีการยกระดับการรายงานอย่างเหมาะสม โดยควรอบรมซ้ำเป็นระยะเพื่อเสริมสร้างพฤติกรรมที่พึงประสงค์อย่างต่อเนื่องในระยะยาว
- รางวัลที่ไม่เป็นทางการ (Informal rewards) เช่น การชมเชยด้วยวาจาหรือลายลักษณ์อักษร และการยกย่องชมเชยต่อหน้าสาธารณะสำหรับบุคคลที่รายงานปัญหา
- การสอบทานกระบวนการยกระดับการรายงานเป็นประจำเพื่อให้มั่นใจในประสิทธิผลและประสิทธิภาพ ซึ่งรวมถึงการขอความคิดเห็นจากพนักงานเพื่อระบุและแก้ไขอุปสรรคในการรายงานโดยทันที
- การสื่อสารเกี่ยวกับแนวทางการแก้ไขปัญหาจากข้อเสนอแนะที่ได้รับ

D. โปรแกรมสิ่งจูงใจและมาตรการยับยั้ง (Incentive-disincentive programs) สอดคล้องกับพฤติกรรมที่พึงประสงค์และวัตถุประสงค์ขององค์กร และมีการสื่อสาร ผู้ตรวจสอบภายในอาจสอบทานวิธีการควบคุม เช่น:

- สิ่งจูงใจ - ทั้งที่เป็นตัวเงิน (ตัวอย่างเช่น โบนัส การเลื่อนตำแหน่ง) และไม่ใช่ตัวเงิน (ตัวอย่างเช่น การยอมรับ โอกาสในการพัฒนา) สอดคล้องกับวัตถุประสงค์ขององค์กรและเชื่อมโยงกับการแสดงออกถึงพฤติกรรมที่พึงประสงค์
- เกณฑ์การทบทวนผลการปฏิบัติงานที่สมเหตุสมผลได้ผนวกวิธีการที่จะบรรลุมูลค่าวัตถุประสงค์ (ตัวอย่างเช่น ความร่วมมือ ความซื่อสัตย์ และการยึดลูกค้าเป็นศูนย์กลาง) ควบคู่ไปกับมาตรวัดผลสำเร็จแบบดั้งเดิม (เช่น เป้าหมายทางการเงิน)
- เกณฑ์ให้สิ่งจูงใจและระดับเงื่อนไขที่จะลดหรือระงับสิ่งจูงใจ (Incentive criteria and disincentive thresholds) ถูกกำหนดไว้อย่างชัดเจน ใช้อย่างสม่ำเสมอ และได้รับการสอบทานโดยฝ่ายบริหารหรือฝ่ายทรัพยากรบุคคลเพื่อหลีกเลี่ยงความลำเอียง และผลลัพธ์ที่ไม่ได้ตั้งใจ
- กลุ่มทำงานข้ามสายงาน (Cross-functional groups) ยืนยันความสอดคล้องและความเป็นธรรมในการตัดสินใจเกี่ยวกับสิ่งจูงใจระหว่างหน่วยธุรกิจต่างๆ



- ผลที่ตามมาของการประพฤติมิชอบ (Misconduct) และการฝ่าฝืนทางวัฒนธรรมรวมถึงมาตรการยับยั้งที่ชัดเจนและเหมาะสม (ตัวอย่างเช่น การลดโบนัส หรือการระงับการเลื่อนตำแหน่ง) โดยมีการอธิบายและจัดทำเอกสารเพื่อความโปร่งใส
- โปรแกรมการยกย่องชมเชยที่ไม่ใช่ตัวเงินให้ความสำคัญกับพนักงานที่เป็นแบบอย่างของคุณค่าทางวัฒนธรรม เช่น การตัดสินใจอย่างมีจริยธรรมและความปลอดภัยทางจิต
- ผลกระทบของโปรแกรมสิ่งจูงใจได้รับการประเมินอย่างสม่ำเสมอโดยผ่านความคิดเห็นของพนักงานและมาตรวัดทางพฤติกรรม เพื่อปรับปรุงหรือปรับสมดุลกลไกการให้รางวัล ควรประเมินและปรับปรุงโปรแกรมสิ่งจูงใจ เพื่อให้มั่นใจว่า:
 - เป้าหมายไม่แคบหรือกว้างจนเกินไป
 - เป้าหมายสามารถบรรลุได้จริง
 - เป้าหมายระยะสั้นไม่บ่อนทำลายผลลัพธ์ระยะยาว
 - มีการระบุระดับการรับความเสี่ยง (Risk-taking) ไว้อย่างชัดเจน
 - มีการนำมาตรการป้องกันมาใช้เพื่อให้มั่นใจว่าเกิดพฤติกรรมที่มีจริยธรรมในขณะที่กำลังบรรลุเป้าหมาย (ตัวอย่างเช่น ผู้นำเป็นแบบอย่าง ต้นทุนของการทุจริตสูงกว่าผลประโยชน์ที่จะได้รับ และมีการควบคุมดูแลที่เข้มแข็ง)
 - เป้าหมายถูกปรับให้เหมาะสมกับความสามารถและสถานการณ์ของแต่ละบุคคล โดยยังคงรักษาความเป็นธรรมไว้
 - เป้าหมายของทีมไม่ขัดแย้งกับเป้าหมายส่วนบุคคล
 - มีการประเมินแรงจูงใจภายใน และฝ่ายบริหารตระหนักว่าเป้าหมายบางอย่างอาจลดทอนแรงจูงใจภายในได้
 - เป้าหมายสูงสุดขององค์กรได้รับการพิจารณา และประเมินความเหมาะสมของประเภทเป้าหมาย (ตัวอย่างเช่น เป้าหมายด้านผลการปฏิบัติงานหรือการเรียนรู้)
- องค์กรบูรณาการการเสริมแรงเชิงบวก และมาตรการแก้ไข เพื่อปลูกฝังพฤติกรรมเชิงรุกในองค์กรที่สอดคล้องกับวัตถุประสงค์ขององค์กรและข้อกำหนดทางกฎหมายต่างๆ วิธีการควบคุมที่สำคัญควรประกอบด้วย:



- การประเมินประสิทธิผลของโปรแกรมการสื่อสารและการฝึกอบรมเป็นประจำเพื่อให้มั่นใจว่าพนักงานเข้าใจถึงความสำคัญของการรายงานปัญหาและผลที่ตามมาของการไม่ปฏิบัติตาม และรู้สึกได้รับการสนับสนุนให้รายงานปัญหาต่างๆ
- ระบบการติดตามและรายงานผลที่ติดตามการปฏิบัติตามกฎระเบียบและระบุปัญหาการรายงานที่ต่ำกว่าความเป็นจริง
- มาตรการทางวินัยถูกนำมาใช้สม่ำเสมอและเป็นธรรม ไม่รุนแรงจนทำให้ไม่กล้ารายงานปัญหา และไม่ผ่อนปรนเกินไปจนไม่สามารถยับยั้งพฤติกรรมที่ผิดจรรยาบรรณได้
- กลไกการให้ข้อเสนอแนะที่อนุญาตให้พนักงานรายงานปัญหาโดยไม่เปิดเผยตัวตนจะได้รับการสอบถามอย่างสม่ำเสมอ เพื่อให้แน่ใจว่ากลไกดังกล่าวมีประสิทธิภาพและส่งเสริมการรายงานตามความเป็นจริง

E. กระบวนการบริหารจัดการประเด็นปัญหา ขององค์กรมีการระบุพฤติกรรมที่ไม่สอดคล้องกับวัตถุประสงค์และยกระดับการรายงานเมื่อจำเป็น เพื่อจัดทำแผนปฏิบัติการของผู้บริหาร (Management Action Plan) ในการลดความเสี่ยงจากผลลัพธ์ที่บกพร่อง ผู้ตรวจสอบภายในสามารถสอบถามวิธีการควบคุมที่สำคัญสำหรับการแทรกแซงเพื่อปรับเปลี่ยนพฤติกรรมที่มีประสิทธิผล เช่น:

- แนวทางที่อ้างอิงตามหลักฐาน (Evidence-based approaches): แผนปฏิบัติการต้องผนวกแนวทางที่มีหลักฐานมาใช้ในการเปลี่ยนพฤติกรรม โดยมีพื้นฐานมาจากหลักพฤติกรรมศาสตร์ แบบจำลองพฤติกรรมต่างๆ และการบริหารการเปลี่ยนแปลง ถ้าแนวทางดังกล่าวไม่ได้อ้างอิงแบบจำลองการเปลี่ยนแปลงพฤติกรรมใดโดยเฉพาะ แนวทางนั้นควรมีการรวมกลยุทธ์การแทรกแซงสำหรับ:
 - การสื่อสาร: การเพิ่มความตระหนักรู้ในหมู่พนักงานและผู้บริหารอย่างสม่ำเสมอเกี่ยวกับความจำเป็นในการเปลี่ยนแปลงพฤติกรรม รวมถึงการยอมรับและการสนับสนุนการเปลี่ยนแปลง
 - การฝึกอบรมและพัฒนาพนักงาน: การลงทุนในโปรแกรมฝึกอบรมที่ปรับให้เหมาะสมกับแต่ละบทบาท และการเสริมสร้างทักษะและพฤติกรรมที่จำเป็นให้แก่พนักงานผ่านการประชุมเชิงปฏิบัติการ การเรียนรู้ผ่านระบบออนไลน์ และโอกาสในการพัฒนาอย่างต่อเนื่อง ซึ่งรวมถึงการเรียนรู้และสามารถนำทักษะและพฤติกรรมใหม่ๆ ไปใช้ได้อย่างมีประสิทธิภาพ เพื่อให้บรรลุการเปลี่ยนแปลงที่องค์กรต้องการ



- การพัฒนาผู้บริหาร: ผู้จัดการทุกระดับคำนึงถึงวิธีการสนับสนุนและแสดงให้เห็นถึงการเปลี่ยนแปลงพฤติกรรมในสถานการณ์ประจำวัน ซึ่งอาจรวมถึงการที่ผู้บริหารปรับเปลี่ยนพฤติกรรมของตนเองเพื่อช่วยให้พนักงานรู้สึกสบายใจที่จะนำพฤติกรรมใหม่ไปปฏิบัติ การขอให้พนักงานนำพฤติกรรมใหม่ไปปฏิบัติโดยตรง รวมถึงการส่งเสริมการเรียนรู้และการขอให้ฝึกอบรมทักษะและพฤติกรรมต่างๆ ที่ยังคงจำเป็น โปรแกรมพัฒนาภาวะผู้นำและการเป็นพี่เลี้ยงสอนงาน (Coaching) สามารถพัฒนาทักษะและความมั่นใจได้
- การเสริมแรงอย่างสม่ำเสมอในสถานการณ์ประจำวัน (Consistence reinforcement): บุคลากรต้องการการสนับสนุน การให้กำลังใจ และการเตือนความจำอย่างสม่ำเสมอ เพื่อสร้างและบูรณาการกำกับพฤติกรรมใหม่ให้เป็นส่วนหนึ่งของการทำงานประจำวัน
- การเสริมแรงที่สอดคล้องกับพฤติกรรม (Congruent reinforcement): แผนการแทรกแซงควรได้รับการปรับให้สอดคล้องกันทั้งในแง่สารจากผู้นำ กระบวนการทำงาน ระบบงาน การเป็นพี่เลี้ยงสอนงาน และกลไกการให้ข้อมูลตอบกลับที่ไม่เป็นทางการ เพื่อเสริมสร้างการเปลี่ยนแปลงที่ต้องการ การปรับแนวทางให้สอดคล้องดังกล่าวช่วยจัดความไม่แน่นอนและความสับสน เพื่อให้มั่นใจได้ว่าพนักงานเข้าใจถึงการเปลี่ยนแปลงพฤติกรรมที่คาดหวัง วิธีการปรับใช้พฤติกรรมดังกล่าว และตระหนักถึงความสำคัญของการเปลี่ยนแปลงนั้น
- การมุ่งเป้าไปที่ปัจจัยขับเคลื่อนพฤติกรรม (Targeting the drivers): การเปลี่ยนแปลงพฤติกรรมอย่างยั่งยืนจำเป็นต้องจัดการกับปัจจัยขับเคลื่อนพื้นฐานของพฤติกรรม (Underlying drivers) (ดูข้อ C การบริหารความเสี่ยง) มากกว่าจัดการแค่ตัวพฤติกรรมนั้น
- การวัดผล (Measurement): การวัดความคืบหน้าและประสิทธิผลของการดำเนินการแทรกแซงช่วยให้ตัดสินใจว่าการแทรกแซงนั้นๆ บรรลุผลตามที่ต้องการหรือไม่ และจำเป็นต้องมีการปรับปรุงแก้ไขเพิ่มเติมหรือไม่ การรายงานความคืบหน้าอย่างสม่ำเสมอจะทำหน้าที่เป็นแรงเสริมทางบวกและทำให้ผู้มีส่วนได้เสียรับทราบความคืบหน้า แนวทางการวัดผลที่มีประสิทธิผลเป็นการผสมผสานวิธีเชิงคุณภาพและเชิงปริมาณ เช่น แบบสำรวจและการสัมภาษณ์ และให้ความเข้าใจในความคืบหน้าได้อย่างรอบด้าน

F. โปรแกรมการฝึกอบรม (Training programs) ที่เชื่อมโยงอย่างชัดเจนกับความคาดหวังด้านพฤติกรรมหรือระดับความเสี่ยงที่ยอมรับได้ที่กำหนดไว้ ตัวอย่างหัวข้อการฝึกอบรมได้แก่เรื่อง จริยธรรม การปฏิบัติตาม



กฎเกณฑ์ ภาวะผู้นำ การยอมรับความหลากหลาย ความตระหนักรู้ด้านความเสี่ยง และการตัดสินใจ ผู้ตรวจสอบภายในอาจสอบถามโปรแกรมการฝึกอบรมว่า:

- สะท้อนถึงความปลอดภัยและทัศนคติที่พึงประสงค์ และมีวัตถุประสงค์การเรียนรู้ที่เป็นลายลักษณ์อักษรอย่างชัดเจน
- อิงตามหลักฐานด้านพฤติกรรมหรือบทเรียนจากเหตุการณ์ในอดีต (ตัวอย่างเช่น ข้อตรวจพบจากการตรวจสอบ การวิเคราะห์สาเหตุที่แท้จริง และกลไกการรับฟังความคิดเห็น)
- จัดให้ทุกกลุ่มงานที่เกี่ยวข้อง โดยปรับเนื้อหาหลักสูตรให้เหมาะสมสำหรับผู้บริหารระดับสูง ผู้จัดการระดับปฏิบัติการ และพนักงานทั่วไป
- เป็นหลักสูตรภาคบังคับในส่วนที่เกี่ยวข้อง (ตัวอย่างเช่น กระบวนการที่มีความเสี่ยงสูง มีหน้าที่งานอยู่ภายใต้การกำกับดูแลของทางการ และบทบาทด้านการควบคุม)
- มีการปรับปรุงเนื้อหาเป็นประจำอย่างน้อยปีละครั้ง เพื่อให้มั่นใจว่ามีความเกี่ยวข้องและมีประสิทธิผล
- ออกแบบมาเพื่อ:
 - มีการนำสถานการณ์จริงหรือกรณีศึกษามาประกอบเพื่อทำให้ความคาดหวังด้านพฤติกรรมมีความชัดเจนและสามารถเข้าใจได้อย่างเป็นรูปธรรม
 - ใช้เทคนิคที่ให้ผู้เรียนได้มีส่วนร่วม (เช่น การเล่าเรื่อง และการตั้งคำถามเชิงสะท้อนความคิด)
 - ให้ผู้บริหารระดับสูงเข้ามามีส่วนร่วมอย่างจริงจัง เพื่อแสดงให้เห็นถึงแบบอย่างของผู้นำและส่งเสริมให้พนักงานปรับเปลี่ยนพฤติกรรม
- มีวิธีการควบคุมผลกระทบและการให้ความเชื่อมั่น ซึ่ง:
 - ติดตามความสำเร็จของการฝึกอบรมภาคบังคับและรายงานกรณีที่ไม่เป็นไปตามข้อกำหนด
 - วัดผลกระทบด้านพฤติกรรมและการคงอยู่ของผลที่เกิดขึ้น ผ่านการสำรวจที่ไม่เป็นทางการ การทดสอบแบบง่าย ๆ หรือการประเมินจากการสังเกต
 - รวบรวมมุมมองของผู้เข้าร่วมและประสิทธิผลของการฝึกอบรมผ่านกระบวนการให้ความคิดเห็นที่เป็นระบบ
 - ดำเนินการให้มั่นใจว่าเนื้อหาการฝึกอบรมสอดคล้องกับกรอบการบริหารความเสี่ยงและข้อกำหนดการควบคุม และมีกระบวนการสอบทานและการลงนามอย่างเป็นทางการ



G. กระบวนการจ้างงาน (Hiring processes) มีความสอดคล้องกับความคาดหวังด้านพฤติกรรมขององค์กร และผนวกความสามารถด้านพฤติกรรม (Behavioral competencies) ไว้ด้วย ผู้ตรวจสอบภายในอาจสอบถามคุณลักษณะของการควบคุม เช่น:

- เครื่องมือที่ช่วยประเมินความสอดคล้องของผู้สมัครกับค่านิยมขององค์กร ซึ่งรวมถึงแนวทางการสัมภาษณ์แบบมีโครงสร้าง และคำถามที่มีสถานการณ์จำลอง
- การสัมภาษณ์เชิงพฤติกรรมและความคิดเห็นจากเพื่อนร่วมงาน เพื่อประเมินลักษณะนิสัย เช่น ความเห็นอกเห็นใจผู้อื่น การใช้ดุลยพินิจด้านจริยธรรม และความรับผิดชอบ
- โฆษณาการรับสมัครงานและภาพลักษณ์ของนายจ้างสะท้อนถึงความมุ่งมั่นด้านวัฒนธรรมขององค์กร เพื่อดึงดูดผู้สมัครที่มีวัฒนธรรมสอดคล้องกัน
- มีกลไกการรับฟังความคิดเห็นช่วยให้สามารถประเมินการปรับตัวเข้ากับวัฒนธรรมองค์กรของพนักงานใหม่ เพื่อให้สามารถจัดการกับความไม่สอดคล้องได้ตั้งแต่นั้นๆ
- เอกสาร (ตัวอย่างเช่น กรอบการให้คะแนน และบันทึกการสัมภาษณ์) ที่แสดงให้เห็นว่ามีการใช้เกณฑ์การตัดสินใจในการจ้างงานที่เสมอต้นเสมอปลาย
- ฝ่ายทรัพยากรบุคคลและผู้บริหารระดับสูงมีการสอบทานรูปแบบการจ้างงานเพื่อหาความเสี่ยงต่างๆ เช่น การเลือกที่รักมักที่ชัง อคติ หรือความล้มเหลวในการปฏิบัติตามมาตรฐานด้านพฤติกรรม
- นโยบายการจ้างงานและการเลื่อนตำแหน่งได้รับการทบทวนเป็นประจำ เพื่อให้สอดคล้องกับค่านิยมขององค์กร และความมีประสิทธิภาพในการนำไปปฏิบัติจริง



ภาคผนวก A. ตัวอย่างการประยุกต์ใช้ในทางปฏิบัติ

ตัวอย่างต่อไปนี้อธิบายสถานการณ์ที่ข้อกำหนดเฉพาะเรื่องพฤติกรรมองค์กรจะสามารถนำไปใช้ได้

ตัวอย่างที่ 1: การสอบทานกรอบด้านพฤติกรรมขององค์กรแบบที่เป็นเอกเทศ (Standalone review)

หน่วยงานตรวจสอบภายในได้ริเริ่มการสอบทานกรอบการปฏิบัติงานในภาพรวมขององค์กรแบบที่เป็นเอกเทศ เพื่อประเมินการออกแบบและประสิทธิผลของการปฏิบัติงานในการจัดการความเสี่ยงด้านพฤติกรรม โดยขอบเขตของงานตรวจสอบที่ได้รับมอบหมายนี้ครอบคลุมถึงโครงสร้างการกำกับดูแล กิจกรรมด้านการบริหาร ความเสี่ยง และวิธีการควบคุมด้านพฤติกรรมที่เป็นรากฐานของการสร้างความสอดคล้องกันทั่วทั้งองค์กร

ผู้ตรวจสอบภายในได้ประเมินว่าหน้าที่ในการควบคุมดูแลด้านพฤติกรรมนั้นมีการกำหนดไว้อย่างชัดเจนและปราศจากความขัดแย้งทางผลประโยชน์หรือไม่ ทีมตรวจสอบได้ทบทวนขอบเขตอำนาจหน้าที่ของ คณะกรรมการ และสอบย้อนแล้วว่าคณะกรรมการได้รับรายงานเกี่ยวกับตัวชี้วัดความเสี่ยงด้านพฤติกรรมอย่างสม่ำเสมอ เช่น ผลการสำรวจ และแนวโน้มของการแสดงความคิดเห็น การสอบทานยังรวมถึงการประเมินว่า นโยบายที่เกี่ยวข้องกับวัฒนธรรมองค์กร เช่น การกำกับดูแลการแจ้งเบาะแส และความประพฤติที่มีจริยธรรม ได้รับการปรับปรุงให้เป็นปัจจุบันและมีการบังคับใช้เป็นประจำหรือไม่

ผู้ตรวจสอบภายในยังได้ประเมินองค์ประกอบของการบริหารความเสี่ยง โดยเริ่มจากกรอบการบริหาร ความเสี่ยงด้านพฤติกรรมที่ดูแลโดยหน่วยงานในแนวป้องกันด้านที่สอง (Second Line) ซึ่งมุ่งเน้นว่ากรอบการทำงานดังกล่าวสามารถระบุปัจจัยขับเคลื่อนความเสี่ยงด้านพฤติกรรมที่สำคัญได้หรือไม่ (เช่น ความปลอดภัยทางจิตใจในระดับต่ำ หรือเป้าหมายการดำเนินงานที่ไม่สอดคล้องกับความเป็นจริง) การประเมินให้ ความสำคัญกับวิธีการที่องค์กรใช้ติดตามและจัดการกับความแตกต่างระหว่างพฤติกรรมที่คาดหวังกับ พฤติกรรมที่ได้สังเกตเห็น ซึ่งรวมถึงว่าพฤติกรรมที่ผิดปกตินั้นได้รับการยกระดับการรายงาน และได้รับการ แก้ไขอย่างเป็นระบบหรือไม่



มีการตรวจสอบ (examined) สภาพแวดล้อมการควบคุมเพื่อตัดสินใจว่ากระบวนการที่เป็นทางการเหล่านั้น สนับสนุนความคาดหวังด้านพฤติกรรมหรือไม่ ผู้ตรวจสอบได้ประเมินระเบียบปฏิบัติในการสรรหาบุคลากรว่า ได้รวมการประเมินบนพื้นฐานของค่านิยมองค์กรหรือไม่ เนื้อหาการปฐมนิเทศพนักงานใหม่สอดคล้องกับ บรรทัดฐานทางวัฒนธรรมขององค์กรหรือไม่ และขอบเขตที่สิ่งจูงใจ (ทั้งที่เป็นตัวเงินและไม่ใช้ตัวเงิน) ได้รับการ สอบทานเพื่อดูว่าส่งผลกระทบที่ไม่พึงประสงค์หรือไม่ นอกจากนี้ ยังมีการทดสอบโปรแกรมการฝึกอบรม ช่อง ทางการแสดงความคิดเห็น การสื่อสารจากผู้นำ และการใช้วิธีการวิเคราะห์ข้อมูล (Data analytics) เพื่อ ตรวจสอบข้อกังวลด้านพฤติกรรมด้วย

งานตรวจสอบนี้ช่วยให้เข้าใจภาพรวมเกี่ยวกับการจัดการความเสี่ยงด้านพฤติกรรมในระดับองค์กร และเป็น พื้นฐานสำหรับการเสนอแนะแนวทางในการปรับปรุงโครงสร้างพื้นฐานด้านพฤติกรรมขององค์กรต่อไป

ตัวอย่างที่ 2: การสอบทานเฉพาะเรื่องวิธีปฏิบัติในการให้สิ่งจูงใจ

งานตรวจสอบที่ได้รับมอบหมายนี้มุ่งเน้นการประเมินว่ากรอบการให้สิ่งจูงใจ (Incentive Frameworks) มี อิทธิพลต่อพฤติกรรมอย่างไร และสอดคล้องกับจุดมุ่งหมาย ค่านิยมขององค์กร และความคาดหวังของทางการ หรือไม่ หน่วยงานตรวจสอบภายในเลือกหัวข้อนี้เนื่องจากมีความกังวลเพิ่มขึ้นเกี่ยวกับความเสี่ยงด้านการ ประพฤติมิชอบ และมีหลักฐานใหม่ๆ เกี่ยวกับพฤติกรรมที่เกิดจากแรงกดดันในหน่วยธุรกิจต่าง ๆ

การสอบทานเริ่มต้นด้วยการประเมินการจัดวางกลไกการกำกับดูแลสำหรับการออกแบบและอนุมัติโครงสร้าง สิ่งจูงใจ หน่วยงานตรวจสอบประเมินว่าหน่วยงานที่มีหน้าที่ในการนำมติด้านการกำกับดูแลไปปฏิบัติ เช่น ฝ่าย ทรัพยากรบุคคล หรือคณะกรรมการค่าตอบแทนมีการควบคุมดูแลการออกแบบระบบสิ่งจูงใจอย่างเป็น ทางการหรือไม่ และงานดังกล่าวได้รับการสอบทานอย่างเป็นอิสระจากหน่วยงานบริหารความเสี่ยง หน่วยงาน กำกับดูแลการปฏิบัติตามกฎเกณฑ์ หรือหน่วยงานตรวจสอบภายในหรือไม่

มีการนำมุมมองด้านการบริหารความเสี่ยงมาใช้เพื่อทำความเข้าใจว่าการพัฒนาโครงสร้างสิ่งจูงใจได้พิจารณา ถึงผลกระทบด้านพฤติกรรมหรือไม่ ผู้ตรวจสอบได้พิจารณาว่าองค์กรมีการทดสอบสถานการณ์จำลอง หรือ วิเคราะห์ความเสี่ยงด้านพฤติกรรมที่เกี่ยวข้องกับโครงสร้างการให้รางวัลหรือไม่ รวมถึงสอบทานว่าองค์กรมีการ ติดตามและนำตัวชี้วัดผลการปฏิบัติงานหลัก ด้านพฤติกรรม เช่น คะแนนการให้ความร่วมมือ มาใช้ในการ ประเมินผลลัพธ์หรือไม่



การทดสอบการควบคุมครอบคลุมกลไกต่างๆ ที่ออกแบบมาเพื่อกำหนดทิศทางพฤติกรรมที่เกี่ยวข้องกับการให้รางวัล ซึ่งรวมถึงการใช้ Balanced scorecards ที่มีเกณฑ์วัดซึ่งวัดทั้งผลสำเร็จและวิธีการบรรลุผลสำเร็จ การใช้มาตรการลดหรือระดับค่าตอบแทน และ/หรือการเรียกคืนเงินรางวัล และการมีอยู่ของกระบวนการให้ความคิดเห็นแบบ 360 องศา ผู้ตรวจสอบยังได้สอบถามการฝึกอบรมที่จัดให้แก่ผู้จัดการระดับปฏิบัติการเกี่ยวกับการให้ความคิดเห็นด้านพฤติกรรม และสำรวจโปรแกรมการให้รางวัลที่ไม่ใช่ตัวเงินซึ่งให้รางวัลแก่พฤติกรรมที่ยึดมั่นในคุณค่า

ตลอดช่วงที่ปฏิบัติงานตรวจสอบนี้ ผู้ตรวจสอบภายในพยายามระบุว่าวิธีปฏิบัติในการให้สิ่งจูงใจอาจส่งผลให้เกิดพฤติกรรมที่ไม่พึงประสงค์โดยไม่ตั้งใจได้หรือไม่ เช่น การรับความเสี่ยงมากเกินไป การใช้หนทางลัด หรือการลงโทษที่เข้มงวดเกินไปให้ผู้บริหารที่สูงขึ้นไปทราบ มีการให้ข้อเสนอแนะเพื่อปรับปรุงความโปร่งใส นูรณาการเป้าหมายที่สอดคล้องกับค่านิยมให้มีความสม่ำเสมอยิ่งขึ้น และเสริมสร้างการสอบทานอิสระของผู้บริหารในหน่วยงานแนวป้องกันด้านที่สอง ในระหว่างกระบวนการออกแบบการให้รางวัล

ตัวอย่างที่ 3: การบูรณาการเข้ากับการตรวจสอบแบบดั้งเดิม – การบริหารความเสี่ยงด้านไซเบอร์

ในตัวอย่างนี้ หน่วยงานตรวจสอบภายในได้บูรณาการความเสี่ยงด้านพฤติกรรมเข้ากับการตรวจสอบแบบดั้งเดิมเพื่อประเมินการบริหารความเสี่ยงด้านไซเบอร์ โดยตระหนักว่ามีความล้มเหลวด้านไซเบอร์จำนวนมากที่ไม่ได้เกิดจากปัญหาทางเทคนิคเท่านั้น แต่ยังเกิดจากพฤติกรรมของมนุษย์ด้วย ผู้ตรวจสอบได้รวมการสอบทานเกี่ยวกับพฤติกรรมไว้ตลอดระยะเวลาของการตรวจสอบ

การตรวจสอบเริ่มต้นด้วยการประเมินระดับการตระหนักถึงความเสี่ยงด้านพฤติกรรมที่มีอยู่ในการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ ผู้ตรวจสอบได้สอบถามการควบคุมดูแลกลยุทธ์ด้านไซเบอร์ของคณะกรรมการและผู้บริหารระดับสูง โดยมองหาหลักฐานว่าองค์กรเหล่านั้นกำลังติดตามและหาหรือเกี่ยวกับความสอดคล้องของพฤติกรรม เช่น การปฏิบัติตามวิธีปฏิบัติที่ปลอดภัย หรือการเป็นแบบอย่างที่ดีของผู้นำในพฤติกรรมที่ปลอดภัยและการปฏิบัติตามวัตถุประสงค์ขององค์กร

ในแง่ของการบริหารความเสี่ยง ทีมตรวจสอบได้ประเมินว่าการประเมินความเสี่ยงด้านไซเบอร์ขององค์กรได้คำนึงถึงปัจจัยด้านมนุษย์หรือไม่ ซึ่งรวมถึงการประเมินว่ามีการใช้ข้อมูลด้านพฤติกรรม (เช่น ความถี่ของการทดสอบการหลอกลวงทางอีเมล (phishing) ที่ล้มเหลว การฝ่าฝืนการเข้าถึงระบบ หรืออัตราการผ่านการ



ฝึกอบรมที่ต่ำ) เพื่อติดตามและยกระดับการรายงานความเสี่ยงหรือไม่ งานตรวจสอบนี้ยังรวมถึงการหาสาเหตุที่แท้จริงของเหตุการณ์ด้านความปลอดภัยที่เกิดขึ้นก่อนหน้านี้ เพื่อระบุปัจจัยขับเคลื่อนพฤติกรรมที่อาจเกิดขึ้น เช่น ความรับผิดชอบไม่ชัดเจน หรือท่าทีของผู้บริหาร (management tone)

การทดสอบการควบคุมได้มุ่งเน้นไปที่การออกแบบด้านพฤติกรรมและการปฏิบัติงานที่ปลอดภัย ผู้ตรวจสอบสอบถามเกี่ยวกับการคัดกรองพฤติกรรมอยู่ในกระบวนการจ้างงานสำหรับตำแหน่งงานที่มีสิทธิเข้าถึงเป็นพิเศษหรือไม่ โครงสร้างสิ่งจูงใจได้รับการประเมิน เพื่อดูว่าสิ่งจูงใจเหล่านั้นส่งเสริมวิธีปฏิบัติในการใช้งานออนไลน์ที่มีความปลอดภัยหรือไม่ หรือให้ความสำคัญกับพฤติกรรมเสี่ยงมากกว่าความปลอดภัยโดยไม่ได้ตั้งใจ รวมถึงมีการประเมินการฝึกอบรมด้านความปลอดภัยทางไซเบอร์เพื่อตัดสินว่าการอบรมนั้นมีความน่าสนใจ ได้รับการปรับปรุงเป็นประจำ และมีการจำลองสถานการณ์เพื่อทดสอบพฤติกรรมที่ตอบสนองต่อการหลอกลวงทางอีเมล และการใช้การใช้อิทธิพลหลอกลวงผู้คนหรือไม่

สุดท้ายแล้ว งานตรวจสอบนี้ได้ดูว่าผู้บริหารเสริมสร้างพฤติกรรมด้านความปลอดภัยผ่านการสื่อสารอย่างไร และพนักงานรู้สึกสบายใจที่จะรายงานพฤติกรรมทางไซเบอร์ที่ไม่ปลอดภัยหรือไม่ วัฒนธรรมองค์กรที่ส่งเสริมให้พนักงานกล้าแสดงความคิดเห็นถือเป็นปัจจัยสำคัญที่ช่วยเสริมสร้างความสามารถในการรับมือและการฟื้นตัวขององค์กร (resilience)

การนำแง่มุมด้านพฤติกรรมมาพิจารณาในการตรวจสอบด้านไซเบอร์ครั้งนี้ นำไปสู่การได้ข้อมูลเชิงลึกที่ลึกซึ้งยิ่งขึ้นและข้อเสนอแนะที่เป็นประโยชน์ ซึ่งช่วยเสริมสร้างขีดความสามารถขององค์กรในการจัดการความเสี่ยงอย่างหนึ่งในด้านที่มีความสำคัญที่สุดขององค์กร



ภาคผนวก B. กรณีศึกษาของการตรวจสอบเฉพาะด้าน (Appendix B. Case Studies of Specific Audits)

กรณีศึกษาที่ 1: กรมการเคหะ (หน่วยงานภาครัฐ)

ตัวอย่างในกรณีศึกษานี้แสดงให้เห็นว่าหน่วยงานตรวจสอบภายในของหน่วยงานภาครัฐ จะสามารถนำข้อกำหนดเฉพาะ เรื่องพฤติกรรมองค์กรมาใช้เพื่อประเมินว่าหน่วยงานบรรลุวัตถุประสงค์ในการให้บริการด้านที่อยู่อาศัยแก่ประชาชนอย่างเท่าเทียมได้อย่างไร ผู้ตรวจสอบภายในควรตระหนักว่าลำดับความสำคัญของเจ้าหน้าที่รัฐ ความอ่อนไหวทางการเมือง การจัดสรร งบประมาณ และการตัดสินใจเชิงนโยบายบางประการนั้นอยู่นอกขอบเขตการตรวจสอบ อย่างไรก็ตาม สิ่งที่อยู่ในขอบเขตอย่างชัดเจนคือ วิธีที่เจ้าหน้าที่ระดับสูงและผู้จัดการนำนโยบายเหล่านี้ไปตีความและปรับใช้ได้เป็นอย่างดีกับวัฒนธรรมภายในของหน่วยงาน

การกำกับดูแล (Governance)

- A. บทบาทและภาระหน้าที่ (Roles and responsibilities): หน่วยงานมีโครงสร้างองค์กรที่ชัดเจน โดยมีการ แยกหน้าที่ระหว่างการออกแบบนโยบาย (เจ้าหน้าที่ระดับสูง) ออกจากการส่งมอบที่อยู่อาศัย ส่วนหนึ่งของวัตถุประสงค์ในการตรวจสอบคือ เพื่อตัดสินใจว่าการหลีกเลี่ยงความขัดแย้งทางผลประโยชน์เชิงโครงสร้างหรือไม่ เช่น หน้าที่ในการปฏิบัติตามนโยบายแยกออกจากหน้าที่การควบคุมดูแลผู้รับเหมาหรือไม่
- B. ความรับผิดชอบ (Accountability): หัวหน้าส่วนงานและผู้บริหารระดับสูงได้รับมอบหมายหน้าที่ในการเชื่อมโยงวัตถุประสงค์ขององค์กรกับผลลัพธ์ที่เกี่ยวข้องกับวัฒนธรรม เช่น ความเป็นธรรมในการจัดสรรที่อยู่อาศัยและความเป็นอยู่ที่ดีของพนักงาน หน่วยงานตรวจสอบภายในจะประเมินว่าความรับผิดชอบนั้นเป็นที่รับรู้และได้รับการยอมรับหรือไม่
- C. การควบคุมดูแลและการติดตามผล (Oversight and monitoring): มีการจัดตั้ง "คณะกรรมการดูแลด้านวัฒนธรรม" ซึ่ง ประธานคือผู้บริหารระดับสูง เพื่อทบทวนผลสำรวจพนักงาน ข้อมูลการแจ้ง



เบาะแส และข้อร้องเรียนของผู้มีส่วนได้เสียเป็นรายไตรมาส ผู้ตรวจสอบจะประเมินว่ากระบวนการเหล่านี้สามารถส่งสัญญาณเตือนภัย เกี่ยวกับพฤติกรรมที่ไม่สอดคล้องได้หรือไม่

- D. นโยบายและวิธีการปฏิบัติงาน (Policies and procedures): มีประมวลความประพฤติ แนวทางการจัดสรรที่อยู่อาศัย และมีทะเบียนความขัดแย้งทางผลประโยชน์ที่ได้รับการทบทวนเป็นระยะ (เช่น อย่างน้อยทุก 2 ปี) หน่วยงานตรวจสอบภายในประเมินว่า การปรับปรุงได้สะท้อนบทเรียนที่ได้รับจากกรณีข้อผิดพลาดเกี่ยวกับการเคหะในอดีตหรือรายงานการตรวจสอบภาครัฐหรือไม่

การบริหารความเสี่ยง (Risk Management)

- A. กรอบการบริหารความเสี่ยงด้านพฤติกรรม (Behavioral risk framework): หน่วยงานระบุความเสี่ยงด้านวัฒนธรรมที่อาจส่งผลกระทบต่อการส่งมอบบริการสาธารณะ เช่น การเลือกที่รักมักที่ชังในการจัดสรรที่อยู่อาศัย ระบบราชการที่เย็นเยือกเกินจำเป็น หรือพนักงานลังเลที่จะโต้แย้งหรือคัดค้านคำสั่งที่เป็นทางการ หน่วยงานตรวจสอบภายในต้องทำให้มั่นใจได้ว่าความเสี่ยงเหล่านี้ถูกบันทึกไว้ในทะเบียนความเสี่ยง (Risk Register) ที่เป็นทางการ และได้รับการพิจารณาจากฝ่ายบริหารและมีการดำเนินการตอบสนองเมื่อจำเป็น
- B. ตัวชี้วัดและการวิเคราะห์ (Indicators and analytics): มีการใช้แดชบอร์ดติดตามข้อมูลด้านพฤติกรรม เช่น อัตราการหมุนเวียนของพนักงาน ข้อร้องเรียน จำนวนการร้องเรียนอย่างไม่เป็นทางการจากผู้เช่าและประชาชน และความรวดเร็วในการตอบสนองต่อคำขอข้อมูล สาธารณะหรือเสรีภาพในการขอข้อมูลข่าวสาร ผู้ตรวจสอบจะประเมินว่าตัวชี้วัดและการวิเคราะห์ข้อมูลดังกล่าวมีความน่าเชื่อถือ และได้รับการนำไปหารือกันภายในหน่วยงานหรือไม่
- C. การจัดการความเบี่ยงเบน (Variance management): เมื่อเกิดความแตกต่างขึ้น (เช่น กรณีแจ้งเบาะแสที่ชี้ให้เห็นถึงการเบี่ยงเบนจากไปหลักความเป็นธรรม) เรื่องดังกล่าวจะถูกยกระดับส่งต่อไปยังผู้บริหารระดับสูง ผู้ตรวจสอบจะสอบย้อนว่าการวิเคราะห์ความเบี่ยงเบนดังกล่าวนำไปสู่การดำเนินการแก้ไข (Corrective Action) หรือไม่
- D. การรับฟังข้อมูลจากผู้มีส่วนได้เสียในการแก้ไขปัญหา มีการปรึกษาหารือกับหน่วยงานที่มีอำนาจตามกฎหมาย สมาคมการเคหะ สหภาพแรงงาน และคณะกรรมการภาคประชาชน เมื่อพบประเด็นด้านวัฒนธรรม (เช่น พฤติกรรมที่ไม่สุภาพของเจ้าหน้าที่ให้บริการ หรือความลำเอียงในการจัดสรร) ผู้ตรวจสอบจะสอบย้อนว่าข้อเสนอแนะจากการปรึกษาหารือนั้นส่งผลต่อแผนการแก้ไขปัญหาหรือไม่



การควบคุม (Controls)

- A. การสอบทานความเสี่ยงด้านพฤติกรรม (Behavioral risk reviews): มีการสอบทานย้อนหลัง หลังจากเกิดความล้มเหลวของโครงการด้านที่อยู่อาศัย (เช่น ความล่าช้าในการก่อสร้างที่อยู่อาศัยเพื่อสังคม) ผู้ตรวจสอบจะสอบทานว่ามีการประเมินหาสาเหตุที่แท้จริงด้านพฤติกรรมหรือไม่ (เช่น การไม่ให้ความร่วมมือกัน หรือวัฒนธรรมการกล่าวโทษกัน)
- B. การกำหนดทิศทาง (Tone setting): ผู้บริหารระดับสูงสื่อสารความคาดหวังเกี่ยวกับความเป็นธรรมาภิบาล และคุณภาพการให้บริการผ่านการประชุมพนักงานทั้งองค์กร และวิดีโอบนอินเทอร์เน็ต ผู้ตรวจสอบภายในจะสอบทานว่าพนักงานมีการรับรู้และนำความคาดหวังดังกล่าวไปปฏิบัติจริงหรือไม่
- C. กลไกการยกระดับการรายงาน (Escalation mechanisms): หน่วยงานมีสายด่วนแจ้งเบาะแส ที่ประชาชนเข้าถึงได้ และกระบวนการรับเรื่องร้องเรียนสำหรับผู้เช่าพนักงาน และประชาชนทั่วไป ผู้ตรวจสอบจะตรวจสอบความเหมาะสมของเวลาในการดำเนินการ การรักษาความลับ และหลักฐานที่แสดงว่าไม่มีการตอบโต้หรือกลั่นแกล้งผู้รายงาน
- D. สิ่งจูงใจ (Incentives): การประเมินผลการปฏิบัติงานให้ความสำคัญกับเรื่องความร่วมมือของพนักงาน การมีส่วนร่วมของผู้มีส่วนได้เสีย และความเป็นธรรมในการมีปฏิสัมพันธ์กับผู้เช่า ผู้ตรวจสอบจะประเมินว่า การเลื่อนตำแหน่งหรือการให้รางวัลได้ช่วยส่งเสริมพฤติกรรมเหล่านี้จริงหรือไม่
- E. การติดตามพฤติกรรม (Monitoring of behavior): ผู้จัดการสายงานประเมินพนักงานตามมาตรฐานด้านพฤติกรรม (ความซื่อสัตย์ ความเห็นอกเห็นใจต่อผู้เช่าที่เปราะบาง) ระหว่างการทบทวนประจำปี ผู้ตรวจสอบจะตัดสินว่าผลการประเมินมีความสม่าเสมอและมีการจัดการกับรูปแบบพฤติกรรมที่ไม่เหมาะสมหรือไม่
- F. การฝึกอบรม (Training): มีหลักสูตรภาคบังคับที่ครอบคลุมเรื่องอคติโดยไม่รู้ตัว (Unconscious Bias) การจัดการความขัดแย้ง และการตัดสินใจเชิงจริยธรรมในการจัดสรรที่อยู่อาศัย ผู้ตรวจสอบจะสอบทานว่าอัตราการผ่านการฝึกอบรมอยู่ในระดับสูงหรือไม่ และประเมินผลจากแบบสำรวจภายหลังการอบรมด้วย
- G. กระบวนการปรับปรุงแก้ไข (Remediation processes): เมื่อพบการฝ่าฝืนด้านวัฒนธรรม (เช่น การบิดเบือนหรือแทรกแซงรายชื่อผู้รอคิวการจัดสรรที่อยู่อาศัย) จะต้องมีการวิเคราะห์สาเหตุที่แท้จริงและ



ติดตามแผนการดำเนินการแก้ไข ผู้ตรวจสอบสอบทานว่ามาตรการแก้ไขนั้นมีประสิทธิผลและยั่งยืนหรือไม่

ข้อมูลเชิงลึกที่สำคัญ (Key Insight)

แม้ว่าทิศทางจากเจ้าหน้าที่รัฐและการกำหนดนโยบายในระดับสูงจะอยู่นอกเหนือขอบเขตและการควบคุมของหน่วยงานตรวจสอบภายใน แต่โครงสร้างด้านการกำกับดูแล การบริหารความเสี่ยง และการควบคุมที่เกี่ยวข้องกับพฤติกรรมของหน่วยงานนั้นสามารถตรวจสอบได้ (Auditable) การประยุกต์ใช้ข้อกำหนดทั้ง 15 ข้อในข้อกำหนดเฉพาะเรื่องพฤติกรรมองค์กรจะช่วยให้มั่นใจได้ว่า ผู้ตรวจสอบภายในสามารถประเมินว่าพฤติกรรมองค์กรกำลังส่งผลกระทบต่อวิธีการส่งมอบบริการอย่างไร เช่น การให้บริการอย่างเป็นธรรม โปร่งใส และสอดคล้องกับค่านิยม แม้จะอยู่ภายใต้บริบททางการเมืองก็ตาม

กรณีศึกษาที่ 2: บริษัทก่อสร้างขนาดเล็ก (หน่วยงานตรวจสอบภายในขนาดเล็ก)

หน่วยงานตรวจสอบภายในของบริษัทก่อสร้างสมมติแห่งหนึ่งมีพนักงาน 50 คน กำลังเผชิญกับข้อกังวลว่าข้อกำหนดเฉพาะเรื่องพฤติกรรมองค์กรได้ถูกออกแบบมาสำหรับองค์กรขนาดใหญ่และซับซ้อนเท่านั้น อย่างไรก็ตาม หลักการเดียวกันนี้สามารถนำมาประยุกต์ใช้ได้โดยการปรับให้เหมาะสมกับขนาด แม้จะไม่มีคณะกรรมการชุดย่อยของคณะกรรมการ หรือแดชบอร์ดที่ซับซ้อน บริษัทก็สามารถแสดงให้เห็นถึงความสอดคล้องกับข้อกำหนดทั้ง 15 ข้อภายใต้ข้อกำหนดเฉพาะดังกล่าวได้

การกำกับดูแล (Governance)

- A. บทบาทและหน้าที่ (Roles and responsibilities): ผู้บริหารระดับสูงของบริษัทมอบหมายหน้าที่ด้านทรัพยากรบุคคลให้แก่ผู้จัดการสำนักงาน และมอบหมายการควบคุมดูแลโครงการให้ผู้จัดการสำนักงานอย่างเป็นทางการ ผู้ตรวจสอบภายในจะประเมินว่าบทบาทเหล่านี้มีความชัดเจนและหลีกเลี่ยงความขัดแย้งในหน้าที่หรือไม่ (ตัวอย่างเช่น การที่บุคคลเดียวทำหน้าที่ทั้งอนุมัติและติดตามค่าใช้จ่ายของผู้รับเหมา)



- B. ความรับผิดชอบ (Accountability): ผู้จัดการแต่ละคนต้องลงนามรับรองรายงานรายไตรมาสเพื่อยืนยันหน้าที่ที่มีต่อพฤติกรรมของทีม รวมถึงการปฏิบัติตามกฎความปลอดภัยและการปฏิบัติต่อผู้รับเหมาช่วง ผู้ตรวจสอบประเมินว่าการรับรองเหล่านี้มีความสมเหตุสมผลและมีการติดตามผลหรือไม่
- C. การควบคุมดูแลและการติดตามผล (Oversight and monitoring): ฝ่ายบริหารประชุมรายเดือนเพื่อทบทวนอัตราการหมุนเวียนของพนักงาน ข้อร้องเรียนของลูกค้า และรายงานด้านความปลอดภัยของโครงการ ผู้ตรวจสอบจะสอบย้อนว่าประเด็นที่เกี่ยวข้องกับวัฒนธรรมได้รับการยกขึ้นมาหารือและติดตามอย่างต่อเนื่องหรือไม่
- D. นโยบายและวิธีการปฏิบัติงาน (Policies and procedures): ผู้ตรวจสอบสอบย้อนว่าประมวลความประพฤติ ระเบียบวิธีการด้านความปลอดภัย และแนวทางป้องกันการกลั่นแกล้ง (Anti-bullying) ที่เป็นลายลักษณ์อักษร ได้รับการทบทวนเป็นประจำทุกปีและสื่อสารให้พนักงานทราบ

การบริหารความเสี่ยง (Risk Management)

- A. กรอบการบริหารความเสี่ยงด้านพฤติกรรม (Behavioral risk framework): บริษัทระบุความเสี่ยง เช่น การเร่งรีบหรือการหลีกเลี่ยงวิธีการปฏิบัติงานตามขั้นตอนความปลอดภัยอย่างครบถ้วนเพื่อให้ทันกำหนดเวลา การเลือกปฏิบัติในการจัดสรรการทำงานล่วงเวลา และการคุกคามในสถานที่ก่อสร้าง ผู้ตรวจสอบสอบย้อนว่าความเสี่ยงเหล่านี้ถูกระบุไว้ในทะเบียนความเสี่ยงด้วย
- B. ตัวชี้วัดและการวิเคราะห์ (Indicators and analytics): แทนที่จะใช้แคชบอร์ด บริษัทใช้สเปรดชีต (Spreadsheets) แบบง่าย เพื่อติดตามการขาดงาน การร้องเรียน และเหตุการณ์ด้านความปลอดภัย ผู้ตรวจสอบจะประเมินว่าข้อมูลเหล่านี้ชี้ให้เห็นประเด็นหรือพื้นที่ที่ควรได้รับการสอบสวนหรือไม่
- C. การจัดการความเบี่ยงเบน (Variance management): หากผลสำรวจพนักงานแสดงให้เห็นถึงช่องว่างระหว่าง "ความคาดหวังที่คาดหวัง" กับ "ประสบการณ์ที่เกิดขึ้นจริง" ผู้จัดการต้องนำเสนอแนวทางแก้ไขในการประชุมครั้งถัดไป ผู้ตรวจสอบจะตัดสินว่ามีการดำเนินการแก้ไขประเด็นเหล่านั้นและแล้วเสร็จหรือไม่
- D. การรับฟังข้อมูลจากผู้มีส่วนได้เสียในการแก้ไขปัญหา (Stakeholder input): เมื่อเกิดปัญหาด้านวัฒนธรรม บริษัทจะเชิญหน่วยงานที่มีอำนาจตามกฎหมาย ตัวแทนพนักงาน หรือในบางกรณีเชิญลูกค้ารายสำคัญมาให้ความเห็นเมื่อเกิดปัญหาด้านวัฒนธรรม ผู้ตรวจสอบจะตัดสินว่าการตอบสนองหรือแก้ไขสะท้อนถึงข้อเสนอแนะที่ได้รับหรือไม่



การควบคุม (Controls)

- A. การสอบทานความเสี่ยงด้านพฤติกรรม (Behavioral risk reviews): ภายหลังความล้มเหลวของโครงการใดๆ (เช่น ต้นทุนบานปลายเนื่องจากการขาดความร่วมมือ) ผู้บริหารระดับสูงจะจัดประชุม "ถอดบทเรียน" (Lessons Learned) ผู้ตรวจสอบสอบยืนยันว่าสาเหตุด้านวัฒนธรรม (การกล่าวโทษกัน การสื่อสารที่แย่) ได้ถูกบันทึกไว้หรือไม่ และมีการนำวิธีการควบคุมมาใช้เพื่อแก้ไขการกระทำนั้นๆ ในอนาคตหรือไม่
- B. การกำหนดทิศทาง (Tone setting): ผู้บริหารระดับสูงจัดประชุมชี้แจงพนักงานเป็นรายไตรมาสเพื่อเน้นย้ำค่านิยมเรื่องความเป็นธรรม คุณภาพ และความเคารพ ผู้ตรวจสอบภายในรวบรวมความคิดเห็นจากพนักงานเพื่อทดสอบว่าการสื่อสารดังกล่าวเข้าถึงพนักงานจริงหรือไม่
- C. กลไกการยกระดับการรายงานตามลำดับขั้น (Escalation mechanisms): แม้ไม่มีสายด่วนที่เป็นทางการแต่มี กล่องรับความคิดเห็นที่ลือลือคฤญแจไว้ และการเปิดให้เข้าพบผู้บริหารระดับสูงได้โดยตรง เพื่อใช้เป็นช่องทางการรายงาน ผู้ตรวจสอบจะตรวจสอบยืนยันว่าพนักงานมีการใช้ช่องทางการดังกล่าวหรือไม่ และมีนโยบายป้องกันการตอบโต้ผู้แจ้งเบาะแสหรือไม่
- D. สิ่งจูงใจ (Incentives): การจ่ายโบนัสมีจำนวนไม่มากแต่เชื่อมโยงกับการทำงานเป็นทีมและความคิดเห็นจากลูกค้า ไม่ใช่แค่การทำงานให้ทันกำหนดเวลาเท่านั้น ผู้ตรวจสอบสอบถามว่าการจัดสรรรางวัลมีความสม่ำเสมอและสมเหตุสมผลหรือไม่
- E. การติดตามพฤติกรรม (Monitoring of behavior): หัวหน้างานให้ข้อคิดเห็นอย่างไม่เป็นทางการเกี่ยวกับพฤติกรรมของพนักงานระหว่างการหารือเรื่องผลการปฏิบัติงาน ผู้ตรวจสอบประเมินว่าการให้ข้อคิดเห็นดังกล่าวถูกนำไปประยุกต์ใช้อย่างสม่ำเสมอทั่วทุกทีมหรือไม่
- F. การฝึกอบรม (Training): มีการจัดเวิร์กช็อประยะสั้น เรื่องการให้เกียรติกันในที่ทำงานและความปลอดภัยในสถานที่ก่อสร้างเป็นประจำทุกปี ผู้ตรวจสอบสอบยืนยันการเข้าร่วมอบรมและประสิทธิผลผ่านการสุ่มสัมภาษณ์พนักงาน
- G. กระบวนการแก้ไขให้ถูกต้อง (Remediation processes): หากเกิดการกลั่นแกล้งหรือประพฤติมิชอบ ผู้บริหารระดับสูง (หรือผู้มีอำนาจระดับสูงกว่าหากจำเป็น) จะดำเนินการสอบสวน บันทึกรายละเอียดดังกล่าว และทำให้เกิดผลลัพธ์ตามที่ต้องการ ผู้ตรวจสอบจะสอบถามว่า มาตรการลงโทษหรือการแก้ไขนั้นมีการดำเนินภายในเวลาที่เหมาะสม และได้สัดส่วนกับความผิด



ข้อมูลเชิงลึกที่สำคัญ (Key Insight)

แม้จะไม่มีหน่วยงานในแนวป้องกันด้านที่สอง (Second Line) หรือคณะกรรมการชุดย่อยของคณะกรรมการ บริษัทขนาดเล็กก็ยังสามารถนำข้อกำหนดทั้ง 15 ข้อของข้อกำหนดเฉพาะเรื่องพฤติกรรมองค์กรมาประยุกต์ใช้ได้ผ่านกลไกที่ปรับขนาดให้เล็กลง เช่น การใช้ทะเบียนข้อมูลอย่างง่าย การควบคุมดูแลโดยตรงจากผู้บริหารระดับสูง การสอบถามอย่างไม่เป็นทางการ และการฝึกอบรมที่ได้สัดส่วน สิ่งนี้แสดงให้เห็นว่าข้อกำหนดเฉพาะนี้สามารถนำไปใช้ได้จริงและมีความเกี่ยวข้องกับทุกองค์กรโดยไม่ว่าจะมีขนาดใด



ภาคผนวก C. เครื่องมือในการจัดทำเอกสารที่เลือกใช้ได้

ผู้ตรวจสอบภายในได้รับการคาดหวังให้ใช้ดุลยพินิจทางวิชาชีพในการพิจารณาความเหมาะสมของข้อกำหนดต่าง ๆ ไปใช้โดยอิงจากผลการประเมินความเสี่ยง และบันทึกข้อยกเว้นของข้อกำหนดบางประการอย่างเหมาะสม ข้อกำหนดเฉพาะสามารถบันทึกไว้ในแผนการตรวจสอบภายในหรือในกระดาษทำการงานตรวจสอบตามดุลยพินิจทางวิชาชีพของผู้ตรวจสอบ โดยอาจมีงานตรวจสอบภายในหนึ่งงานหรือหลายงานที่ครอบคลุมข้อกำหนดดังกล่าว นอกจากนี้ ข้อกำหนดทั้งหมดอาจไม่สามารถนำมาบังคับใช้ได้ในทุกกรณี แบบฟอร์มที่สามารถพิมพ์ได้ด้านล่างนี้เป็นหนึ่งในทางเลือกสำหรับการจัดทำเอกสารเพื่อแสดงความสอดคล้องกับข้อกำหนดเฉพาะเรื่องพฤติกรรมองค์กร โดยไม่บังคับว่าต้องใช้แบบฟอร์มนี้

การกำกับดูแลพฤติกรรมองค์กร

ข้อกำหนด (Requirement)	การดำเนินการที่ครอบคลุมแล้ว หรือเหตุผลในการยกเว้น (Executed Coverage or Rationale for Exclusion)	เอกสารอ้างอิง (Documentation Reference)
A. คณะกรรมการกำกับดูแล และฝ่ายบริหารระดับสูงจัดโครงสร้างบทบาทและหน้าที่เพื่อหลีกเลี่ยงผลกระทบที่ไม่ได้ตั้งใจอันเป็นผลมาจากพฤติกรรมองค์กรที่ไม่สอดคล้องกัน โดยผลกระทบที่ไม่ได้ตั้งใจดังกล่าวอาจรวมถึงความขัดแย้งทางผลประโยชน์ หรือกระบวนการตัดสินใจที่ไม่ชัดเจน		



ข้อกำหนด (Requirement)	การดำเนินการที่ครอบคลุม แล้ว หรือเหตุผลในการ ยกเว้น (Executed Coverage or Rationale for Exclusion)	เอกสารอ้างอิง (Documentation Reference)
B. คณะกรรมการกำกับดูแล และ ฝ่ายบริหารระดับสูงกำหนดและ ดำรงไว้ซึ่งความรับผิดชอบของ บุคคลและกลุ่มต่อความ คาดหวัง ด้านพฤติกรรม เพื่อให้มั่นใจว่า บทบาทหน้าที่ได้รับการยอมรับ มี ความเข้าใจ และสอดคล้องกับ วัตถุประสงค์ขององค์กรอย่าง สม่ำเสมอ		
C. มีกระบวนการด้านการกำกับ ดูแลเพื่อให้มั่นใจว่ามีการติดตาม ประเมินผล และตั้งคำถาม เกี่ยวกับ ความสอดคล้องระหว่างข้อมูลเชิง ลึกด้านพฤติกรรมกับวัตถุประสงค์ ขององค์กรอย่างสม่ำเสมอ รวมถึงมีการ ดำเนินการแก้ไขเมื่อพบความไม่ สอดคล้องใดๆ		
D. มีการกำหนดและทบทวน นโยบายและวิธีการปฏิบัติงานที่ เกี่ยวกับระเบียบความเสี่ยงด้าน พฤติกรรมเป็นระยะ เพื่อให้มั่นใจใน ความเกี่ยวข้องและความถูกต้อง โดยนโยบายและวิธีการปฏิบัติงาน เหล่านี้ได้รับการสื่อสารและบูรณา การเข้ากับการปฏิบัติงานและการ ตัดสินใจอย่างมีประสิทธิภาพ		

ข้อกำหนดด้านการบริหารความเสี่ยง

ข้อกำหนด (Requirement)	การดำเนินการที่ครอบคลุม แล้ว หรือเหตุผลในการ ยกเว้น (Executed Coverage or Rationale for Exclusion)	เอกสารอ้างอิง (Documentation Reference)
A. องค์กรมีการกำหนดแนวทางการบริหารความเสี่ยงด้านพฤติกรรมอย่างเหมาะสม รวมถึงลักษณะด้านพฤติกรรมที่สำคัญต่อการบรรลุวัตถุประสงค์ขององค์กร		
B. การติดตามพฤติกรรมองค์กรมีความเพียงพอและภายในเวลาที่เหมาะสม โดยมีการสื่อสารผลลัพธ์ให้แก่ผู้มีส่วนได้เสียทราบ		
C. มีการสื่อสารช่องว่าง (Gaps) ระหว่างพฤติกรรมที่คาดหวังและพฤติกรรมที่เกิดขึ้นจริงพร้อมผลการวิเคราะห์สาเหตุที่แท้จริง ให้แก่ผู้มีส่วนได้เสียอย่างสม่ำเสมอและมีประสิทธิภาพ		
D. ช่องว่างระหว่างพฤติกรรมที่คาดหวังและวิธีปฏิบัติในปัจจุบันได้รับการแก้ไขโดยรับฟังความคิดเห็นจากผู้มีส่วนได้เสีย การดำเนินการแก้ไขได้รับการติดตามผลจนเสร็จสิ้น และมีการวัดผลอย่างมีประสิทธิภาพเพื่อให้มั่นใจว่าการดำเนินการที่เพียงพอ		



การควบคุมพฤติกรรมองค์กร

ข้อกำหนด (Requirement)	การดำเนินการที่ ครอบคลุมแล้ว หรือ เหตุผลในการยกเว้น (Executed Coverage or Rationale for Exclusion)	เอกสารอ้างอิง (Documentation Reference)
A. องค์กรได้ออกแบบแนวทางในการ ระบุและบรรเทาความเสี่ยงจากรูปแบบ พฤติกรรมที่อาจก่อให้เกิดความเสี่ยง ต่อการบรรลุวัตถุประสงค์ขององค์กร ภายในองค์กร ตัวอย่างเช่น การ ทบทวนผลการปฏิบัติงาน และการสอบ ทานความเสี่ยงด้านการปฏิบัติงานที่ มุ่งเน้นด้านพฤติกรรม		
B. องค์กรกำหนดทิศทาง (Tone) ที่ ชัดเจนและสม่ำเสมอ เกี่ยวกับพฤติกรรม ที่คาดหวัง และสื่อสารความคาดหวัง ดังกล่าวผ่านช่องทางที่เชื่อถือได้และ เข้าถึงได้ มีกลไกรับฟังความคิดเห็นที่ เป็นระบบ เพื่อประเมินความเข้าใจและ การสนับสนุนจากพนักงาน รวมทั้ง รองรับการเปลี่ยนแปลงเมื่อจำเป็น		
C. มีการกำหนดกระบวนการส่งเสริมการ รายงานพฤติกรรม องค์กรที่ขัดแย้งกับ การบรรลุวัตถุประสงค์ขององค์กร โดย กระบวนการดังกล่าวรวมถึงระเบียบการ คุ้มครอง (Protection) และการแก้ไข ปัญหา (Resolution)		



ข้อกำหนด (Requirement)	การดำเนินการที่ ครอบคลุมแล้ว หรือ เหตุผลในการยกเว้น (Executed Coverage or Rationale for Exclusion)	เอกสารอ้างอิง (Documentation Reference)
D. มีการกำหนดและสื่อสารโปรแกรม สิ่งจูงใจ (Incentive programs) ทั้งใน รูปแบบค่าตอบแทนและรางวัลที่ไม่ใช่ตัว เงินสอดคล้องกับวัตถุประสงค์องค์กร และกฎระเบียบ รวมถึงมาตรการเชิงลบ และผลกระทบสำหรับพฤติกรรมองค์กรที่ ไม่เหมาะสม		
E. มีกระบวนการบริหารจัดการประเด็น ปัญหาต่าง ๆ (Issue management) รวมถึงการระบุและแก้ไขรูปแบบ พฤติกรรมที่ไม่สอดคล้องกับ วัตถุประสงค์ขององค์กร และยกระดับ การรายงานประเด็นปัญหาขึ้นตามลำดับ ชั้น เมื่อจำเป็น		
F. มีโปรแกรมการฝึกอบรมและสร้าง ความตระหนักรู้ เพื่อให้มั่นใจว่า พฤติกรรมองค์กรสอดคล้องกับ วัตถุประสงค์ขององค์กร โดยมีการจัด อบรมอย่างสม่ำเสมอและมีประสิทธิผล		
G. กระบวนการสรรหาบุคลากรที่มี ศักยภาพ (Talent acquisition) และการ ปฐมนิเทศ สอดคล้องกับความคาดหวัง ด้านพฤติกรรมขององค์กร และผนวก ความสามารถด้านพฤติกรรม (Behavioral Competencies) เข้าไว้ใน กระบวนการดังกล่าว		

ภาคผนวก D. การเทียบเคียงกับกรอบการควบคุมภายในและการบริหารความเสี่ยงของ COSO

ตารางด้านล่างแสดงความเชื่อมโยงระหว่างข้อกำหนดเฉพาะด้านพฤติกรรมองค์กร การกำกับดูแล การบริหารความเสี่ยง และ กระบวนการควบคุม กับกรอบการควบคุมภายในแบบบูรณาการของ COSO Internal Control – Integrated Framework (2013) และกรอบการบริหารความเสี่ยงระดับองค์กรของ COSO Enterprise Risk Management Framework (2017) การอ้างอิงเชื่อมโยงนี้ช่วยให้ผู้ตรวจสอบภายในสามารถตรวจสอบความสอดคล้องของการทดสอบที่อ้างอิง COSO กับความครอบคลุมตามข้อกำหนดเฉพาะด้านพฤติกรรมองค์กรได้

ข้อกำหนดด้านการกำกับดูแล

ข้อกำหนด (Requirement)	การอ้างอิง COSO Internal Control (2013)	การอ้างอิง COSO ERM (2017)
A. คณะกรรมการควบคุมดูแลและผู้บริหารระดับสูงจัดโครงสร้างบทบาทและหน้าที่เพื่อหลีกเลี่ยงผลกระทบที่ไม่ได้ตั้งใจอันเป็นผลมาจากพฤติกรรม องค์กรที่ไม่สอดคล้องกันซึ่งรวมถึงความขัดแย้งทางผลประโยชน์ หรือกระบวนการ ตัดสินใจที่ไม่ชัดเจน	สภาพแวดล้อมการควบคุม - หลักการที่ 2 (ความอิสระของคณะกรรมการและการควบคุมดูแล ช่องทางการยกระดับการรายงาน) หลักการที่ 3 (โครงสร้าง อำนาจ และหน้าที่)	การกำกับดูแลและวัฒนธรรม - หลักการที่ 1 (ควบคุมดูแลความเสี่ยงโดย คณะกรรมการ) หลักการที่ 2 กำหนดโครงสร้างการดำเนินงาน)
B. คณะกรรมการควบคุมดูแลและผู้บริหารระดับสูงและรักษาความ รับผิดชอบรายบุคคลและกลุ่มต่อความคาดหวังด้านพฤติกรรม เพื่อให้มั่นใจว่าบทบาท	สภาพแวดล้อมการควบคุม - หลักการที่ 1 (คุณธรรมและค่านิยมด้านจริยธรรม) หลักการที่ 5 (ความรับผิดชอบ และมาตรวัดผลการปฏิบัติงาน)	การกำกับดูแลและวัฒนธรรม - หลักการที่ 4-5 (แสดงความมุ่งมั่นต่อค่านิยมหลัก การดึงดูด พัฒนา และรักษานักวิชาการที่มีความสามารถ)

ข้อกำหนด (Requirement)	การอ้างอิง COSO Internal Control (2013)	การอ้างอิง COSO ERM (2017)
หน้าที่เป็นที่ยอมรับเข้าใจและสอดคล้องกับวัตถุประสงค์องค์กรอย่าง สม่่าเสมอ		
C. มีกระบวนการด้านการกำกับดูแลเพื่อให้มั่นใจว่ามีการติดตามประเมินผล และตั้งคำถามเกี่ยวกับความสอดคล้องระหว่างข้อมูลเชิงลึกด้านพฤติกรรมกับวัตถุประสงค์ขององค์กรเป็นประจำ รวมถึงการดำเนินการเมื่อพบความไม่สอดคล้องต่างๆ	การติดตาม - หลักการที่ 16 (การประเมินผลอย่างต่อเนื่อง/แยกต่างหาก) หลักการที่ 17 (ประเมินผลและสื่อสารข้อบกพร่อง) สารสนเทศและการสื่อสาร - หลักการที่ 13 (ใช้ข้อมูลที่เกี่ยวข้อง) หลักการที่ 14 (สื่อสารภายใน) หลักการที่ 15 (สื่อสารภายนอกในกรณีที่เกี่ยวข้อง)	การกำกับดูแลและวัฒนธรรม - หลักการที่ 1 (ควบคุมดูแลความเสี่ยงโดย คณะกรรมการ) ผลการปฏิบัติงาน - หลักการที่ 10 -14 (ระบุความเสี่ยง ประเมินความรุนแรง จัดลำดับความสำคัญ นำการตอบสนองต่อความเสี่ยงไปปฏิบัติ) สารสนเทศ การสื่อสาร และการรายงาน - หลักการที่ 18 - 20 (การรายงานการฝึกอบรม/การตระหนักรู้)
D. มีการจัดทำและทบทวนนโยบายและวิธีการปฏิบัติงานที่เกี่ยวข้องกับระเบียบความเสี่ยงด้านพฤติกรรมเพื่อให้มีความเกี่ยวข้องและถูกต้องเป็นระยะ นโยบายและวิธีการปฏิบัติงานเหล่านี้ได้รับการสื่อสารและบูรณาการเข้ากับกระบวนการปฏิบัติงานทางธุรกิจและการตัดสินใจ	กิจกรรมการควบคุม - หลักการที่ 10 (เลือกและพัฒนากิจกรรม การควบคุม) หลักการที่ 12 (นำไปใช้ผ่านนโยบายและวิธีการปฏิบัติงาน)	การทบทวนและการปรับปรุง - หลักการที่ 15-17 (ประเมินการเปลี่ยนแปลง) ทบทวนผลการปฏิบัติงาน แสวงหาการปรับปรุง)

ข้อกำหนดด้านการบริหารความเสี่ยง

ข้อกำหนด (Requirement)	การอ้างอิง COSO Internal Control (2013)	การอ้างอิง COSO ERM (2017)
A. องค์กรกำหนดแนวทางบริหารความเสี่ยงด้านพฤติกรรมอย่างเหมาะสม รวมถึงลักษณะทางพฤติกรรมที่สำคัญต่อการบรรลุวัตถุประสงค์องค์กร	การประเมินความเสี่ยง - หลักการที่ 6 (กำหนด วัตถุประสงค์ที่เหมาะสม) หลักการที่ 7 (ระบุและวิเคราะห์ความเสี่ยง) หลักการที่ 8 (ประเมินความเสี่ยงด้านการทุจริต) หลักการที่ 9 (ระบุและวิเคราะห์การเปลี่ยนแปลงที่สำคัญ)	การกำกับดูแลและวัฒนธรรม - หลักการที่ 3-5 (แสดงความมุ่งมั่นต่อค่านิยมหลัก การดึงดูด พัฒนา และรักษาบุคลากรที่มีความสามารถ) การกำหนดกลยุทธ์และวัตถุประสงค์ - หลักการที่ 6-9 (กำหนดระดับความเสี่ยงที่ยอมรับได้ ประเมินกลยุทธ์ทางเลือก พิจารณาความเสี่ยงในวัตถุประสงค์)
B. การติดตามพฤติกรรมองค์กรมีความเพียงพอและภายในเวลาที่เหมาะสม โดยมีการสื่อสารผลลัพธ์ให้แก่ผู้มีส่วนได้เสียทราบ	สารสนเทศและการสื่อสาร - หลักการที่ 13 (ใช้ข้อมูลที่เกี่ยวข้อง) หลักการที่ 14 (สื่อสารภายใน) การติดตาม - หลักการที่ 16 (ประเมินผลอย่างต่อเนื่อง/แยกต่างหาก) หลักการที่ 17 (ประเมินผลและสื่อสารข้อบกพร่อง)	ผลการปฏิบัติงาน - หลักการที่ 10-14 (ระบุความเสี่ยง ประเมิน ความรุนแรง จัดลำดับความเสี่ยง นำการตอบสนองต่อความเสี่ยงไปปฏิบัติ) สารสนเทศ การสื่อสาร และการรายงาน - หลักการที่ 18 - 20 (การรายงานการฝึกอบรม/การตระหนักรู้)
C. ช่องว่างระหว่างความคาดหวังและพฤติกรรมจริง รวมถึงผลการวิเคราะห์สาเหตุที่แท้จริง ได้รับการสื่อสารแก่ผู้มีส่วนได้เสียอย่างสม่ำเสมอและมีประสิทธิผล	สารสนเทศและการสื่อสาร - หลักการที่ 14 (สื่อสารภายใน) หลักการที่ 15 (สื่อสารภายนอกในกรณีที่เกี่ยวข้อง)	สารสนเทศ การสื่อสาร และการรายงาน - หลักการที่ 19 - 20 (สื่อสารข้อมูลความเสี่ยง รายงานเกี่ยวกับความเสี่ยงด้านวัฒนธรรม และผลการปฏิบัติงาน)



D. ช่องว่างระหว่างพฤติกรรมที่คาดหวังและวิธีปฏิบัติในปัจจุบันได้รับการแก้ไข โดยรับฟังความคิดเห็นจากผู้มีส่วนได้เสีย โดยมีการติดตามผลจนเสร็จสมบูรณ์ และวัดผลอย่างมีประสิทธิภาพ เพื่อให้มั่นใจว่ามีการนำไปปฏิบัติจริง	กิจกรรมการควบคุม – หลักการที่ 10 (เลือกและพัฒนา กิจกรรม การควบคุม) หลักการที่ 12 (นำไปใช้ผ่าน นโยบายและวิธีการปฏิบัติงาน) การติดตาม - หลักการที่ 16 (ประเมินผลอย่างต่อเนื่อง/แยก ต่างหาก) หลักการที่ 17 (ประเมินผลและ สื่อสารข้อบกพร่อง)	การทบทวนและการปรับปรุง - หลักการที่ 15 - 17 (ประเมินการ เปลี่ยนแปลง ทบทวนผลการ ปฏิบัติงาน แสวงหาการปรับปรุง)
--	---	---

ข้อกำหนดด้านการควบคุม

ข้อกำหนด (Requirement)	การอ้างอิง COSO Internal Control (2013)	การอ้างอิง COSO ERM (2017)
A. องค์กรออกแบบแนวทางระบุและลดรูปแบบพฤติกรรมที่อาจก่อให้เกิดความเสี่ยงต่อการบรรลุวัตถุประสงค์องค์กรภายในองค์กร ตัวอย่างรวมถึง การทบทวนผลการปฏิบัติงาน และการสอบทานความเสี่ยงด้านปฏิบัติการที่มุ่งเน้นเรื่องพฤติกรรม	การประเมินความเสี่ยง – หลักการที่ 7 (ระบุและวิเคราะห์ความเสี่ยง) หลักการที่ 8 (ประเมินความเสี่ยงด้านการทุจริต) หลักการที่ 9 (วิเคราะห์ การเปลี่ยนแปลงที่สำคัญ) การติดตาม - หลักการที่ 16 (ประเมินผลอย่างต่อเนื่อง/แยกต่างหาก) หลักการที่ 17 (ประเมินผลและสื่อสารข้อบกพร่อง)	ผลการปฏิบัติงาน – หลักการที่ 10 - 14 (ระบุความเสี่ยง ประเมินความรุนแรง จัดลำดับความเสี่ยง นำการตอบสนองต่อความเสี่ยงไปปฏิบัติ) การทบทวนและปรับปรุง - หลักการที่ 15 - 17 (ประเมินการเปลี่ยนแปลง ทบทวนผลการปฏิบัติงาน แสวงหาการปรับปรุง)

ข้อกำหนด (Requirement)	การอ้างอิง COSO Internal Control (2013)	การอ้างอิง COSO ERM (2017)
B. องค์การกำหนดทิศทาง (Tone) ที่ชัดเจนและสอดคล้องเกี่ยวกับพฤติกรรมที่คาดหวัง และสื่อสารผ่านช่องทางที่เข้าถึงได้และน่าเชื่อถือ มีกลไกรับฟังความคิดเห็นที่มีโครงสร้างเพื่อประเมินความเข้าใจและสนับสนุนการเปลี่ยนแปลงเมื่อจำเป็นของพนักงาน	สภาพแวดล้อมการควบคุม - หลักการที่ 1 (คุณธรรมและค่านิยมด้านจริยธรรม) หลักการที่ 5 (ความรับผิดชอบและมาตรวัดผลงาน) สารสนเทศและการสื่อสาร - หลักการที่ 13 (ใช้ข้อมูลที่เกี่ยวข้อง) หลักการที่ 14 (สื่อสารภายใน) หลักการที่ 15 (สื่อสารภายนอกในกรณีที่เกี่ยวข้อง)	การกำกับดูแลและวัฒนธรรม - หลักการที่ 1 (ควบคุมดูแลความเสี่ยงโดยคณะกรรมการ) หลักการที่ 4 (แสดงให้เห็นถึงการยึดมั่นค่านิยมหลัก) หลักการที่ 5 (ตั้งดูด พัฒนา และรักษา บุคลากรที่มีความสามารถ) สารสนเทศ การสื่อสาร และการรายงาน - หลักการที่ 18 - 20 (การรายงานการฝึกอบรม/การตระหนักรู้)
C. มีการจัดตั้งกระบวนการส่งเสริมการรายงานพฤติกรรมองค์กรที่ขัดแย้งกับการบรรลุมัตถุประสงค์ขององค์กร กระบวนการรวมถึงระเบียบการคุ้มครอง (Protection) และการแก้ไขปัญหา (Resolution)	สารสนเทศและการสื่อสาร - หลักการที่ 14 (ช่องทางการสื่อสารภายใน) สภาพแวดล้อมการควบคุม - หลักการที่ 2 (ความอิสระของคณะกรรมการและการควบคุมดูแลช่องทางการยกระดับการรายงาน)	การกำกับดูแลและวัฒนธรรม - หลักการที่ 1 (ควบคุมดูแลความเสี่ยงโดยคณะกรรมการ) หลักการที่ 4 (แสดงให้เห็นถึงการยึดมั่นค่านิยมหลัก) หลักการที่ 5 (ตั้งดูด พัฒนา และรักษา บุคลากรที่มีความสามารถ) สารสนเทศ การสื่อสาร และการรายงาน - หลักการที่ 19 - 20 (สื่อสารข้อมูลความเสี่ยง รายงานความเสี่ยง วัฒนธรรม และผลการปฏิบัติงาน)
D. มีโปรแกรมสิ่งจูงใจ รวมถึงรูปแบบค่าตอบแทนและรางวัลที่ไม่ใช่ตัวเงิน มีการสื่อสารและสอดคล้องกับวัตถุประสงค์ของ	สภาพแวดล้อมการควบคุม - หลักการที่ 1 (คุณธรรมและค่านิยมด้านจริยธรรม)	การกำกับดูแลและวัฒนธรรม - หลักการที่ 4 (แสดงให้เห็นถึงการยึดมั่นค่านิยมหลัก)

ข้อกำหนด (Requirement)	การอ้างอิง COSO Internal Control (2013)	การอ้างอิง COSO ERM (2017)
องค์กรและข้อกำหนดตามกฎระเบียบของทางการ รวมถึงมีมาตรการยับยั้งและผลที่ตามมาสำหรับพฤติกรรมองค์กรที่ไม่เหมาะสม	หลักการที่ 5 (ความรับผิดชอบและมาตรวัดผลการปฏิบัติงาน)	หลักการที่ 5 (ตั้งดูด พัฒนา และรักษาบุคลากรที่มีความสามารถ) ผลการปฏิบัติงาน - หลักการที่ 10 -14 (ระบุความเสี่ยง ประเมินความเสี่ยงรุนแรง จัดลำดับ ความเสี่ยง นำการตอบสนองต่อความเสี่ยงไปปฏิบัติ)
E. มีกระบวนการบริหารจัดการประเด็นปัญหา รวมถึงการระบุและแก้ไขรูปแบบพฤติกรรมที่ไม่สอดคล้องกับวัตถุประสงค์ขององค์กร และการยกระดับการรายงานเมื่อจำเป็น	การติดตาม - หลักการที่ 16 (ประเมินผลอย่างต่อเนื่อง/แยกต่างหาก) หลักการที่ 17 (ประเมินผลและสื่อสารข้อบกพร่อง) สารสนเทศ และการสื่อสาร - หลักการที่ 13 (ใช้ข้อมูลที่เกี่ยวข้อง)	การทบทวนและปรับปรุง - หลักการที่ 15- 17 (ประเมินการเปลี่ยนแปลง ทบทวนผลการปฏิบัติงาน แสวงหาการปรับปรุง) ผลการปฏิบัติงาน - หลักการที่ 10 - 14 (ระบุความเสี่ยง ประเมินความเสี่ยงรุนแรง จัดลำดับ ความเสี่ยง นำการตอบสนองต่อความเสี่ยงไปปฏิบัติ)
F. มีโปรแกรมการฝึกอบรมและสร้างความตระหนักรู้ เพื่อให้มั่นใจว่าพฤติกรรมองค์กรสอดคล้องกับวัตถุประสงค์ขององค์กร โดยมีการจัดอบรมเป็นระยะๆ และมีประสิทธิผล	สภาพแวดล้อมการควบคุม - หลักการที่ 4 (ความมุ่งมั่นในความสามารถ) สารสนเทศและการสื่อสาร - หลักการที่ 13 (ใช้ ข้อมูลที่เกี่ยวข้อง)	การกำกับดูแลและวัฒนธรรม - หลักการ ที่ 5 (ตั้งดูด พัฒนา และรักษาบุคลากรที่มีความสามารถ) สารสนเทศ การสื่อสาร และการรายงาน - หลักการที่ 18-20 (การรายงานการฝึกอบรม/การตระหนักรู้)

ข้อกำหนด (Requirement)	การอ้างอิง COSO Internal Control (2013)	การอ้างอิง COSO ERM (2017)
G. กระบวนการสรรหาบุคลากรที่มีความสามารถและการปฐมนิเทศ สอดคล้องกับความต้องการด้านพฤติกรรมขององค์กร และมีการรวมความสามารถด้านพฤติกรรมเข้าไว้ด้วย	สภาพแวดล้อมการควบคุม - หลักการที่ 1 (คุณธรรมและค่านิยมด้านจริยธรรม) หลักการที่ 4 (ความมุ่งมั่นในความสามารถ)	การกำกับดูแลและวัฒนธรรม - หลักการที่ 5 (ดึงดูด พัฒนา และรักษาบุคลากรที่มีความสามารถ)



ภาคผนวก E. กิจกรรมการตรวจสอบและการให้ความเชื่อมั่นที่เกี่ยวข้องกับพฤติกรรม

ผู้ตรวจสอบภายในอาจพบว่างานที่กำลังดำเนินการอยู่แล้ว จะชี้ให้เห็นถึงการปฏิบัติตามข้อกำหนดเฉพาะเรื่องพฤติกรรมองค์กรได้ ตารางนี้ระบุถึงงานตรวจสอบเฉพาะจุด (Focused audits) และองค์ประกอบ การตรวจสอบทั่วไป (Common audit elements) ที่อาจเทียบเคียงได้กับข้อกำหนดและสามารถใช้เพื่อแสดงถึงการปฏิบัติตามมาตรฐานตามความเหมาะสม ตัวอย่างเหล่านี้ไม่ใช่การตรวจสอบที่ถูกต้องว่าเป็นการตรวจสอบที่ต้องทำแต่มีไว้เพื่อแสดงให้เห็นว่ากิจกรรมการตรวจสอบที่ดำเนินการโดยทั่วไปอาจให้ความครอบคลุมถึงข้อกำหนดเฉพาะได้

ตัวอย่างของการตรวจสอบและกิจกรรมการให้ความเชื่อมั่นที่สามารถจัดการกับเรื่องพฤติกรรมได้ทั้งทางตรงและทางอ้อม:

ขอบเขต (Area)	การตรวจสอบที่เฉพาะจุด (Focused audits)	องค์ประกอบทดสอบทั่วไปในงานตรวจสอบ (Common testing elements in audits)
การกำกับดูแล (Governance)	- วัฒนธรรมความเสี่ยง - การกำกับดูแลกิจการ - การสอบทานประสิทธิผลของคณะกรรมการ/ภาวะผู้นำ - การตอบสนองต่อกฎเกณฑ์ของทางการ - ค่าตอบแทนและสิ่งจูงใจ - การวัดผลการปฏิบัติงาน - กลยุทธ์และการวางแผนองค์กร	- นโยบายและวิธีการปฏิบัติงานขององค์กร - การควบคุมระดับองค์กร/การสอบทานโดยฝ่ายบริหาร (Entity level/Management review) - การแก้ไขปรับปรุงประเด็นด้านกฎระเบียบทั่วทั้งองค์กร (ตัวอย่างเช่น แผนปรับปรุงทางธุรกิจ)



ขอบเขต (Area)	การตรวจสอบที่เฉพาะจุด (Focused audits)	องค์ประกอบทดสอบทั่วไป ในงานตรวจสอบ (Common testing elements in audits)
	● การวางแผนการปรับเปลี่ยนองค์กร ● การควบคุมและซื้อกิจการ	● การมอบอำนาจ (Delegation of authority)
การบริหารความเสี่ยง (Risk Management)	● หน่วยงานด้านกฎหมายและการปฏิบัติตามกฎเกณฑ์ ● กรอบการบริหารความเสี่ยง (Risk management framework) ● โปรแกรมด้านจริยธรรมและการปฏิบัติตามกฎเกณฑ์ ● ด้านสิ่งแวดล้อม สังคม และ การกำกับดูแล ● การสอบสวนการทุจริต/สายด่วนแจ้งเบาะแส	● การดูแลรักษาทะเบียนความเสี่ยงและวิธีการควบคุม (Risk & Control Registers) ● การประเมินตนเองของฝ่ายบริหาร (Management self-assessments) ● การตอบสนองต่อความล้มเหลวของการควบคุมและข้อตรวจพบจากการตรวจสอบหรือหน่วยงานอื่น
การควบคุม (Controls)	● ทรัพยากรบุคคล (รวมถึงการสรรหาและการรักษาพนักงาน) ● กระบวนการขาย (ตัวอย่างเช่น พฤติกรรมการขายและการปฏิบัติตามกฎเกณฑ์) ● การจัดซื้อจัดจ้าง (ตัวอย่างเช่น ความเป็นอิสระของผู้ขาย การรับรองลูกค้า) ● สาขา/หน่วยงานย่อย (ตัวอย่างเช่น การจัดการ และการสอบสวน) ● สายด่วนแจ้งเบาะแสการทุจริต	● การแบ่งแยกหน้าที่งาน ● การสอบสวนโดยฝ่ายบริหาร และการติดตามวิธีการควบคุม ● ความเสี่ยงจากการทุจริตในระดับบุคคล ● ความสามารถ ทักษะ และความตระหนักด้านความเสี่ยง ● การแก้ไขปรับปรุงกระบวนการและวิธีการควบคุม

เกี่ยวกับสมาคมผู้ตรวจสอบภายใน (The Institute of Internal Auditors)

สมาคมผู้ตรวจสอบภายใน (IIA) เป็นสมาคมวิชาชีพระหว่างประเทศที่ให้บริการสมาชิกมากกว่า 265,000 คนทั่วโลก และได้มอบวุฒิบัตรผู้ตรวจสอบภายในที่ได้รับการรับรอง (Certified Internal Auditor® - CIA®) ไปแล้วกว่า 200,000 ฉบับ สมาคมก่อตั้งขึ้นในปี ค.ศ. 1941 โดย สมาคมได้รับการยอมรับทั่วโลกในฐานะผู้นำวิชาชีพการตรวจสอบภายในด้านมาตรฐาน วุฒิบัตรรับรองคุณวุฒิ การศึกษา การวิจัย และแนวทางปฏิบัติต่างๆ สำหรับข้อมูลเพิ่มเติมโปรดเยี่ยมชม theiia.org

ข้อความปฏิเสธความรับผิดชอบ (Disclaimer)

IIA ตีพิมพ์เอกสารนี้เพื่อวัตถุประสงค์ในการให้ข้อมูลและเพื่อการศึกษาเท่านั้น ไม่ได้มีวัตถุประสงค์เพื่อให้คำตอบที่ชัดเจนที่สุดสำหรับสถานการณ์เฉพาะแต่ละสถานการณ์ ดังนั้น จึงมีวัตถุประสงค์เพียงเพื่อใช้เป็นแนวทางในการปฏิบัติงานเท่านั้น IIA จึงใคร่แนะนำให้ท่านขอคำปรึกษาจากผู้เชี่ยวชาญอิสระซึ่งมีความรู้เกี่ยวข้องโดยตรงกับสถานการณ์เฉพาะนั้นๆ IIA จะไม่รับผิดชอบใดๆ ต่อการที่ผู้ใดก็ตามที่เชื่อและอาศัยคำแนะนำนี้เพียงอย่างเดียว

ลิขสิทธิ์ (Copyright)

© 2025 สมาคมผู้ตรวจสอบภายในสงวนลิขสิทธิ์ สำหรับการขออนุญาตทำซ้ำ โปรดติดต่อ

copyright@theiia.org

ธันวาคม 2025 (พ.ศ.2568)



The Institute of
Internal Auditors

Global Headquarters

The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, USA
Phone: +1-407-937-1111
Fax: +1-407-937-1101