



THE IIA'S THREE LINES MODEL

แนวป้องกันสามด้าน ฉบับปรับปรุงใหม่

สารบัญ

บทนำ	1
หลักการของโมเดลสามด้าน	3
หลักการที่ 1: การกำกับดูแล	3
หลักการที่ 2: บทบาทขององค์คณะผู้มีหน้าที่กำกับดูแล	3
หลักการที่ 3: บทบาทของฝ่ายบริหารและด้านที่หนึ่งกับด้านที่สอง	4
หลักการที่ 4: บทบาทของด้านที่สาม	4
หลักการที่ 5: ความเป็นอิสระของด้านที่สาม	4
หลักการที่ 6: การสร้างและปกป้องคุณค่า	5
บทบาทที่สำคัญในโมเดลสามด้าน	7
ฝ่ายบริหาร	7
ตรวจสอบภายใน	8
ผู้ให้บริการให้ความเชื่อมั่นจากภายนอก	8
ความสัมพันธ์ในระหว่างบทบาทหลัก	9
ระหว่างองค์คณะผู้มีหน้าที่กำกับดูแลกับฝ่ายบริหาร (ทั้งบทบาทที่อยู่ในด้านแรกและด้านที่สอง)	9
ระหว่างฝ่ายบริหาร (ทั้งบทบาทที่อยู่ในด้านแรกและด้านที่สอง) กับตรวจสอบภายใน	10
ระหว่างตรวจสอบภายในกับองค์คณะผู้มีหน้าที่กำกับดูแล	10
ในท่ามกลางบทบาททั้งหมด	11
การประยุกต์ใช้โมเดล	12
โครงสร้าง บทบาท และภาระหน้าที่	12
การดูแลและการให้ความเชื่อมั่น	13
การประสานงานและเป็นไปในทิศทางเดียวกัน	13

บทนำ

องค์กรทั้งหลายเป็นสิ่งที่ดำเนินงานโดยมนุษย์ ปฏิบัติงานภายใต้ความไม่แน่นอน ความซับซ้อน เชื่อมโยงระหว่างกัน และเปลี่ยนแปลงตลอดเวลามากขึ้นเรื่อยๆ องค์กรเหล่านั้นมักจะมีผู้มีส่วนได้เสียที่หลากหลาย แปรเปลี่ยนง่าย และในบางครั้งก็แข่งขันกันในเรื่องผลประโยชน์ ผู้มีส่วนได้เสียต่างๆ จะมอบความไว้วางใจในการดูแลองค์กรให้แก่องค์กรและผู้มีหน้าที่กำกับดูแล ซึ่งในทางกลับกันก็จะมอบหมายทรัพยากรและอำนาจให้แก่ฝ่ายบริหารเพื่อดำเนินการต่างๆ ตามความเหมาะสม ซึ่งหมายรวมถึงการดำเนินการจัดการความเสี่ยงด้วย

ด้วยเหตุผลเหล่านี้และเหตุผลอีกมากมาย องค์กรหลายๆ แห่งต่างจำเป็นต้องมีโครงสร้างและกระบวนการที่มีประสิทธิภาพเพื่อช่วยให้บรรลุวัตถุประสงค์ได้ในขณะเดียวกันก็ส่งเสริมการกำกับดูแลและการบริหารความเสี่ยงที่แข็งแกร่ง เนื่องจากองค์กรและผู้มีหน้าที่กำกับดูแลจะรับรายงานเกี่ยวกับกิจกรรม ผลประกอบการและประมาณการจากฝ่ายบริหาร ทั้งองค์กรและผู้มีหน้าที่กำกับดูแลและฝ่ายบริหารต่างก็ต้องพึ่งพาตรวจสอบภายในในการให้ความเชื่อมั่นอย่างเป็นอิสระและเที่ยงธรรม รวมทั้งให้คำแนะนำในเรื่องต่างๆ เพื่อส่งเสริมและช่วยให้เกิดนวัตกรรมและการปรับปรุงไปในทางที่ดีขึ้น แต่ในที่สุดแล้ว องค์กรและผู้มีหน้าที่กำกับดูแลก็ต้องรับผิดชอบต่อผลการกำกับดูแล ซึ่งจะบรรลุผลได้โดยผ่านทางกรกระทำและพฤติกรรมต่างๆ ขององค์กรและผู้มีหน้าที่กำกับดูแลเอง รวมทั้งฝ่ายบริหารและตรวจสอบภายในด้วย

โมเดลสามด้าน จะช่วยองค์กรระบุโครงสร้างและกระบวนการที่จะช่วยให้บรรลุวัตถุประสงค์ได้ดีที่สุด และเชื่อมต่อการกำกับดูแลและการบริหารความเสี่ยงที่แข็งแกร่ง โมเดลนี้ใช้ได้กับทุกองค์กรและจะมีประสิทธิภาพสูงสุดโดย:

คำศัพท์ที่สำคัญ

องค์กร (Organization) - กลุ่มของกิจกรรม ทรัพยากร และคน ซึ่งทำงานโดยมุ่งสู่เป้าหมายร่วมกันโดยได้รับการจัดระเบียบมาแล้ว

ผู้มีส่วนได้เสีย (Stakeholders) - กลุ่มต่างๆ หรือบุคคลซึ่งได้รับผลประโยชน์หรือได้รับผลกระทบจากองค์กร

องค์กรและผู้มีหน้าที่กำกับดูแล (Governing body) - บุคคลต่างๆ ผู้ซึ่งรับผิดชอบต่อผู้มีส่วนได้เสีย ในความสำเร็จขององค์กร

ฝ่ายบริหาร (Management) - บุคคล ทีม และงานที่ทำหน้าที่สนับสนุนที่ได้รับมอบหมายให้ต้องส่งมอบผลิตภัณฑ์และ/หรือบริการ แก่ลูกค้าขององค์กร

ตรวจสอบภายใน (Internal audit) - บุคคลทั้งหลายที่ปฏิบัติงานอย่างเป็นอิสระจากฝ่ายบริหารในการให้ความเชื่อมั่นและข้อมูลที่ลึกซึ้งเกี่ยวกับความพอเพียงและประสิทธิผลของการกำกับดูแลและการบริหารความเสี่ยง (รวมทั้งการควบคุมภายในด้วย)

โมเดลสามด้าน (The Three Lines Model) - โมเดลที่แต่เดิมรู้จักกันในชื่อที่ว่า แนวป้องกันสามด้าน (Three Lines of Defense)

การควบคุมภายใน (Internal control) - กระบวนการต่างๆ ที่ได้ออกแบบมาเพื่อก่อให้เกิดความเชื่อมั่นในการบรรลุวัตถุประสงค์ต่างๆ

- การยอมรับแนวทางที่อาศัยหลักการ (principles-based approach) และปรับโมเดลให้เหมาะสมกับวัตถุประสงค์ขององค์กรและสถานการณ์
- การมุ่งเน้นไปที่ผลที่ได้รับจากการบริหารความเสี่ยงในการช่วยให้บรรลุวัตถุประสงค์และช่วยเพิ่มคุณค่า รวมทั้งให้ความสำคัญในเรื่องของการ "ป้องกัน" และปกป้องคุณค่า
- ความเข้าใจอย่างแจ่มแจ้งในบทบาทและหน้าที่ต่างๆ ตามที่แสดงไว้ในโมเดล รวมทั้งความสัมพันธ์ในระหว่างบทบาทเหล่านั้น
- การนำเอามาตรการต่างๆ ไปใช้ปฏิบัติเพื่อที่จะทำให้เชื่อมั่นได้ว่า กิจกรรมและวัตถุประสงค์ต่างๆ สอดคล้องกับลำดับความสำคัญของผลประโยชน์ของผู้มีส่วนได้เสียต่างๆ

หลักการของโมเดลสามด้าน

หลักการที่ 1: การกำกับดูแล

การกำกับดูแลขององค์กรหนึ่ง ๆ จำเป็นต้องมีโครงสร้างและกระบวนการที่เหมาะสม ซึ่งจะช่วยส่งเสริม:

- ความรับผิดชอบขององค์คณะผู้มีหน้าที่กำกับดูแลที่มีต่อผู้มีส่วนได้เสีย ในการดูแลองค์กรโดยผ่านทาง ความมีคุณธรรม ความเป็นผู้นำ และความโปร่งใส
- การกระทำ/การปฏิบัติ (ซึ่งรวมถึงการจัดการความเสี่ยง) โดยฝ่ายบริหาร เพื่อที่จะบรรลุวัตถุประสงค์ขององค์กรโดยผ่านทาง การตัดสินใจที่ตั้งอยู่บนพื้นฐานของความเสี่ยง และการใช้ทรัพยากรต่างๆ
- การให้ความเชื่อมั่นและคำแนะนำ โดยหน่วยงานตรวจสอบภายในที่เป็นอิสระ เพื่อให้ความชัดเจนและความมั่นใจ และเพื่อที่จะส่งเสริมและช่วยให้เกิดการปรับปรุงอย่างต่อเนื่อง โดยผ่านทาง การสอบถามอย่างเข้มงวดและการสื่อสารอย่างชาญฉลาด

คำศัพท์ที่สำคัญ

การตัดสินใจที่ตั้งอยู่บนพื้นฐานของความเสี่ยง (Risk-based decision-making) - กระบวนการที่ได้พิจารณาแล้ว ซึ่งรวมถึง การวิเคราะห์ การวางแผน การดำเนินการ การเฝ้าติดตาม และการสอบทาน และคำนึงถึงผลกระทบที่อาจเกิดขึ้นจากจากความไม่แน่นอนที่มีต่อวัตถุประสงค์

ความเชื่อมั่น (Assurance) - การยืนยันและความมั่นใจอย่างอิสระ

หลักการที่ 2: บทบาทขององค์คณะผู้มีหน้าที่กำกับดูแล

องค์คณะผู้มีหน้าที่กำกับดูแลให้ความมั่นใจว่า:

- มีโครงสร้างและกระบวนการที่เหมาะสม สำหรับการกำกับดูแลที่มีประสิทธิภาพ
- วัตถุประสงค์และกิจกรรมขององค์กรสอดคล้องกับผลประโยชน์ของผู้มีส่วนได้เสียตามลำดับความสำคัญ

องค์คณะผู้มีหน้าที่กำกับดูแลจะ:

- มอบหมายภาระหน้าที่และจัดสรรทรัพยากรให้แก่ฝ่ายบริหารเพื่อให้บรรลุวัตถุประสงค์ขององค์กร ในขณะที่ให้ความมั่นใจว่าจะบรรลุความคาดหวังทั้งในทางกฎหมาย ระเบียบทางการและจริยธรรม
- จัดตั้งและดูแลงานตรวจสอบภายในที่เที่ยงธรรมและมีความสามารถ เพื่อให้ความชัดเจนและความมั่นใจในความคืบหน้าในการบรรลุเป้าหมาย

หลักการที่ 3: บทบาทของฝ่ายบริหารและด้านที่หนึ่งกับด้านที่สอง

ภาระหน้าที่ของฝ่ายบริหารในการบรรลุเป้าหมายทางองค์กรนั้น ประกอบด้วยบทบาทในด้านที่หนึ่งและด้านที่สอง¹ บทบาทในด้านที่หนึ่ง ส่วนใหญ่จะสอดคล้องโดยตรงกับการส่งมอบผลิตภัณฑ์และบริการให้แก่ลูกค้าขององค์กรซึ่งรวมถึงงานสนับสนุน² ด้วย ส่วน บทบาทในด้านที่สอง นั้นจะทำหน้าที่ให้ความช่วยเหลือด้านการบริหารความเสี่ยง

บทบาทในด้านที่หนึ่งและสองนั้น อาจอยู่ด้วยกัน หรืออาจจะแยกกันอยู่ก็ได้ บทบาทบางอย่างในด้านที่สองสามารถมอบหมายไปให้แก่ผู้เชี่ยวชาญเพื่อเสริมความเชี่ยวชาญ ความสนับสนุน การเฝ้าติดตาม และการตั้งคำถามไปยังฝ่ายบริหารที่อยู่ในด้านที่หนึ่งก็ได้ บทบาทในด้านที่สองนั้น ควรมุ่งเน้นไปที่วัตถุประสงค์เฉพาะบางเรื่อง เช่น เรื่องการปฏิบัติตามกฎหมายข้อบังคับและพฤติกรรมอันมีจริยธรรมที่ยอมรับได้ การควบคุมภายใน ความปลอดภัยของข้อมูลและเทคโนโลยี ความมั่นคงยั่งยืน และการประกันคุณภาพ หรืออีกทางเลือกหนึ่ง บทบาทในด้านที่สองอาจขยายภาระหน้าที่ในด้านการบริหารความเสี่ยงให้กว้างออกไปได้ อย่างเช่น การบริหารความเสี่ยงทั่วทั้งองค์กร (หรือ ERM) อย่างไรก็ตาม หน้าที่การบริหารความเสี่ยงยังคงเป็นส่วนหนึ่งของบทบาทในด้านที่หนึ่งและภายในขอบเขตงานของฝ่ายบริหาร

หลักการที่ 4: บทบาทของด้านที่สาม

ตรวจสอบภายในจะให้ความเชื่อมั่นและคำแนะนำอย่างเป็นอิสระและเที่ยงธรรม เกี่ยวกับความพอเพียงและประสิทธิผลของการกำกับดูแลและการบริหารความเสี่ยง³ ซึ่งจะบรรลุได้ด้วยการใช้กระบวนการที่เป็นระบบระเบียบ ความเชี่ยวชาญและข้อมูลเชิงลึก ตรวจสอบภายในจะรายงานสิ่งที่ตรวจพบไปยังฝ่ายบริหารและองค์คณะผู้มีหน้าที่กำกับดูแลเพื่อส่งเสริมและช่วยให้เกิดการปรับปรุงอย่างต่อเนื่อง ในการนี้ ตรวจสอบภายในอาจพิจารณาใช้ความเชื่อมั่นที่ให้อาจให้ความเชื่อมั่นอื่นจากภายในและภายนอกองค์กรก็ได้

หลักการที่ 5: ความเป็นอิสระของด้านที่สาม

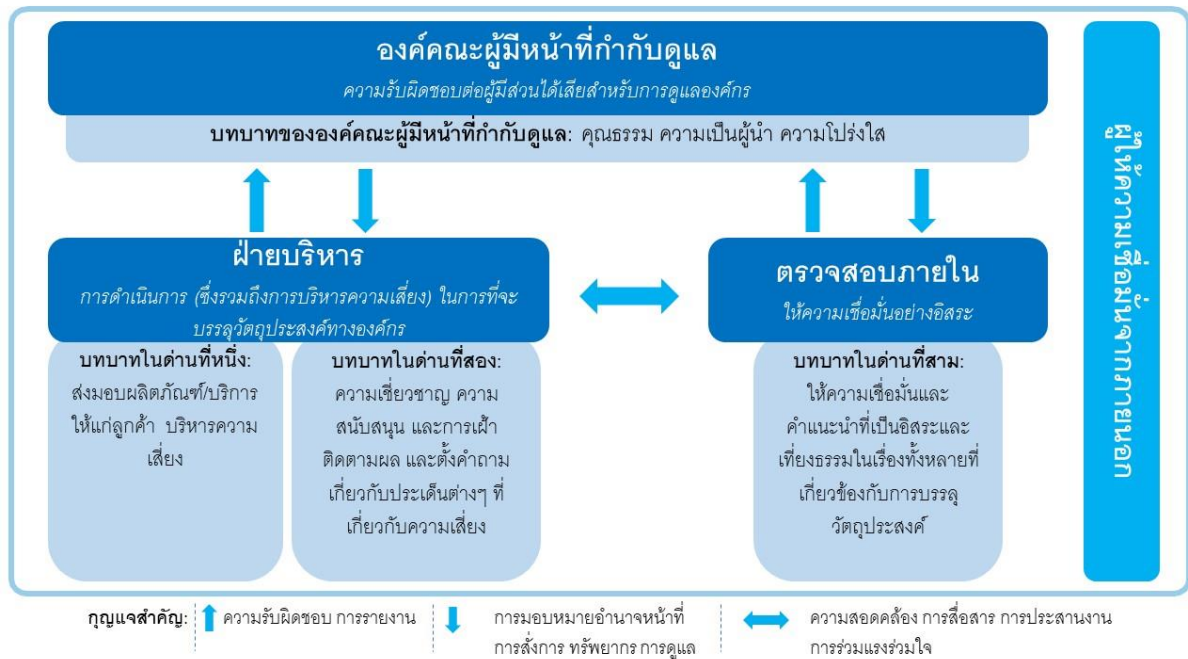
ความเป็นอิสระจากภาระหน้าที่ในทางการบริหารของตรวจสอบภายในเป็นสิ่งสำคัญยิ่งต่อความเที่ยงธรรม อำนวย และความน่าเชื่อถือ ซึ่งจะเกิดขึ้นได้โดยผ่านทางความรับผิดชอบต่อองค์คณะผู้มีหน้าที่กำกับดูแล การเข้าถึงบุคคลากร ทรัพยากร และข้อมูลที่จำเป็นในอันที่จะปฏิบัติงานให้สำเร็จลุล่วงได้อย่างไม่มีข้อจำกัด และเป็นอิสระจากอคติหรือการแทรกแซง ในการวางแผนและการส่งมอบบริการตรวจสอบ

หลักการที่ 6: การสร้างและปกป้องคุณค่า

บทบาททั้งหมดซึ่งทำงานร่วมกันจะมีส่วนช่วยในการสร้างและปกป้องคุณค่าก็ต่อเมื่อบทบาทเหล่านั้นสอดคล้องซึ่งกันและกัน และสอดคล้องกับผลประโยชน์ของผู้มีส่วนได้เสียตามที่ได้จัดลำดับความสำคัญไว้แล้ว การจัดกิจกรรมสอดคล้องไปในทิศทางเดียวกันจะบรรลุได้โดยผ่านทาง การสื่อสาร ความร่วมมือ ร่วมแรงร่วมใจกัน สิ่งนี้จะทำให้นั่นใจได้ในเรื่องความน่าเชื่อถือ ความสอดคล้อง และความโปร่งใสของข้อมูลที่จำเป็นต้องใช้ในการตัดสินใจโดยอาศัยความเสี่ยงเป็นพื้นฐาน

-
1. การใช้คำว่า "ด้านที่หนึ่ง" "ด้านที่สอง" และ "ด้านที่สาม" นี้ยังคงไว้เช่นเดียวกับโมเดลแรกเริ่มเพื่อประโยชน์ในเรื่องความคุ้นชิน อย่างไรก็ตาม คำว่า "ด้าน" หรือ "lines" ไม่ได้มุ่งหวังที่จะแสดงองค์ประกอบในเชิงโครงสร้าง แต่เป็นการแยกแยะบทบาทอย่างมีประโยชน์ ตามหลักแล้ว องค์คณะผู้มีหน้าที่กำกับดูแลยังเป็น "ด้าน" เองด้วย แต่แนวคิดนี้ยังไม่ได้รับการยอมรับในการหลีกเลี่ยงความสับสน การให้ลำดับหมายเลข (ที่หนึ่ง ที่สอง ที่สาม) ไม่ควรนำมาใช้เพื่อตีความว่าเป็นการปฏิบัติงานตามลำดับขั้น แท้จริงแล้วบทบาททั้งหมดจะทำงานไปพร้อมๆ กัน
 2. บางคนถือว่า หน่วยงานสนับสนุน (เช่น งานทรัพยากรบุคคล งานธุรการ และงานบริการอาคาร) เป็นบทบาทในด้านที่สอง เพื่อความชัดเจน โมเดลสามด้านนี้ถือว่าบทบาทในด้านแรกได้รวมถึงกิจกรรมใน "หน้าบ้าน" และ "หลังบ้าน" ด้วย และบทบาทในด้านที่สองจะประกอบด้วยกิจกรรมต่างๆ ที่มุ่งความสนใจไปที่เรื่องต่างๆ ที่เกี่ยวกับความเสี่ยง
 3. ในบางครั้ง บทบาทอื่นในด้านที่สามอาจถูกระบุไว้ เช่นว่า การกำกับดูแล การตรวจสอบผลิตภัณฑ์ การสอบสวน การประเมินผล และการแก้ไขปัญหา ซึ่งอาจเป็นส่วนหนึ่งในหน้าที่งานตรวจสอบภายใน หรืออาจแยกออกไปก็ได้

โมเดลสามด้านของ IIA



บทบาทที่สำคัญในโมเดลสามด้าน

การแบ่งแยกหน้าที่ในองค์กรต่างๆ มีความแตกต่างกันเป็นอย่างมาก อย่างไรก็ตาม บทบาทในระดับสูงต่อไปนี้จะอธิบายขยายความหลักการของโมเดลสามด้าน (Principles of the Three Lines Model)

องค์กรที่มีหน้าที่กำกับดูแล (Governing body)

- รับผิดชอบต่อผู้มีส่วนได้เสียในการดูแลองค์กร
- ร่วมกับผู้มีส่วนได้เสียในการเฝ้าระวังผลประโยชน์ของผู้มีส่วนได้เสีย และสื่อสารเกี่ยวกับการบรรลุวัตถุประสงค์อย่างโปร่งใส
- ดูแลเอาใจใส่วัฒนธรรมที่ส่งเสริมพฤติกรรมและความรับผิดชอบที่มีจริยธรรม
- กำหนดโครงสร้างและกระบวนการสำหรับการกำกับดูแล ซึ่งรวมถึง การจัดตั้งคณะกรรมการขึ้นมาช่วยเหลือตามความจำเป็น
- มอบหมายภาระหน้าที่ และจัดทรัพยากรให้แก่ฝ่ายบริหารเพื่อการบรรลุวัตถุประสงค์ขององค์กร
- กำหนดระดับการยอมรับความเสี่ยง (appetite for risk) ขององค์กร และกำกับดูแลการบริหารความเสี่ยง (รวมทั้งการควบคุมภายใน)
- คอยดูแลให้มีการปฏิบัติตามกฎหมาย ข้อบังคับทางการ และความคาดหวังที่ค้างงมีจริยธรรม
- จัดให้มีและดูแลหน้าที่งานตรวจสอบภายในที่เป็นอิสระและเที่ยงธรรม

ฝ่ายบริหาร

บทบาทในด้านแรก

- เป็นผู้นำและสั่งการการดำเนินการต่างๆ (ซึ่งรวมทั้งการบริหารความเสี่ยง) และการใช้ทรัพยากรเพื่อบรรลุวัตถุประสงค์ขององค์กร
- มีการสนทนากับองค์กรที่มีหน้าที่กำกับดูแลอย่างต่อเนื่อง และรายงานเกี่ยวกับผลประกอบการที่ได้วางแผนไว้ ผลประกอบการจริง และผลประกอบการที่คาดว่าจะเกิดขึ้นโดยเชื่อมโยงกับวัตถุประสงค์ขององค์กร และความเสี่ยง
- จัดให้มีและรักษาไว้ซึ่งโครงสร้างและกระบวนการที่เหมาะสม สำหรับการบริหารการปฏิบัติงานต่างๆ และความเสี่ยง (รวมทั้งการควบคุมภายใน)
- มั่นใจได้ในเรื่องการปฏิบัติตามกฎหมาย ข้อบังคับทางการ และความคาดหวังที่มีจริยธรรม

บทบาทในด้านที่สอง

- ให้ความเชี่ยวชาญ ความสนับสนุน การเฝ้าระวัง และตั้งคำถามเกี่ยวกับการบริหารความเสี่ยง รวมทั้ง:
 - การพัฒนา การนำไปปฏิบัติ และการปรับปรุงอย่างต่อเนื่องในวิธีปฏิบัติเกี่ยวกับการบริหารความเสี่ยง (รวมทั้งการควบคุมภายใน) ณ ที่ระดับกระบวนการ ระบบ และที่ระดับองค์กร
 - การบรรลุวัตถุประสงค์ของการบริหารความเสี่ยง เช่น การปฏิบัติตามกฎหมาย ข้อบังคับทางการ และความคาดหวังที่มีจริยธรรม ความมั่นคงปลอดภัยของข้อมูล และเทคโนโลยี ความยั่งยืนของกิจการ และการประกันคุณภาพ
- ทำการวิเคราะห์และจัดทำรายงานเกี่ยวกับความพอเพียงและประสิทธิผลของการบริหารความเสี่ยง (รวมทั้งการควบคุมภายใน)

ตรวจสอบภายใน

- คงไว้ซึ่งความรับผิดชอบหลักที่มีต่อองค์กรและผู้มีหน้าที่กำกับดูแล และเป็นอิสระจากภาระหน้าที่ในทางการบริหาร
- สื่อสารความเชื่อมั่นและคำแนะนำที่เป็นอิสระและเที่ยงธรรม เกี่ยวกับความพอเพียงและประสิทธิผลของการกำกับดูแลและการบริหารความเสี่ยง (รวมทั้งการควบคุมภายใน) เพื่อสนับสนุนการบรรลุเป้าหมายในทางองค์กร และเพื่อส่งเสริมและเอื้อให้เกิดการปรับปรุงอย่างต่อเนื่อง
- รายงานความเสียหายต่อความเป็นอิสระ และความเที่ยงธรรม ต่อองค์กรและผู้มีหน้าที่กำกับดูแล และนำมาตรการป้องกันไปใช้ปฏิบัติตามความจำเป็น

ผู้ให้บริการให้ความเชื่อมั่นจากภายนอก

- ให้ความเชื่อมั่นเพิ่มเติม เพื่อ:
 - สนองตอบต่อความคาดหวังในทางกฎหมายและข้อบังคับทางการที่ทำหน้าที่ปกป้องผลประโยชน์ของผู้มีส่วนได้เสีย
 - สนองตอบต่อคำร้องขอของฝ่ายบริหารและองค์กรและผู้มีหน้าที่กำกับดูแลเพื่อเสริมความเชื่อมั่นที่มาจากภายใน

ความสัมพันธ์ในระหว่างบทบาทหลัก

ระหว่างองค์คณะผู้มีหน้าที่กำกับดูแลกับฝ่ายบริหาร (ทั้งบทบาทที่อยู่ในด้านแรกและด้านที่สอง)

องค์คณะผู้มีหน้าที่กำกับดูแลมักจะเป็นผู้กำหนดทิศทางขององค์กร ด้วยการกำหนด วิสัยทัศน์ พันธกิจ และคุณค่า/ค่านิยมองค์กร รวมทั้งระดับการยอมรับความเสี่ยงขององค์กร แล้วจึงมอบหมายภาระหน้าที่ไปพร้อมๆ กับให้ทรัพยากรที่จำเป็นแก่ผู้บริหารในการบรรลุวัตถุประสงค์ขององค์กร องค์คณะผู้มีหน้าที่กำกับดูแลจะรับรายงานจากฝ่ายบริหาร เกี่ยวกับผลประกอบการที่ได้วางแผนไว้ ผลประกอบการจริงที่เกิดขึ้น และผลประกอบการที่คาดว่าจะ เป็น รวมทั้งรายงานเกี่ยวกับความเสี่ยงและการบริหารความเสี่ยง

คำศัพท์ที่สำคัญ

ประธานเจ้าหน้าที่บริหาร (Chief executive officer -- CEO) - บุคลากรระดับสูงสุดภายในองค์กร ที่มีหน้าที่ด้านการดำเนินงานต่างๆ

องค์กรต่างๆ จะแตกต่างกันไปในเรื่องของ การทับซ้อนและการแบ่งแยกบทบาทระหว่างองค์คณะผู้มีหน้าที่กำกับดูแลและฝ่ายบริหาร องค์คณะผู้มีหน้าที่กำกับดูแลสามารถ "ลงมือเอง" ในส่วนที่เกี่ยวกับกลยุทธ์และการปฏิบัติงานไม่มากนักน้อย องค์คณะผู้มีหน้าที่กำกับดูแลหรือฝ่ายบริหารอาจจะเป็นผู้ดำเนินการพัฒนาแผนกลยุทธ์หรืออาจจะแค่มีส่วนในการดำเนินการ ในบางเขตอำนาจศาล ประธานเจ้าหน้าที่บริหาร (Chief Executive Officer -- CEO) อาจจะเป็นสมาชิกอยู่ในองค์คณะผู้มีหน้าที่กำกับดูแลและอาจเป็นถึงประธานองค์คณะฯ ก็ได้ แต่ในทุกกรณี จำเป็นต้องมีการสื่อสารที่แข็งแกร่งระหว่างฝ่ายบริหารและองค์คณะฯ CEO มักจะเป็นจุดศูนย์กลางสำหรับการสื่อสารนี้ แต่ผู้บริหารระดับสูงอื่นๆ อาจจะมีปฏิสัมพันธ์กับองค์คณะฯ ได้เสมอ องค์คณะฯ อาจต้องการและทางการอาจจะกำหนดให้ ผู้นำในบทบาทที่อยู่ในด้านที่สอง ดังเช่นประธานเจ้าหน้าที่บริหารความเสี่ยง (Chief Risk Officer -- CRO) และประธานเจ้าหน้าที่กำกับ การปฏิบัติตามกฎระเบียบ (Chief Compliance Officer -- CCO) มีสายการรายงานตรงต่อองค์คณะผู้มีหน้าที่กำกับดูแล ซึ่งสายการรายงานเช่นนี้จะสอดคล้องกับหลักการของโมเดลสามด้าน (Principles of the Three Lines Model) อย่างสมบูรณ์

ระหว่างฝ่ายบริหาร (ทั้งบทบาทที่อยู่ในด้านแรกและด้านที่สอง) กับตรวจสอบภายใน

ความเป็นอิสระจากฝ่ายบริหารของตรวจสอบภายในจะทำให้มั่นใจได้ว่า ตรวจสอบภายในจะปราศจากอุปสรรคและอคติในการวางแผนและการทำงาน สามารถเข้าถึงบุคคลากร ทรัพยากร และข้อมูลที่ต้องการได้อย่างอิสระ ตรวจสอบภายในรับผิดชอบต่อองค์คณะผู้มีหน้าที่กำกับดูแล อย่างไรก็ตาม ความเป็นอิสระไม่ได้หมายความว่าต้องแยกตัวไปอยู่โดดเดี่ยว ตรวจสอบภายในจำเป็นต้องมีปฏิสัมพันธ์อย่างสม่ำเสมอ กับฝ่ายบริหารเพื่อที่จะมั่นใจได้ว่า งานของตรวจสอบภายในมีความเกี่ยวข้องและสอดคล้องกับความต้องการในทางกลยุทธ์และการปฏิบัติงานขององค์กรโดยผ่านทางกิจกรรมทั้งหมดของตรวจสอบภายใน ตรวจสอบภายในจะสั่งสมความรู้และความเข้าใจในองค์กร ซึ่งจะมีส่วนช่วยในการให้ความเชื่อมั่นและคำแนะนำในฐานะที่เป็นผู้ให้คำแนะนำที่ไว้วางใจได้และในฐานะที่เป็นหุ้นส่วนในทางกลยุทธ์ จำเป็นต้องมีการร่วมแรงร่วมใจและการสื่อสารในระหว่างผู้บริหารที่มีบทบาททั้งในด้านที่หนึ่งและด้านที่สอง กับตรวจสอบภายใน เพื่อที่จะเชื่อมั่นได้ว่า ไม่มีการทำงานซ้ำ การทับซ้อน หรือช่องว่าง โดยไม่จำเป็น

ระหว่างตรวจสอบภายในกับองค์คณะผู้มีหน้าที่กำกับดูแล

ตรวจสอบภายในรับผิดชอบต่อองค์คณะผู้มีหน้าที่กำกับดูแล และบางครั้งถูกเรียกว่าเป็น "หูเป็นตา" ขององค์คณะผู้มีหน้าที่กำกับดูแลด้วย

องค์คณะผู้มีหน้าที่กำกับดูแลมีหน้าที่ในการสอดส่องดูแลตรวจสอบภายใน ซึ่งจำเป็นต้องมี: การทำให้มั่นใจได้ว่า มีการจัดให้มีหน้าที่งานตรวจสอบภายในที่มีความเป็นอิสระซึ่งรวมถึงการว่าจ้างและการไล่ออกหัวหน้าหน่วยงานตรวจสอบภายใน (Chief Audit Executive -- CAE) การทำหน้าที่เป็นสายการรายงานเบื้องต้นสำหรับ CAE⁴ การอนุมัติ และจัดสรรทรัพยากรให้แก่แผนงานตรวจสอบ การรับและพิจารณารายงานจาก CAE และการให้สิทธิ CAE เข้าพบองค์คณะผู้มีหน้าที่กำกับดูแลได้อย่างอิสระ ซึ่งรวมถึงการเข้าพบเป็นการส่วนตัวโดยไม่มีผู้บริหารเข้าร่วม

คำศัพท์ที่สำคัญ

หัวหน้าหน่วยงานตรวจสอบภายใน

(Chief Audit Executive -- CAE) - บุคคลที่อาวุโสที่สุดในองค์กรที่มีความรับผิดชอบในการบริการตรวจสอบภายในซึ่งมักรู้จักกันในนามหัวหน้างานตรวจสอบภายในหรือตำแหน่งที่คล้ายกัน

4. เพื่อวัตถุประสงค์ในการบริหาร CAE อาจรายงานต่อผู้บริหารระดับสูงที่เหมาะสมด้วยก็ได้

ในท่ามกลางบทบาททั้งหมด

องค์คณะผู้มีหน้าที่กำกับดูแล ฝ่ายบริหาร และตรวจสอบภายใน มีภาระหน้าที่ที่แตกต่างกัน แต่กิจกรรมทั้งหมดจำเป็นต้องสอดคล้องกับวัตถุประสงค์ขององค์กร พื้นฐานสำหรับการเชื่อมโยงที่ประสบความสำเร็จก็คือ การประสานงาน การร่วมแรงร่วมใจ และการสื่อสารอย่างสม่ำเสมอ และมีประสิทธิภาพ

การประยุกต์ใช้โมเดล

โครงสร้าง บทบาท และภาระหน้าที่

โมเดลสามด้านจะมีประสิทธิผลมากที่สุดต่อเมื่อ ได้นำไปดัดแปลงให้สอดคล้องกับวัตถุประสงค์และสถานการณ์ขององค์กร องค์กรจะจัดโครงสร้างอย่างไร และบทบาทต่างๆ จะถูกมอบหมายให้ผู้ใดเป็นเรื่องที่ฝ่ายบริหารและองค์คณะผู้มีหน้าที่กำกับดูแลจะเป็นผู้กำหนด องค์คณะผู้มีหน้าที่กำกับดูแลอาจจะแต่งตั้งคณะอนุกรรมการเพิ่มเติมเพื่อดูแลบางแง่มุมซึ่งเป็นหน้าที่ขององค์คณะผู้มีหน้าที่กำกับดูแล เป็นต้นว่า ตรวจสอบ ความเสี่ยง การเงิน การวางแผน และการกำหนดค่าตอบแทน ภายในฝ่ายบริหารเอง ก็อาจมีการจัดหน้าทำงานและลำดับชั้นการบังคับบัญชา และมีแนวโน้มสู่ความเชี่ยวชาญเฉพาะด้านเพิ่มขึ้น ในขณะที่องค์กรมีขนาดและความซับซ้อนที่เติบโตขึ้น

หน้าทำงาน ทีม และแม้แต่บุคคลแต่ละคนอาจมีภาระหน้าที่ซึ่งมีบทบาททั้งในด้านที่หนึ่งและด้านที่สอง อย่างไรก็ตาม การสั่งการและการควบคุมดูแลของบทบาทในด้านที่สองอาจได้รับการออกแบบมาเพื่อรักษาระดับความเป็นอิสระจากบทบาทในด้านที่หนึ่ง (และแม้แต่เป็นอิสระจากฝ่ายบริหารระดับสูงสุด) ด้วยการกำหนดความรับผิดชอบหลักและสายการรายงานต่อองค์คณะผู้มีหน้าที่กำกับดูแล โมเดลสามด้านนี้ยินยอมให้มีสายการรายงานระหว่างผู้บริหารและองค์คณะผู้มีหน้าที่กำกับดูแลได้มากมายหลายสายเท่าที่ ต้องการ ในบางองค์กร อย่างเช่น สถาบันการเงินซึ่งถูกควบคุมจากทางการอย่างเห็นได้ชัดที่สุด จะมีข้อกำหนดจากทางการสำหรับการกำหนดสายการรายงานดังกล่าว เพื่อที่จะเชื่อมั่นได้ว่ามีความเป็นอิสระเพียงพอ แม้ในสถานการณ์เหล่านี้ ผู้บริหารที่มีบทบาทในด้านที่หนึ่งก็ยังคงมีหน้าที่ในการบริหารความเสี่ยง บทบาทในด้านที่สองอาจรวมถึง การเฝ้าระวังติดตามผล การให้คำแนะนำ ให้แนวทาง ทดสอบ วิเคราะห์ และรายงานประเด็นต่างๆ ที่เกี่ยวกับการบริหารความเสี่ยง ตรวจจับที่บทบาทเหล่านี้สนับสนุนและท้าทายผู้ที่มีบทบาทในด้านแรก และเป็นส่วนประกอบที่สำคัญในการตัดสินใจของฝ่ายบริหารและการดำเนินการต่างๆ บทบาทต่างๆ ในด้านที่สองเป็นส่วนหนึ่งในภาระหน้าที่ทางการบริหารและไม่เคยเป็นอิสระจากฝ่ายบริหารได้อย่างเต็มที่ไม่ว่าสายการรายงานและความรับผิดชอบจะเป็นเช่นใด

การกำหนดลักษณะของบทบาทในด้านที่สามให้เป็นอิสระจากฝ่ายบริหาร หลักการของโมเดลสามด้านนี้จะอธิบายถึงความสำคัญและลักษณะของความเป็นอิสระของตรวจสอบภายใน โดยการกำหนดให้ตรวจสอบภายในแยกออกไปจากหน้าที่งานอื่นๆ และการช่วยส่งเสริมคุณค่าที่โดดเด่นของการให้ความเชื่อมั่นและคำแนะนำ ความเป็นอิสระของตรวจสอบภายในจะได้รับการปกป้องด้วยการไม่ทำการตัดสินใจหรือดำเนินการใดๆ อันเป็นส่วนหนึ่งของภาระหน้าที่ในทางการบริหาร (ซึ่งรวมถึงการบริหารความเสี่ยง)

และด้วยการปฏิเสธที่จะให้ความเชื่อมั่นในกิจกรรมที่ตรวจสอบภายในมีหน้าที่อยู่ในปัจจุบัน หรือเคยทำหน้าที่นั้นมาไม่นาน ตัวอย่างเช่น ในบางองค์กร CAE ได้รับการร้องขอให้รับทำหน้าที่เพิ่มเติมในการตัดสินใจในกิจกรรมที่ต้องใช้ความสามารถคล้ายคลึงกัน เช่น ในเรื่องของการปฏิบัติตามกฎหมาย หรือการบริหารความเสี่ยงทั่วทั้งองค์กร (ERM) ในสถานการณ์เช่นนี้ ตรวจสอบภายในจะไม่เป็นอิสระจากหน่วยงานเหล่านี้หรือจากผลงานของหน่วยงานเหล่านี้ และดังนั้น เมื่อองค์กรคณะผู้มีหน้าที่กำกับดูแลจะแสวงหาความเชื่อมั่นและคำแนะนำที่เป็นอิสระและเที่ยงธรรมที่เกี่ยวข้องกับหน่วยงาน/ประเด็นนั้นๆ ก็จำเป็นต้องใช้บริการจากกลุ่มบุคคลที่สามที่มีคุณสมบัติเหมาะสม

การดูแลและการให้ความเชื่อมั่น

องค์กรคณะผู้มีหน้าที่กำกับดูแลพึงพิจารณาจากฝ่ายบริหาร (ซึ่งประกอบด้วยบทบาทที่อยู่ในด้านแรกและด้านที่สอง) ตรวจสอบภายใน และอื่นๆ เพื่อการกำกับดูแลและการบรรลุมิติประสงค์ซึ่งต้องรับผิดชอบต่อผู้มีส่วนได้เสีย ฝ่ายบริหารจะให้ความเชื่อมั่นที่มีค่า (บางทีก็เรียกว่าคำรับรอง -- attestations) เกี่ยวกับผลประกอบการที่วางแผนไว้ ที่เป็นจริง และที่คาดว่าจะเป็นอย่างนั้น เกี่ยวกับความเสี่ยงและการบริหารความเสี่ยง ด้วยการให้ประสบการณ์และความเชี่ยวชาญโดยตรง ส่วนพวกที่อยู่ในด้านที่สองจะให้ความเชื่อมั่นเพิ่มเติมในเรื่องที่เกี่ยวกับความเสี่ยง เนื่องจากตรวจสอบภายในมีความเป็นอิสระจากฝ่ายบริหาร ดังนั้น ความเชื่อมั่นที่ตรวจสอบภายในให้มาก็จะมีความเที่ยงธรรมและความเชื่อมั่นในระดับสูงสุดซึ่งสูงเกินกว่าพวกที่มีบทบาทอยู่ในด้านที่หนึ่งหรือสองจะสามารถให้แก่องค์กรคณะผู้มีหน้าที่กำกับดูแลได้ไม่ว่าสายการรายงานจะเป็นเช่นใด ความมั่นใจเพิ่มเติมอาจจะได้มาจากผู้ให้บริการภายนอกด้วยก็ได้

การประสานงานและเป็นไปในทิศทางเดียวกัน

การกำกับดูแลที่มีประสิทธิภาพนั้นจำเป็นต้องมีการมอบหมายภาระหน้าที่อย่างเหมาะสม รวมทั้งการจัดวางกิจกรรมต่างๆ อย่างเข้มข้นให้เป็นไปในทิศทางเดียวกันโดยผ่านทาง การร่วมมือ การร่วมแรงร่วมใจ และการสื่อสาร องค์กรคณะผู้มีหน้าที่กำกับดูแลแสวงหาความมั่นใจโดยผ่านทางตรวจสอบภายในว่า โครงสร้างและกระบวนการกำกับดูแลได้รับการออกแบบมาอย่างเหมาะสมและทำงานได้ตามต้องการ

เกี่ยวกับสมาคม

สมาคมผู้ตรวจสอบภายใน (IIA) เป็นหน่วยงานด้านการตรวจสอบภายในที่ได้รับการยอมรับอย่างกว้างขวางในการเป็นผู้ให้การสนับสนุนผู้ให้ความรู้ และผู้กำหนดมาตรฐาน แนวทางปฏิบัติต่างๆ และวุฒิบัตรรับรองคุณวุฒิต่างๆ ที่เกี่ยวข้องกับการวิชาชีพตรวจสอบภายใน สมาคมก่อตั้งขึ้นในปีพ.ศ. 2484 ในปัจจุบัน IIA ได้ให้บริการสมาชิกมากกว่า 200,000 คน จากมากกว่า 170 ประเทศและดินแดน สำนักงานใหญ่ของสมาคมตั้งอยู่ที่เลคแมรี่ (Lake Mary) มลรัฐฟลอริดา สหรัฐอเมริกา สำหรับข้อมูลเพิ่มเติมโปรดเยี่ยมชม www.globaliia.org

ข้อความปฏิเสธความผิดชอบ

IIA ตีพิมพ์เอกสารนี้เพื่อจุดประสงค์ในการให้ข้อมูลและเพื่อการศึกษาเท่านั้น และไม่ได้มีวัตถุประสงค์เพื่อให้คำตอบที่ชัดเจนที่สุดสำหรับสถานการณ์เฉพาะแต่ละสถานการณ์ ดังนั้น จึงมีวัตถุประสงค์เพียงเพื่อใช้เป็นแนวทางในการปฏิบัติงานเท่านั้น IIA จึงใคร่แนะนำให้ผู้่านขอคำปรึกษาจากผู้เชี่ยวชาญอิสระซึ่งมีความรู้เกี่ยวข้องโดยตรงกับสถานการณ์เฉพาะนั้นๆ IIA จะไม่รับผิดชอบใดๆ ต่อการที่ผู้ใดก็ตามเชื่อและอาศัยคำแนะนำนี้แต่เพียงอย่างเดียว

ลิขสิทธิ์

ลิขสิทธิ์ © สมาคมผู้ตรวจสอบภายใน พ.ศ. 2563 หากต้องการขออนุญาตทำซ้ำ โปรดติดต่อ copyright@theiia.org

เมษายน 2563



Global

Global Headquarters

The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 149
Lake Mary, FL 32746, USA
Phone: +1-407-937-1111
Fax: +1-407-937-1101
www.globaliia.org