แนวทางการตรวจสอบเทคโนโลยีในระดับสากล (GTAG)

กรอบการปฏิบัติงานวิชาชีพตรวจสอบภายในระดับสากล – แนวทางปฏิบัติ

การป้องปรามและการตรวจสอบทุจริตในโลกเทคโนโลยีอัตโนมัติ

สารบัญ

คำนำ

บทสรุปผู้บริหาร

1. บทนำ

1.1 คำจำกัดความของการทุจริต

1.2 มาตรฐานของ IIA ที่เกี่ยวข้องกับการทุจริต

1.3 การใช้เทคโนโลยีในการป้ องกันและตรวจจับการทุจริต

2. ความเสี่ยงจากการทุจริตด้านเทคโนโลยีสารสนเทศ

2.1 การประเมินความเสี่ยงจากการทุจริตด้านเทคโนโลยีสารสนเทศ

2.2 วิธีการประเมินการทุจริต

2.3 การทุจริตด้านเทคโนโลยีสารสนเทศ

3. การตรวจจับการทุจริตโดยใช้การวิเคราะห์ข้อมูล

3.1 เหตุใดจึงใช้การวิเคราะห์ข้อมูลเพื่อตรวจจับการทุจริต

3.2 เทคนิคการวิเคราะห์สำหรับการตรวจจับการทุจริต

3.3 ประเภทของการทดสอบการทุจริต

3.4 การวิเคราะห์ข้อมูลเต็มจำนวนของประชากรทั้งหมด

3.5 กลยุทธ์การใช้แผนการป้องกันและตรวจจับการทุจริตและ

3.6 การวิเคราะห์ข้อมูลโดยใช้แหล่งข้อมูลจากภายในและภายนอก

4. บทบาทของ CAE ในการรับมือกับการทุจริตด้านเทคโนโลยีสารสนเทศ

4.1 คณะอนุกรรมการตรวจสอบ

4.2 คำถาม 20 ข้อเกี่ยวกับการทุจริต**ที่ CAE** ควรถาม

อ้างอิงและแหล่งที่มา

ผู้เขียน

คำนำ

ความก้าวหน้าทางเทคโนโลยีที่ไม่เคยหยุดนิ่งทำให้ทุกสิ่งทุกอย่างที่เราพบเห็นในปัจจุบันผูกติดเข้ากับกับเทคโนโลยีอย่างแยกไม่ออก ไม่ว่าจะในองค์กรหรืออุตสาหกรรมใด เทคโนโลยีสารสนเทศล้วนเป็นปัจจัยสำคัญในการดำรงไว้ซึ่งความสามารถในการแข่งขัน การบริหารความเสี่ยงและการดำเนินการเพื่อให้บรรลุวัตถุประสงค์ทางธุรกิจ องค์กรทั่วโลกจึงต่างทุ่มเททรัพยากรจำนวนมากให้กับโครงการด้านเทคโนโลยีที่สำคัญ

ในขณะที่เทคโนโลยีมีความก้าวหน้ามากขึ้นนั้น การกระทำทุจริตก็มีความซับซ้อนยิ่งขึ้นเช่นเดียวกัน การพึ่งพาเทคโนโลยีอัตโนมัติในการทำธุรกิจนี้ก่อให้เกิดความท้าทายใหม่ๆ ในการตรวจสอบและป้องปรามการทุจริต

ตามการบัญญัติของ Black's Law Directory การทุจริตประกอบด้วย "วิธีการต่างๆ ทั้งหมดที่คิดค้นขึ้นด้วยปัญญาของมนุษย์เพื่อแสวงหาประโยชน์จากผู้อื่น โดยการให้ข้อมูลเท็จหรือปกปิดความจริงไว้" การทุจริตสร้างความเสียหายอย่างใหญ่หลวงแก่องค์กรและส่งผลเสียต่อเศรษฐกิจ เทคโนโลยีช่วยให้ผู้ทำการทุจริตดำเนินการและปกปิดการทุจริตแบบเดิมๆ ได้ง่ายขึ้น ตัวอย่างเช่น ผู้ทำการทุจริตสามารถปลอมแปลงเอกสารได้โดยง่าย เช่น ออกใบแสดงรายการทางบัญชีเพื่อหลอกลวงผู้อื่น

แต่เทคโนโลยีก็ใช้เป็นเครื่องมือช่วยป้องปรามและตรวจสอบทุจริตได้เช่นกัน องค์กรสามารถลดเวลาที่ใช้ในการตรวจสอบทุจริตซึ่งจะช่วยลดความเสียหายได้โดยการใช้เทคโนโลยีโปรแกรมป้องกันการทุจริตแบบตามเวลาที่เกิดขึ้นจริง (realtime) และเครื่องมือตรวจสอบทุจริตขั้นสูง

ดังนั้นผู้ตรวจสอบภายในจำเป็นต้องมีความรู้ด้านเทคโนโลยีและมีเครื่องมือต่างๆ ที่เหนือชั้นกว่าผู้ทำการทุจริต ด้วยซอฟต์แวร์ที่พร้อมใช้งานได้ทันที การใช้คอมพิวเตอร์เพื่อตรวจหาร่องรอยการทุจริตทางบัญชีจึงไม่เพียงแต่เป็นประโยชน์เท่านั้น แต่จะเป็นสิ่งที่จำเป็นอย่างยิ่งที่จะช่วยให้ผู้ตรวจสอบทำหน้าที่ตรวจสอบได้อย่างอิสระ

ด้วยเหตุผลดังกล่าว ข้าพเจ้ารู้สึกยินดีเป็นอย่างยิ่งที่สมาคมผู้ตรวจสอบภายใน (Institute of Internal Auditors: IIA) ได้เผยแพร่ GTAG 13: การป้องปรามและการตรวจสอบทุจริตในโลกเทคโนโลยีอัตโนมัติ (Fraud Prevention and Detection in an Automated World) ซึ่งแนวทางที่เหมาะสมกับโลกปัจจุบัน ฉบับนี้อธิบายถึงภาพรวมของเทคนิคในการดำเนินการร่วมกับทีมงานต่างๆ และผู้บริหารในการประเมินความเสี่ยงที่เกี่ยวข้องกับการทุจริตในสภาวะที่เทคโนโลยีมีความก้าวหน้าอย่างมาก แนวทางฉบับนี้ประกอบด้วย

- คำอธิบายเกี่ยวกับการวิเคราะห์ข้อมูลหลากหลายประเภทเพื่อตรวจสอบทุจริต.
- ความเสี่ยงจากการทุจริตด้านเทคโนโลยีสารสนเทศในรูปแบบต่างๆ
- รูปแบบการประเมินความเสี่ยงในการทุจริตด้านเทคโนโลยี

ขาพเจ้าขอให้ทุกท่านใช้แนวทางที่เป็นทางการฉบับนี้ในการเสริมสร้างความรู้เกี่ยวกับการบูรณาการระหว่างเทคโนโลยีและการทุจริต เพราะจะมีส่วนช่วยให้องค์กรของท่านประสบความสำเร็จในการตรวจสอบทุจริตได้อย่างแน่นอน

Scott Grossfeld CFE, CPA
Chief Executive Officer
Association of Certified Fraud Examiners

บทสรุปผู้บริหาร

การทุจริต คือ ความเสี่ยงทางธุรกิจที่ผู้บริหารโดยเฉพาะหัวหน้าผู้บริหารงานตรวจสอบภายใน (chief audit executives: CAEs) ต้องหาวิธีรับมือด้วยมาโดยตลอด หนังสือพิมพ์หลายฉบับพาดหัวข่าวเรื่องราวอื้อฉาวและการกระทำผิดในบรรษัทต่างๆ ซึ่งชี้ให้เห็นว่าองค์กรและภาครัฐจำเป็นต้องยกระดับการกำกับดูแลตลอดจนการควบคุมดูแลให้ดียิ่งขึ้น การรับมือกับความเสี่ยงด้านการทุจริตในองค์กรอย่างมีประสิทธิภาพและประสิทธิผลเป็นข้อกังวลหลักของคณะกรรมการบริษัท ผู้บริหาร เจ้าของกิจการ ผู้ตรวจสอบภายใน ผู้นำรัฐบาล ฝ่ายนิติบัญญัติ หน่วยงานกำกับดูแล และผู้มีส่วนได้ส่วนเสียอื่นๆ อีกหลายฝ่าย ในหลายกรณี กฎหมายและระเบียบข้อบังคับที่ออกใหม่จากทั่วโลกได้กำหนดให้องค์กรดูแลปัญหาที่มีมายาวนานนี้

แม้ว่าหน่วยงานตรวจสอบภายในหลายแห่งจะประสบปัญหาด้านงบประมาณ กำลังคนที่มีจำกัด และปริมาณงานที่ล้นมือ แต่ผู้ที่อยู่ในวิชาชีพตรวจสอบภายในในปัจจุบันก็ถูกคาดหวังให้มีบทบาทเชิงรุกในการช่วยองค์กรบริหารความเสี่ยงจากการทุจริตโดยดำเนินการให้แน่ใจว่ามีการควบคุมอย่างเหมาะสมเพื่อป้องปรามและตรวจสอบทุจริต CAE ต้องเผชิญกับความท้าทายในการใช้ทรัพยากรที่มีอยู่ให้มีประสิทธิผลและประสิทธิภาพ เพื่อตอบสนองความคาดหวังของผู้บริหาร เจ้าของธุรกิจ และคณะกรรมการบริษัท ดังนั้น ผู้ตรวจสอบภายในจึงต้องมีทักษะที่เหมาะสมและควรใช้เครื่องมือทางเทคโนโลยีที่มีอยู่ในการรักษาไว้ซึ่งความมีประสิทธิผลของโปรแกรมการจัดการการทุจริตที่ครอบคลุมถึงการป้องกัน การตรวจจับ และการสอบสวน ผู้ตรวจสอบภายในทุกด้าน มิใช่เฉพาะผู้เชี่ยวชาญด้านการตรวจสอบเทคโนโลยีสารสนเทศ จึงต้องมีความรู้ความสามารถมากยิ่งขึ้น เช่นในเรื่องการวิเคราะห์ข้อมูลและการใช้เทคโนโลยีเพื่อช่วยให้สามารถปฏิบัติงานได้บรรลุตามเป้าหมาย

นอกจากการประเมินความเพียงพอของการควบคุมภายในแล้ว ความท้าทายของผู้ตรวจสอบภายในคือ การมองให้ลึกไปมากกว่าการควบคุมและการหาช่องโหว่ในระบบที่อาจเกิดการทุจริตขึ้นได้ ผู้ตรวจสอบภายในสามารถปรับใช้การคิดเชิงวิเคราะห์เพื่อระบุถึงเรื่องที่มีความเสี่ยงสูงและเจาะลึกลงไปที่ธุรกรรมเฉพาะอย่างได้ หากมีความเข้าใจในความสัมพันธ์ของระบบและระบบงาน (application) ด้านเทคโนโลยีสารสนเทศที่แตกต่างกัน

GTAG ฉบับนี้ มีวัตถุประสงค์ เพื่อให้แนวทางเพิ่มเติมจาก Practice Guide ของสมาคมผู้ตรวจสอบภายใน (Institute of Internal Auditors: IIA) ว่าด้วยเรื่อง การตรวจสอบภายในและการทุจริต (Internal Auditing and Fraud) และเพื่อให้ข้อมูลและคำแนะนำแก่ CAE และผู้ตรวจสอบภายในในการใช้เทคโนโลยีเพื่อช่วยป้องกัน ตรวจจับ และรับมือกับการทุจริต แนวทางฉบับนี้มุ่งเน้นที่ความเสี่ยงจากการทุจริตด้านเทคโนโลยีสารสนเทศ รวมทั้งการประเมินความเสี่ยงดังกล่าว และยังอธิบายว่าจะใช้เทคโนโลยีช่วยผู้ตรวจสอบภายใน และผู้มีส่วนได้เสียหลักอื่นๆ ภายในองค์กรรับมือกับการทุจริตและความเสี่ยงจากการทุจริตได้อย่างไร

1. บทนำ

วัตถุประสงค์ของบทนี้คือ การนำเสนอมาตรฐานต่างๆ ที่เกี่ยวข้องกับการทุจริตที่ตีพิมพ์ไว้ในกรอบโครงสร้างการปฏิบัติงานวิชาชีพตรวจสอบภายในในระดับสากล (International Professional Practices Framework: IPPF) ของ IIA และยังได้ให้ความหมายของการทุจริต ตลอดจนเสนอภาพรวมในการใช้เทคโนโลยีเพื่อเพิ่มประสิทธิภาพในการป้องปรามและการตรวจสอบทุจริตอีกด้วย

1.1 คำจำกัดความของการทุจริต

การทุจริต หมายรวมถึงการกระทำที่ไม่ถูกต้องและผิดกฎหมายในหลายลักษณะ ซึ่งเกิดจากการตั้งใจหลอกลวงหรือบิดเบือนความจริง IPPF ได้ระบุความหมายของคำว่า *การทุจริต* ไว้ดังนี้

> *"... การกระทำใดๆ ที่ผิดกฎหมายโดยการหลอกลวง การปกปิดหรือการทำลายความไว้วางใจ การกระทำเหล่านี้มีความเกี่ยวข้องกับการข่มขู่คุกคามโดยใช้ความรุนแรงหรือใช้กำลัง การทุจริตกระทำขึ้นโดยบุคคลและองค์กรเพื่อให้ได้มาซึ่งเงิน ทรัพย์สิน หรือบริการ เพื่อหลีกเลี่ยงการจ่ายเงินหรือการสูญเสียการบริการ หรือเพื่อรักษาความได้เปรียบส่วนบุคคลหรือของธุรกิจ"*

ความหมายอย่างกว้างของการทุจริตนี้รวมถึงความเสี่ยงจากการทุจริต การเปิดรับ และการคุกคามที่หน่วยงานเทคโนโลยีสารสนเทศอาจต้องเผชิญ ตลอดจนการทุจริตที่เกิดจากการใช้เทคโนโลยี

1.2 มาตรฐานของ IIA ที่เกี่ยวข้องกับการทุจริต

ตามที่ระบุไว้ใน Practice Guide ของ IIA เรื่อง การตรวจสอบภายในและการทุจริต (Internal Auditing and Fraud) IIA ได้รวมมาตรฐานต่างๆ ที่เกี่ยวข้องโดยตรงกับการทุจริตไว้ใน IPPF มาตรฐานต่อไปนี้ครอบคลุมถึงบทบาทและความรับผิดชอบของผู้ตรวจสอบภายในที่เกี่ยวข้องกับการทุจริตภายในองค์กร

> **1210.A2 –** ผู้ตรวจสอบภายในต้องมีความรู้ที่เพียงพอในการประเมินความเสี่ยงจากการทุจริตและวิธีการที่องค์กรจะจัดการกับความเสี่ยงนี้ แต่อาจไม่จำเป็นต้องมีความเชี่ยวชาญเท่ากับบุคลากรที่มีความรับผิดชอบหลักในการตรวจสอบและสอบสวนการทุจริต
>
> **1220.A1 –** ผู้ตรวจสอบภายในต้องใช้ความระมัดระวังเยี่ยงผู้ประกอบวิชาชีพในการพิจารณาเรื่องต่อไปนี้
>
> - ขอบเขตของงานที่จำเป็นต่อการบรรลุวัตถุประสงค์ของงานตรวจสอบ
> - ความซับซ้อน สาระสำคัญ หรือนัยสำคัญของเรื่องที่ต้องมีกระบวนการให้ความเชื่อมั่น
> - ความเพียงพอและประสิทธิผลของการกำกับดูแล การบริหารความเสี่ยง และกระบวนการควบคุม

- ความเป็นไปได้ของความผิดพลาดที่มีนัยสำคัญ การทุจริต หรือการไม่ปฏิบัติตามระเบียบข้อบังคับ
- ค่าใช้จ่ายในการสร้างความเชื่อมั่นที่เกี่ยวเนื่องกับประโยชน์ที่อาจได้รับ

2060 – การรายงานต่อผู้บริหารระดับอาวุโสและคณะกรรมการ – CAE ต้องรายงานถึงวัตถุประสงค์ อำนาจ ความรับผิดชอบ และผลการดำเนินงานตามแผนการตรวจสอบภายในแก่ผู้บริหารระดับอาวุโสและคณะกรรมการเป็นระยะ โดยการรายงานนั้นควรกล่าวถึงโอกาสที่จะเกิดและการควบคุมความเสี่ยงที่มีนัยสำคัญ รวมถึงความเสี่ยงจากการทุจริต ประเด็นด้านการกำกับดูแลและประเด็นอื่นที่ผู้บริหารระดับอาวุโสและคณะกรรมการกำหนด

2120.A2 – กิจกรรมการตรวจสอบภายในต้องประเมินความเป็นไปได้ที่จะเกิดการทุจริตและวิธีการขององค์กรในการจัดการกับความเสี่ยงดังกล่าว

2210.A2 – ผู้ตรวจสอบภายในต้องพิจารณาความเป็นไปได้ของความผิดพลาด การทุจริต การไม่ปฏิบัติตามระเบียบข้อบังคับ และความเสี่ยงอื่นที่มีนัยสำคัญ เมื่อกำหนดวัตถุประสงค์ของงานตรวจสอบ

1.3 การใช้เทคโนโลยีในการป้องปรามและตรวจสอบการทุจริต

ความก้าวหน้าของเทคโนโลยีช่วยให้องค์กรดำเนินการควบคุมแบบอัตโนมัติเพื่อช่วยป้องปรามและตรวจสอบทุจริตได้มากขึ้น เทคโนโลยียังช่วยให้องค์กรเปลี่ยนจากเทคนิคการติดตามดูแลการทุจริตเป็นระยะหรือเป็นประจำ เช่นการควบคุมแบบสืบค้น เป็นเทคนิคการควบคุมดูแลการทุจริต แบบตามเวลาที่เกิดขึ้นจริง (real-time) และต่อเนื่องโดยสม่ำเสมอซึ่งสามารถป้องกันมิให้เกิดการทุจริตขึ้นได้อย่างแท้จริง แนวทาง GTAG ฉบับนี้จะอธิบายถึงเทคนิคการตรวจสอบทั้งแบบต่อเนื่องและเป็นระยะ ในปัจจุบัน มีซอฟต์แวร์สำเร็จรูปสำหรับการวิเคราะห์ขั้นสูงจำนวนมากที่สามารถช่วยวิเคราะห์ข้อมูลได้ ซึ่งแนวทาง GTAG นี้จะกล่าวถึงเทคนิคโดยทั่วไป มิได้รับรองโปรแกรมใดเป็นพิเศษ

มีเทคโนโลยีและซอฟต์แวร์สำเร็จรูปที่ใช้ในการตรวจสอบคอมพิวเตอร์ที่จะช่วยในการตรวจสอบการทุจริต ซึ่งคอมพิวเตอร์อาจถูกใช้เป็นเครื่องมือกระทำการทุจริต หรืออาจใช้เพื่อบ่งชี้สัญญาณเตือนถึงแนวโน้มเกิดการทุจริต การตรวจสอบทุจริตทางคอมพิวเตอร์คือ การดำเนินการสอบสวนที่รวมถึงการรักษาไว้ การบ่งชี้ การแยกย่อยข้อมูลและการจัดทำเอกสารกำกับที่เกี่ยวข้องกับฮาร์ดแวร์คอมพิวเตอร์และข้อมูลเพื่อใช้เป็นหลักฐานและใช้ในการวิเคราะห์ต้นเหตุของปัญหา ตัวอย่างของกิจกรรมดังกล่าว มีดังต่อไปนี้

- การกู้คืนจดหมายอิเล็กทรอนิกส์ที่ลบทิ้งไปแล้ว
- การติดตามตรวจสอบจดหมายอิเล็กทรอนิกส์เพื่อหาข้อบ่งชี้ถึงการทุจริต
- การดำเนินการสอบสวนภายหลังการเลิกจ้าง
- การกู้คืนหลักฐานหลังจากการฟอร์แมทฮาร์ดดิสก์

กิจกรรมการตรวจสอบการทุจริตทางคอมพิวเตอร์ช่วยสร้างและรักษาไว้ซึ่งการควบคุมดูแลระบบอย่างต่อเนื่อง ซึ่งอาจจำเป็นสำหรับการพิจารณายอมรับเป็นหลักฐานในชั้นศาล แม้ว่า CAE และผู้ตรวจสอบภายในไม่จำเป็นต้องเป็นผู้เชี่ยวชาญในด้านนี้ แต่ CAE ก็ควรมีความเข้าใจในประโยชน์ของเทคโนโลยี เพื่อให้สามารถประสานงานกับผู้เชี่ยวชาญที่เหมาะสมได้ในกรณีที่จำเป็น เพื่อให้ความช่วยเหลือในการสอบสวนการทุจริต

2. ความเสี่ยงจากการทุจริตด้านเทคโนโลยีสารสนเทศ

วัตถุประสงค์ของบทนี้คือ การให้ข้อมูลเกี่ยวกับการทุจริตด้านเทคโนโลยีสารสนเทศในกรณีต่างๆ ที่อาจเกิดขึ้นภายในองค์กร แม้ว่าผู้บริหารในสายงานตรวจสอบภายใน คณะกรรมการบริษัทและผู้บริหารอาจมีความรู้เกี่ยวกับความเสี่ยงในการทุจริตด้านเทคโนโลยีสารสนเทศที่อาจเกิดขึ้นเป็นกรณีเฉพาะในองค์กรของตนแล้ว เนื้อหาในบทนี้จะอธิบายถึงประเภทของการทุจริตโดยทั่วไป ดังนั้นจึงอาจไม่ได้กล่าวถึงกรณีเฉพาะของอุตสาหกรรมหรือองค์กรใดเป็นพิเศษ

2.1 การประเมินความเสี่ยงจากการทุจริตด้านเทคโนโลยีสารสนเทศ

ตาม Practice Guide ของ IIA ในหัวข้อ *การตรวจสอบภายในและการทุจริต* ได้ระบุไว้ว่า ทุกองค์กรมีโอกาสที่จะเกิดความเสี่ยงในการทุจริตด้านเทคโนโลยีสารสนเทศได้ในทุกกระบวนการทำงานที่มนุษย์จำเป็นต้องเข้าไปเกี่ยวข้อง การที่องค์กรต้องเผชิญกับการทุจริตนั้น ถือเป็นความเสี่ยงแฝงที่มีอยู่ในธุรกิจ ซึ่งจะมากน้อยเพียงใดขึ้นอยู่กับประสิทธิผลของการควบคุมภายในเพื่อป้องปรามหรือตรวจสอบการทุจริตที่มีอยู่ รวมทั้งความซื่อสัตย์และความโปร่งใสของผู้ที่เกี่ยวข้องในกระบวนการ ความเสี่ยงในการทุจริตและโอกาสที่จะเกิดความเสี่ยงนี้อาจเกิดขึ้นกับงานด้านเทคโนโลยีสารสนเทศบ่อยครั้งเช่นเดียวกับสายงานอื่นๆ ในองค์กร

Risk management standard (2120.A2) ที่กำหนดไว้ใน IPPF ระบุว่า กิจกรรมการตรวจสอบภายในต้องประเมินความเป็นไปได้ในการเกิดการทุจริตและวิธีการที่องค์กรจะจัดการกับความเสี่ยงนั้น แม้ว่าจะมีวิธีการดำเนินการตามมาตรฐานดังกล่าวอยู่หลายวิธี แต่ผู้ตรวจสอบภายในก็ต้องตรวจสอบว่ามีการดำเนินการดังต่อไปนี้หรือไม่

- ผู้บริหารได้ประเมินความเสี่ยงในการทุจริตภายในองค์กร
- การประเมินดังกล่าวครอบคลุมทุกสายงานที่มีความสำคัญ
- องค์ประกอบหลักต่างๆ เช่น ความเสี่ยงจากการทุจริต การควบคุม และช่องโหว่ ได้รับการบันทึกเป็นลายลักษณ์อักษร
- มีกระบวนการในการแก้ไขปัญหา

การประเมินความเสี่ยงจากการทุจริตด้านเทคโนโลยีสารสนเทศมักเป็นองค์ประกอบหนึ่งของโปรแกรมการบริหารความเสี่ยงระดับทั่วทั้งองค์กร เนื่องจากผู้บริหารเป็นผู้รับผิดชอบการบริหารความเสี่ยงทั่วทั้งองค์กร (enterprise risk management: ERM) ผู้บริหารด้านเทคโนโลยีสารสนเทศจึงควรมุ่งเน้นที่เรื่องการประเมินความเสี่ยงจากการทุจริตด้านเทคโนโลยีสารสนเทศ ในหลายองค์กร ผู้ตรวจสอบภายในอาจได้รับมอบหมายให้มีส่วนร่วมในกิจกรรมเหล่านี้ด้วย เนื่องจากมีทักษะเฉพาะในการบ่งชี้และประเมินความเสี่ยง การประเมินความเสี่ยงจากการทุจริตด้านเทคโนโลยีสารสนเทศเป็นเครื่องมือที่ช่วยให้ผู้บริหารงานด้านเทคโนโลยีสารสนเทศและผู้ตรวจสอบภายในสามารถบ่งชี้ได้อย่างเป็นระบบว่า อาจเกิดการทุจริตได้ตรงจุดไหนอย่างไร และมีใครที่อาจกระทำการทุจริตได้ การสอบทานโอกาสที่จะเกิดความเสี่ยงจากการทุจริตเป็นขั้นตอนสำคัญ ในการลดความกังวลของผู้บริหารด้าน

เทคโนโลยีสารสนเทศเกี่ยวกับความเสี่ยงจากการทุจริตด้านเทคโนโลยีสารสนเทศ เช่นเดียวกับการบริหารความเสี่ยงขององค์กร การประเมินความเสี่ยงจากการทุจริตด้านเทคโนโลยีสารสนเทศมุ่งเน้นที่การดำเนินการทุจริตและเหตุการณ์การทุจริต เพื่อกำหนดให้มีการควบคุมภายใน และพิจารณาว่าจะมีโอกาสเกิดการหลีกเลี่ยงการควบคุมนั้นได้หรือไม่

การประเมินความเสี่ยงจากการทุจริตด้านเทคโนโลยีสารสนเทศ โดยทั่วไปมีขั้นตอนการดำเนินการต่อไปนี้

- การบ่งชี้ปัจจัยความเสี่ยงในการทุจริตด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้อง
- การบ่งชี้การทุจริตด้านเทคโนโลยีสารสนเทศที่อาจเกิดขึ้นและจัดลำดับความสำคัญตามความเป็นไปได้และผลกระทบ
- การจัดวางระบบการควบคุมในปัจจุบันให้รับกับโอกาสที่จะเกิดการทุจริต และการบ่งชี้ช่องโหว่
- การทดสอบความมีประสิทธิผลของการควบคุมการป้องปรามและการตรวจสอบทุจริต
- การประเมินความเป็นไปได้และผลกระทบทางธุรกิจจากการเกิดความล้มเหลวในการควบคุมและ/หรือการทุจริต

เนื้อหาต่อไปนี้ เป็นตัวอย่างรูปแบบของการประเมินความเสี่ยงจากการทุจริตด้านเทคโนโลยีสารสนเทศ

ตาราง 1 ตัวอย่างรูปแบบการประเมินความเสี่ยงจากการทุจริตด้านเทคโนโลยีสารสนเทศ

ผู้รับผิดชอบหน่วยธุรกิจ	ความเสี่ยงจากการทุจริต	การควบคุม	ก้าวม ปรามหรือการตรวจสอบ	การติดตามดูแล	ความเป็นไปได้	ผลกระทบ
IT-CIO	อุปกรณ์ฮาร์ดแวร์ด้านเทคโนโลยีสารสนเทศได้รับการควบคุมทางกายภาพไม่เพียงพอ ส่งผลให้เกิดการเปลี่ยนแปลง ความเสียหาย หรือการยักยอกเพื่อผลประโยชน์ส่วนตัว (ความมั่นคงทางกายภาพ)	● ฮาร์ดแวร์คอมพิวเตอร์ที่สำคัญได้รับการติดตั้งในศูนย์คอมพิวเตอร์ที่มีความปลอดภัย ● กำหนดการเข้าถึงศูนย์คอมพิวเตอร์ตามหน้าที่งานที่รับผิดชอบ ● ใช้รูปแบบการรักษาความปลอดภัยที่หลากหลาย (เช่น ควบคุมการเข้าถึงด้วยคีย์การ์ด ติดตั้งกล้องวงจรปิด มีเจ้าหน้าที่รักษาความปลอดภัย) ● จัดทำนโยบายและขั้นตอนการดำเนินงานเป็นลายลักษณ์อักษร ● มีการเก็บข้อมูลปูมบันทึกผู้มาเยี่ยมชม (visitor logs) ● มีสายเคเบิลรักษาความปลอดภัยสำหรับคอมพิวเตอร์แบบพกพา. ● มีการทำทะเบียนทรัพย์สินในแต่ละสถานีงาน (workstations) เป็นรายไตรมาส ● มีกระบวนการสำรองเผื่อผู้ใช้อย่างเป็นทางการ	ทั้งสองแบบ	● การบริหารศูนย์คอมพิวเตอร์. ● การป องกันการสูญเสีย ● การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ● การปฏิบัติการด้านเทคโนโลยีสารสนเทศ ● ผู้บริหารควบคุมดูแลปูมบันทึกผู้มาเยี่ยมชมทุกวัน ● มีการจัดทำทะเบียนทรัพย์สินเป็นระยะ ๆ ● มีการพิสูจน์ยอดทางการเงินที่เตรียมการไว้ ● การตรวจสอบภายใน	ต่ำ	สูง
IT-CIO	การเข้าถึงระบบหรือข้อมูลเพื่อประโยชน์ส่วนตัว (การเข้าถึงระบบทางตรรกะ) a) การเข้าถึงข้อมูลส่วนตัวของลูกค้าหรือพนักงาน (เช่น ข้อมูล	● การบริหารการระบุตัวตน - กำหนดรหัสผู้ใช้รายบุคคล - มีข้อบังคับในการกำหนดรหัสผ่านที่มีความซับซ้อนโดยอัตโนมัติ - การหมุนเวียนรหัสผ่าน ● การควบคุมการเข้าถึง	ทั้งสองแบบ	● การรักษาความมั่นคงปลอดภัยด้านข้อมูลสารสนเทศ ● ผู้ดูแลระบบ ● ผู้รับผิดชอบหน่วยธุรกิจ ● การตรวจสอบภายใน	ปานกลาง	สูง

	บัตรเครดิต ข้อมูลเงินเดือน) (การสวมรอยบุคคล) b) การเข้าถึงข้อมูลความลับของบริษัท (เช่น รายงานทางการเงิน ข้อมูลผู้ขายหรือผู้ให้บริการ และแผนกลยุทธ์) c) การคัดลอกและการใช้ซอฟต์แวร์หรือข้อมูลเพื่อการเผยแพร่ d) มีการเข้าถึงปูมบันทึกการตรวจสอบหรือเครื่องมือติดตามดูแลอื่นที่ใช้ในการตรวจจับปัญหาเพื่อแก้ไข e) การใช้งานเครือข่ายโทรคมนาคมในทางที่ผิด	● การควบคุมการพิสูจน์ตัวตนที่แท้จริง ● การควบคุมอำนาจอนุมัติ - ผู้รับผิดชอหน่วยธุรกิจอนุมัติการเข้าถึงข้อมูล - รายชื่อการควบคุมการเข้าถึง ● จัดทำนโยบายและขั้นตอนเป็นลายลักษณ์อักษร ● การแบ่งหน้าที่ความรับผิดชอบ ● ทีมงานดูแลรับมือกับเหตุการณ์เกี่ยวกับคอมพิวเตอร์ ● การควบคุมเครือข่าย (เช่น ไฟร์วอลล์และอุปกรณ์กำหนดเส้นทางในระบบเครือข่าย (routers)) ● การเข้าถึงระบบหรือข้อมูลจากระยะไกล (remote access) ที่ปลอดภัย ● การบริหารการป้ องกันไวรัสและซอฟต์แวร์ที่ใช้แก้ไขเพื่อควบคุมช่องโหว่ทางคอมพิวเตอร์ ● การควบคุมรหัสของผู้ดูแลระบบ ● ดำเนินการทดสอบ การบุกรุกเข้าเครือข่าย ● การประเมินช่องโหว่ของซอฟต์แวร์เป็นระยะ ● ขั้นตอนการยกเลิกสิทธิในการเข้าถึงทรัพยากรของเครือข่ายของพนักงานที่สิ้นสุดการจ้างงานไปแล้ว ● การกระทบยอดทางบัญชีและการสอบทาน ● มีการจัดทำปูมบันทึกการฝ าฝืนการรักษาความมั่นคงปลอดภัยและพร้อมให้สอบทานได้ตลอดเวลา ● การจำกัดขอบเขตการเข้าถึงรหัสซอฟต์แวร์ ● ใช้ข้อมูลสมมุติสำหรับการทดสอบ				

		ระบบ ● มีการกำหนดช่องทางเฉพาะและการเข้ารหัสสำหรับการส่งข้อมูลส่วนบุคคล ● มีการเข้ารหัส Secure Sockets Layer (SSL) สำหรับธุรกรรมออนไลน์				
IT-CIO	การเปลี่ยนแปลงโปรแกรมระบบหรือข้อมูลเพื่อผลประโยชน์ส่วนตัว (การบริหารการเปลี่ยนแปลง)	● ขั้นตอนการพัฒนาระบบและบริหารโครงการ ● ขั้นตอนการบริหารการเปลี่ยนแปลงระบบ ● การแบ่งหน้าที่ความรับผิดชอบ ● การจำกัดขอบเขตการเข้าถึงสภาพแวดล้อมที่ใช้งานจริง ● การเปลี่ยนแปลงระบบต้องได้รับการอนุมัติจากผู้บริหาร ● การจำกัดขอบเขตการเข้าถึงรหัสซอฟต์แวร์ ● การกระทบยอดทางบัญชีและการสอบทาน	ทั้งสองแบบ	● ผู้บริหารด้านเทคโนโลยีสารสนเทศ ● ผู้ดูแลงานระบบ ● ผู้รับผิดชอบหน่วยธุรกิจ ● ผู้บริหารด้านการเงิน ● การตรวจสอบภายใน	ต่ำ	ปานกลาง
IT-CIO	กิจกรรมการทุจริตที่กระทำโดยผู้รับจ้างอิสระที่ให้บริการหรือโปรแกรมเมอร์ในต่างประเทศ (เช่น ใบแจ้งหนี้ปลอม การยักยอกข้อมูลความลับของพนักงาน ลูกค้า หรือองค์กร เพื่อประโยชน์ส่วนตัว)	● เงื่อนไขตามสัญญา (เช่น ข้อมูลลับ การไม่เปิดเผยความลับ การส่งคืนข้อมูลลับ สิทธิในการตรวจสอบ) ● การจำกัดขอบเขตการเข้าถึงโดยพิจารณาจากหน้าที่งาน ● การควบคุมการเข้าถึง (เช่น การพิสูจน์ตัวตนที่แท้จริงและการอนุมัติ) ● มีการจัดทำปูมบันทึกการฝ าฝืนการรักษาความมั่นคงปลอดภัยและพร้อมให้สอบทานได้ตลอดเวลา ● มีการกระทบยอดทางบัญชีและการสอบทาน ● มีการสอบทานค่าใช้จ่ายสำหรับผู้	ทั้งสองแบบ	● ผู้บริหารด้านเทคโนโลยีสารสนเทศ ● การรักษาความมั่นคงปลอดภัยด้านข้อมูลสารสนเทศ. ● การป องกันการสูญเสีย ● การตรวจสอบภายใน	ต่ำ	ปานกลาง

		รับจ้างให้บริการเป็นประจำทุกเดือน ● มีการแบ่งหน้าที่ความรับผิดชอบ ● ต้องได้รับการอนุมัติจากผู้บริหาร				
IT-CIO	ผลประโยชน์ทับซ้อนกับผู้ขายหรือผู้ให้บริการและบุคคลที่สาม .	● มีหมายเลขโทรศัพท์สายด่วน ● มีการแบ่งหน้าที่ความรับผิดชอบ ● มีการแข่งขันประกวดราคา ● มีการสื่อสารกับผู้ขายหรือผู้ให้บริการและพนักงานเป็นประจำทุกปี(มาจากท่าทีของผู้บริหารระดับสูง) ● มีคำประกาศด้านจรรยาบรรณในการดำเนินธุรกิจ ● มีคณะอนุกรรมการจัดสรรงบประมาณ – งบลงทุน ● มีรายชื่อผู้ขายหรือผู้ให้บริการที่ได้รับการอนุมัติอย่างเป็นทางการ ● มีการควบคุมทางการเงิน ● มีการตรวจสอบประวัติ	ทั้งสองแบบ	● คณะอนุกรรมการด้านจริยธรรม ● ทรัพยากรบุคคล ● การป้องกันการสูญเสีย ● การจัดซื้อจัดจ้าง ● การเงิน ● การตรวจสอบภายใน	ต่ำ	ปานกลาง
IT-CIO	การละเมิดลิขสิทธิ์ (เช่น การดาวน์โหลดหรือคัดลอกไฟล์โดยผิดกฎหมาย)	● การปิดกั้นการเชื่อมต่อระดับเดียวกัน (Peer-to-peer) ● ซอฟต์แวร์ที่ระบุถึงซอฟต์แวร์ที่ติดตั้งอยู่ในสถานีงานและเครื่องแม่ข่าย ● การจัดทำนโยบายและขั้นตอนการดำเนินงานเป็นลายลักษณ์อักษร ● การจำกัดขอบเขตการเข้าถึงอุปกรณ์เชื่อมต่อทางกายภาพและไฟล์การติดตั้งซอฟต์แวร์	ทั้งสองแบบ	● หน่วยงานปฏิบัติการด้านเทคโนโลยีสารสนเทศ ● การรักษาความมั่นคงปลอดภัยด้านข้อมูลสารสนเทศ ● การตรวจสอบภายใน	ปานกลาง	ปานกลาง
IT-CIO	การนำข้อมูลของบริษัทไปใช้ในทางไม่ชอบโดยบุคคลที่สาม (เช่น ข้อมูลของพนักงานและลูกค้าหรือข้อมูลความลับของบริษัท)	● เงื่อนไขตามสัญญา (เช่น ข้อมูลลับ เรื่องเฉพาะตัว การไม่เปิดเผยความลับ การส่งคืนข้อมูลลับ สิทธิในการตรวจสอบ) ● มีการสร้างไฟล์ฐานข้อมูลเริ่มแรก	ทั้งสองแบบ	● ผู้รับผิดชอบหน่วยธุรกิจ ● การรักษาความมั่นคงปลอดภัยด้านข้อมูลสารสนเทศ ● การตรวจสอบภายใน	ต่ำ	ต่ำ

		ของลูกค้า				

2.2 วิธีการประเมินการทุจริต

ในมุมมองของผู้กระทำการทุจริต มีการประเมินการทุจริต 2 วิธีดังต่อไปนี้[1]

- **วิธีการหาจุดอ่อนของการควบคุม –** มองหาช่องทางในการทุจริตโดยตรวจสอบการควบคุมหลัก พิจารณาว่าใครจะได้ประโยชน์จากจุดอ่อนของการควบคุม และพิจารณาว่าบุคคลผู้กระทำการทุจริตนั้นจะเล็ดรอดจากการควบคุมที่อาจดำเนินการอย่างไม่เหมาะสมได้อย่างไร
- **วิธีการใช้ฟิลด์หลัก (key fields approach) –** มองหาช่องทางในการทุจริตโดยพิจารณาว่าข้อมูลใดที่ป้ อนเข้าไปสามารถดัดแปลงได้ (และโดยใคร) ตลอดจนพิจารณาว่าจะก่อให้เกิดผลอะไร

ทั้งสองวิธีมีจุดมุ่งหมายเพื่อจะประเมินว่าผู้ใดอาจทำการทุจริตได้ จะทำการทุจริตอะไร และสัญญาณอะไรที่บ่งชี้การทุจริตในข้อมูลนั้น การระดมความคิดเห็นกับพนักงานจากหน่วยงานหลักทางธุรกิจเป็นเทคนิคที่ดีในการประเมินการทุจริตและเป็นประโยชน์ต่อวิธีทั้งสองนี้

2.3 รูปแบบการทุจริตด้านเทคโนโลยีสารสนเทศ

เนื่องจากการตรวจสอบภายในจะช่วยประเมินความพยายามขององค์กรในการดำเนินการประเมินความเสี่ยงจากการทุจริตที่มีความครอบคลุมรอบด้าน จำเป็นอย่างยิ่งที่จะต้องระบุและรวมการทุจริตด้านเทคโนโลยีสารสนเทศที่อาจเกิดขึ้นได้ไว้ในการประเมินความเสี่ยงขององค์กรโดยรวมด้วย ขั้นตอนหนึ่งในช่วงเริ่มต้นดำเนินการคือ การระบุถึงบุคคลในองค์กรที่สามารถทำการประเมินได้อย่างมีประสิทธิผล ซึ่งบุคคลหลักที่ต้องร่วมพิจารณาเรื่องดังกล่าวคือ ผู้บริหารด้านเทคโนโลยีสารสนเทศ ผู้จัดการด้านความมั่นคงปลอดภัยของข้อมูลสารสนเทศ ผู้จัดการด้านความเสี่ยงด้านเทคโนโลยีสารสนเทศ ผู้จัดการด้านการป้ องกันการสูญเสีย(loss prevention managers) ผู้จัดการด้านการปฏิบัติตามระเบียบข้อบังคับ และตำแหน่งอื่นที่สามารถเพิ่มคุณค่าให้แก่กระบวนการได้ หากองค์กรไม่มีองค์ความรู้ภายในเกี่ยวกับการประเมินการทุจริตที่เพียงพอ ก็อาจต้องพิจารณาสร้างบุคลากรในด้านนี้โดยการพัฒนาวิชาชีพนี้ให้แก่พนักงานปัจจุบัน ในบางกรณีองค์กรอาจจำเป็นต้องขอความช่วยเหลือจากภายนอกเพื่อดำเนินการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศอย่างมีคุณภาพ

องค์กรควรพิจารณาและหาวิธีจัดการกับกรณีการทุจริตต่อไปนี้ หากสามารถนำไปปรับใช้เมื่อเกิดเหตุการณ์ดังกล่าวขึ้น

[1] Coderre, David G., Computer Aided Fraud Prevention and Detection: A Step-by-Step Guide, John Wiley & Sons, 2009.

การเข้าถึงระบบหรือข้อมูลเพื่อผลประโยชน์ส่วนบุคคล

ข้อมูลสารสนเทศที่มีค่าที่สุดที่ผู้กระทำการทุจริตด้านเทคโนโลยีสารสนเทศต้องการ มักอยู่ในรูปของสินทรัพย์ดิจิทัลที่องค์กรเก็บรักษาไว้ ดังนั้น องค์กรจึงจำเป็นต้องรวมเรื่องดังกล่าวไว้ในการประเมินความเสี่ยงจากการทุจริต องค์กรส่วนใหญ่มักจะรวบรวม สร้าง ใช้ เก็บ เปิดเผย และกำจัดข้อมูลสารสนเทศที่มีมูลค่าทางการตลาดต่อบุคคลภายนอก โดยข้อมูลเหล่านี้อาจอยู่ในรูปแบบของข้อมูลส่วนบุคคลของพนักงานหรือลูกค้าเช่น เลขที่บัตรประจำตัวประชาชน เลขที่บัตรประกันสังคม เลขที่บัญชีธนาคาร เลขที่บัตรเครดิต เลขที่บัญชีเช็ค หมายเลขรหัสสาขาธนาคารที่ใช้ และข้อมูลส่วนบุคคลอื่นๆ โดยไม่ว่าผู้กระทำผิดจะเป็นบุคคลที่ได้รับอนุญาตให้เข้าถึงข้อมูลหรือเป็นนักโจรกรรมข้อมูลคอมพิวเตอร์ ข้อมูลเหล่านี้ก็สามารถขายให้แก่ผู้อื่นหรือใช้เพื่อผลประโยชน์ส่วนบุคคลในการก่ออาชญากรรมได้ เช่น การสวมรอยบุคคล การใช้บัตรเครดิตที่ถูกโจรกรรมซื้อสินค้า การปลอมแปลงบัตรเครดิต หรือการโจรกรรมหรือการลวงให้โอนเงินจากบัญชีธนาคาร

เนื่องจากบุคคลในองค์กรมีสิทธิในการเข้าถึงข้อมูล ระบบ และเครือข่ายขององค์กรโดยชอบธรรม จึงอาจก่อให้เกิดความเสี่ยงที่มีนัยสำคัญต่อนายจ้างได้ พนักงานที่ประสบปัญหาด้านการเงินอาจจำต้องเลือกใช้ระบบที่ตนเองใช้ปฏิบัติงานทุกวันกระทำการทุจริต พนักงานที่ถูกจูงใจด้วยปัญหาทางการเงิน ความโลภ ความแค้น และประโยชน์ทางธุรกิจ หรือความต้องการสร้างความประทับใจแก่นายจ้างใหม่ อาจเลือกที่จะขโมยข้อมูลความลับ ข้อมูลเฉพาะขององค์กร หรือทรัพย์สินทางปัญญาจากนายจ้าง นอกจากนี้ พนักงานด้านเทคนิคก็สามารถใช้ความรู้ทางเทคนิคในการทำลายระบบหรือเครือข่ายของนายจ้างเพื่อแก้แค้นเหตุการณ์ที่ทำให้ตนเองไม่พอใจได้[2]

ตัวอย่างต่อไปนี้แสดงให้เห็นว่า การเข้าถึงระบบหรือข้อมูลอย่างไม่เหมาะสมจะก่อให้เกิดการแสวงหาผลประโยชน์ส่วนตัวหรือการทำลายระบบได้อย่างไร

- *พนักงานในฝ ายบัญชีเงินเดือนของบริษัทโทรคมนาคมแห่งหนึ่งย้ายไปรับตำแหน่งใหม่ภายในฝ ายเดียวกันซึ่งเธอจะไม่มีสิทธิพิเศษในการเข้าถึงข้อมูลเงินเดือนของพนักงานอีกต่อไป แต่ในระหว่างการโยกย้ายตำแหน่งนี้ เธอยังคงได้รับสิทธิในการเข้าถึงข้อมูลเงินเดือนของพนักงานอยู่ เพื่อนร่วมงานคนหนึ่งบอกเธอว่า เขากำลังเริ่มทำธุรกิจการให้บริการด้านการเงินมาระยะหนึ่งและต้องการข้อมูลติดต่อลูกค้า ด้วยสิทธิในการเข้าถึงข้อมูลที่ยังมีอยู่ เธอจึงสามารถให้ข้อมูลความลับของพนักงานของบริษัทจำนวน 1,500 คนแก่เพื่อนร่วมงานคนดังกล่าว ซึ่งหมายถึง เลขที่บัญชีจำนวน 401,000 บัญชี เลขที่บัตรเครดิต และเลขที่บัตรประกันสังคม ซึ่งถูกนำไปใช้สวมรอยบุคคลกว่า 100 กรณี การทุจริตโดยบุคคลภายในครั้งนี้สร้างความเสียหายนับเป็นมูลค่ากว่า 1 ล้านเหรียญสหรัฐฯ แก่บริษัทและพนักงาน*[3]

[2] "The, Big Picture, of Insider IT Sabotage Across U.S. Critical Infrastructures." Carnegie Mellon, May 2008.

[3] Insider Threat Study: Illicit Cyber Activity in the Information Technology and Telecommunications Sector." U.S. Secret Service and CERT Coordination Center/SEI, January 2008.

- *นักวิเคราะห์ฐานข้อมูลในบริษัทที่ตรวจสอบสิทธิในการใช้จ่ายและประมวลผลบัตรเครดิตชั้นนำแห่งหนึ่งใช้สิทธิในการเข้าถึงคอมพิวเตอร์เกินอำนาจ เพื่อโจรกรรมข้อมูลของลูกค้า 8.4 ล้านราย ซึ่งประกอบด้วยข้อมูลชื่อและที่อยู่ ข้อมูลบัญชีธนาคาร และข้อมูลบัตรเครดิตและบัตรเดบิต ข้อมูลเหล่านี้ถูกขายให้แก่ บริษัทที่ขายสินค้าทางโทรศัพท์เป็นระยะเวลา 5 ปี ผู้พิพากษาศาลแขวงของสหรัฐฯ ตัดสินจำคุกนักวิเคราะห์ฐานข้อมูลคนดังกล่าวเป็นเวลา 57 เดือนและปรับเป็นเงิน 3.2 ล้านเหรียญสหรัฐฯ ในข้อหาสมรู้ร่วมคิดและกระทำการทุจริตทางคอมพิวเตอร์[4]*
- *ที่ปรึกษาด้านเทคโนโลยีสารสนเทศคนหนึ่งทำงานให้แก่บริษัทขุดเจาะน้ำมันนอกชายฝั่งภายใต้สัญญาจ้างชั่วคราว หลังจากที่บริษัทปฏิเสธรับเขาเข้าเป็นพนักงานประจำ เขาจึงลักลอบเข้าระบบคอมพิวเตอร์ของบริษัทและสร้างความเสียหาย โดยการทำลายความน่าเชื่อถือและความพร้อมใช้งานของข้อมูล เขาถูกดำเนินคดีและตัดสินจำคุกสูงสุดเป็นเวลา 10 ปี ในเรือนจำของรัฐบาลกลาง[5]*

การทุจริตด้านเทคโนโลยีสารสนเทศอื่นๆ ที่มีโอกาสเกิดขึ้นในประเภทเดียวกันนี้ รวมถึงการคัดลอกและเผยแพร่ซอฟต์แวร์ที่เป็นกรรมสิทธิขององค์กรเพื่อผลประโยชน์ส่วนตัว ตลอดจนการเข้าถึงและใช้ข้อมูลความลับของบริษัท เช่น รายงานทางการเงิน ข้อมูลผู้ขายหรือผู้ให้บริการหรือแผนกลยุทธ์ทางธุรกิจ เพื่อประโยชน์ส่วนตัว ตัวอย่างเช่น พนักงานที่ไม่พอใจหรือที่ถูกให้ออกจากงานอาจคัดลอกและเผยแพร่หรือขายซอฟต์แวร์ที่เป็นกรรมสิทธิขององค์กรอย่างผิดกฎหมาย จากนั้น ผู้กระทำผิดอาจพยายามปกปิดร่องรอยโดยการเปลี่ยนหรือลบปูมบันทึกการตรวจสอบ ตลอดจนเปลี่ยนเครื่องมือติดตามดูแลอื่นๆ ที่ใช้ในการตรวจสอบปัญหา

การเปลี่ยนแปลงโปรแกรมระบบหรือข้อมูลเพื่อประโยชน์ส่วนตัว

หากองค์กรมีปัญหาในการควบคุมหรือมีจุดอ่อนในวงจรการพัฒนาระบบ ก็อาจเปิดโอกาสให้เกิดการทุจริตขึ้นได้ ตัวอย่างใน *ตารางที่ 2 – การทุจริตในการพัฒนาระบบ*[6] จะช่วยแสดงให้เห็นว่า การทุจริตอาจเกิดขึ้นในขั้นตอนการพัฒนาระบบแต่ละระยะได้อย่างไร

[4] U.S. Department of Justice Web site, Computer Crime and Intellectual Property Section, http://usdoj.gov/criminal/cybercrime, 2009.

[5] U.S. Department of Justice Web site, Computer Crime and Intellectual Property Section, http://usdoj.gov/criminal/cybercrime, 2009.

[6] Insider Threat Study: Illicit Cyber Activity in the Information Technology and Telecommunications Sector." U.S. Secret Service and CERT Coordination Center/SEI, January 2008.

ตารางที่ 2 การทุจริตในการพัฒนาระบบ

ระยะ	การทุจริต	ข้อผิดพลาด
ระยะกำหนดความต้องการ	• เจ้าพนักงานตำรวจหญิงคนหนึ่งออกและขายใบขับขี่ปลอมจำนวน 195 ใบ หลังจากที่เธอค้นพบโดยบังเอิญว่าเธอสามารถกระทำการดังกล่าวได้	• ไม่มีการระบุอย่างชัดเจนถึงข้อกำหนดในการพิสูจน์ตัวตนและการควบคุมการเข้าถึงโดยพิจารณาจากบทบาทหน้าที่รับผิดชอบ • ไม่มีการระบุอย่างชัดเจนถึงข้อกำหนดด้านการรักษาความมั่นคงปลอดภัยของกระบวนการธุรกิจที่ดำเนินการโดยอัตโนมัติ • ขาดการแบ่งหน้าที่ความรับผิดชอบ
ระยะออกแบบระบบ	• เจ้าหน้าที่สังคมสงเคราะห์ 2 คนรับเงินใต้โต๊ะจำนวน 32,000 เหรียญสหรัฐฯ จากการรับหน้าที่พิเศษในการช่วยเร่งรัดคำร้อง • พนักงานคนหนึ่งพบว่า บริษัทไม่มีการควบคุมดูแลระบบและกระบวนการดำเนินธุรกิจ เขาจึงก่ออาชญากรรมอย่างเป็นระบบ เพื่อหาผลประโยชน์จากการเบิกจ่ายเงินประกันสุขภาพกว่า 20 ล้านเหรียญสหรัฐฯ	• ไม่ได้ให้ความใส่ใจอย่างเพียงพอกับรายละเอียดของการรักษาความมั่นคงปลอดภัยในกระบวนการทำงานโดยอัตโนมัติ • ขาดการพิจารณาช่องโหว่ในการรักษาความมั่นคงปลอดภัยที่เกิดจากการอนุญาตให้ข้ามขั้นตอนในระบบ
ระยะการใช้ระบบ	• อดีตนักพัฒนาเว็บไซต์อายุ 18 ปี ฝังรหัสไว้ในโปรแกรมที่เขาเขียนขึ้นเอง เพื่อเจาะเข้าเครือข่ายของบริษัทเก่าส่งอีเมลขยะ (spam) ให้ลูกค้า เปลี่ยนระบบงาน และส่งผลให้บริษัทต้องเลิกกิจการไปในที่สุด	• ขาดการสอบทานรหัสเข้าโปรแกรม
ระยะการดำเนินการระบบ	• เจ้าหน้าที่ด้านเทคนิคคอมพิวเตอร์ ใช้อภิสิทธิ์ในการเข้าถึงระบบของลูกค้า เพื่อปล่อยไวรัสในเครือข่าย ส่งผลให้ระบบของลูกค้าหยุดทำงานชั่วคราว • วิศวกรซอฟต์แวร์จงใจไม่จัดทำเอกสารหรือสำรองรหัสโปรแกรมต้นแบบ (source code) จากนั้นก็ลบรหัสโปรแกรมนั้นทิ้งเมื่อระบบเริ่มใช้งานจริง	• ขาดการบังคับให้จัดทำเอกสารและกระบวนการสำรองข้อมูล • ขาดการจำกัดขอบเขตการเข้าถึงระบบของลูกค้าทั้งหมด
ระยะการบำรุงรักษาระบบ	• เจ้าหน้าที่ซื้อขายเงินตราต่างประเทศปกปิดผลขาดทุนจำนวน 691 ล้านเหรียญสหรัฐฯ ที่เกิดขึ้นตลอดระยะเวลากว่า 5 ปี โดยการแก้ไขรหัสโปรแกรมต้นแบบโดยไม่ได้รับอนุญาต • บริษัทโทรคมนาคมมีโปรแกรมสร้างความเสียหายที่จะทำงานเมื่อมีเงื่อนไขที่กำหนดไว้เกิดขึ้น (logic bomb) แฝงตัวอยู่ในระบบมานานกว่า 6 เดือนโดยไม่มีใครตรวจพบ จนในที่สุดข้อมูลจำนวนมากของบริษัทก็ถูกทำลายไป	• ขาดการสอบทานรหัสโปรแกรม • ผู้ใช้งานสามารถเข้าถึงรหัสโปรแกรมต้นแบบได้ • กระบวนการสำรองข้อมูลที่ไม่มีประสิทธิผล ทำให้เกิดผลกระทบที่ร้ายแรงขึ้นจากการที่ข้อมูลถูกทำลาย

ช่องโหว่อื่นๆ ในการทุจริตด้านเทคโนโลยีสารสนเทศ ที่ควรพิจารณาระหว่างการประเมินความเสี่ยงคือ

- การปลอมแปลงใบแจ้งหนี้ค่าบริการหรือการนำข้อมูลลับของพนักงาน ลูกค้า หรือบริษัทไปใช้ในทางไม่ชอบเพื่อผลประโยชน์ส่วนตัวโดยผู้รับจ้างให้บริการอิสระหรือโปรแกรมเมอร์ที่ทำงานอยู่ในประเทศและต่างประเทศ
- การละเมิดลิขสิทธิ์และการสูญเสียทรัพย์สินทางปัญญา เมื่อพนักงานหรือผู้รับจ้างคัดลอกหรือดาวน์โหลดไฟล์อย่างผิดกฎหมาย
- การนำข้อมูลของบริษัทไปใช้ในทางไม่ชอบโดยผู้ให้บริการภายนอกที่ทำหน้าที่ประมวลผลข้อมูลของพนักงานและ/หรือลูกค้า หรือข้อมูลลับอื่นของบริษัท

ต่อไปนี้คือตัวอย่างของแนวปฏิบัติที่ดีที่สุดในการรับมือกับความเสี่ยงจากการทุจริตด้านเทคโนโลยีสารสนเทศ

- มีการประเมินความเสี่ยงจากการทุจริตด้านเทคโนโลยีสารสนเทศทั่วทั้งองค์กรเป็นระยะ
- จัดฝึกอบรมเพื่อสร้างความตระหนักด้านการทุจริตและการรักษาความมั่นคงปลอดภัยแก่พนักงานทุกคนอย่างสม่ำเสมอ
- กำหนดให้มีการแบ่งหน้าที่ความรับผิดชอบ
- จำกัดขอบเขตการเข้าถึงระบบและข้อมูลตามความจำเป็นทางธุรกิจ
- ใช้นโยบายและแนวปฏิบัติในการบริหารการใช้รหัสผ่านและการระบุตัวตนอย่างเคร่งครัด
- บันทึก ติดตามดูแล และตรวจสอบกิจกรรมบนเครือข่ายโดยพนักงาน
- ให้ความระมัดระวังเป็นพิเศษกับผู้ดูแลงานระบบและผู้ใช้งานที่มีสิทธิพิเศษ
- ใช้การป้องกันหลายระดับเพื่อรับมือกับการบุกรุกเครือข่าย
- พัฒนาแผนรับมือกับเหตุการณ์ต่างๆ อย่างมีประสิทธิผล พร้อมทั้งจัดตั้งทีมรับมือกับเหตุการณ์ดังกล่าว
- ยกเลิกสิทธิในการเข้าถึงคอมพิวเตอร์เมื่อพ้นจากสภาพการเป็นพนักงาน
- รวบรวมและบันทึกข้อมูลเกี่ยวกับการทุจริตเพื่อใช้ในการสืบสวน
- มีกระบวนการสำรองข้อมูลและการกู้คืน
- ใช้โปรแกรมบริหารจัดการช่องโหว่ที่มีคุณภาพ

3. การตรวจสอบทุจริตโดยใช้การวิเคราะห์ข้อมูล

วัตถุประสงค์ของบทนี้คือ การช่วยผู้ตรวจสอบภายในให้มีบทบาทเชิงรุกในการจัดการกับการทุจริตโดยใช้เทคนิคการวิเคราะห์ข้อมูล เนื้อหาในบทนี้ครอบคลุมรายละเอียดว่า เหตุใดเทคโนโลยีการวิเคราะห์ข้อมูลจึงมีความสำคัญ รวมทั้งเทคนิคการวิเคราะห์แบบเฉพาะเจาะจงที่พิสูจน์แล้วว่ามีประสิทธิผลสูง วิธีการทดสอบทั่วไป ความสำคัญของการวิเคราะห์ข้อมูลเต็มจำนวนของประชากรทั้งหมด (full data populations) แผนกลยุทธ์การตรวจสอบทุจริต และการวิเคราะห์ข้อมูลโดยใช้แหล่งข้อมูลภายในและภายนอก

3.1 เหตุใดจึงใช้การวิเคราะห์ข้อมูลเพื่อตรวจสอบทุจริต

เทคโนโลยีการวิเคราะห์ข้อมูลช่วยให้ผู้ตรวจสอบภายในและผู้ตรวจสอบการทุจริตอื่นๆ วิเคราะห์ข้อมูลทางธุรกรรมเพื่อให้ได้ข้อมูลเชิงลึกเกี่ยวกับประสิทธิผลของการดำเนินการควบคุมภายในและเพื่อระบุถึงตัวชี้วัดความเสี่ยงจากการทุจริตหรือการทุจริตที่เกิดขึ้นจริง เทคโนโลยีการวิเคราะห์ข้อมูลจะช่วยผู้ตรวจสอบภายในรับมือกับความเสี่ยงจากการทุจริตภายในองค์กรได้ ไม่ว่าจะเป็นการสอบทานการบันทึกเงินเดือนเพื่อหาพนักงานที่ไม่มีตัวตนจริง หรือการสอบทานบัญชีเจ้าหนี้ที่มีการออกใบแจ้งหนี้ซ้ำ

องค์กรควรวิเคราะห์ธุรกรรมที่เกี่ยวข้องทั้งหมดโดยเทียบกับค่าตัวแปรควบคุม ให้ทั่วทั้งระบบและทุกระบบงานเพื่อให้ทดสอบและติดตามดูแลการควบคุมภายในได้อย่างมีประสิทธิผล การตรวจสอบธุรกรรมที่แหล่งเกิด (source level) จะช่วยให้มั่นใจได้ถึงความถูกต้องครบถ้วนและแม่นยำของข้อมูล

ปัจจัยหลักที่บ่งชี้ว่าผู้ตรวจสอบภายในสามารถเชื่อถือข้อมูลนั้นๆ ได้หรือไม่ หรือควรต้องทดสอบความน่าเชื่อถือของข้อมูลเพิ่มเติม คือ

- ความคุ้นเคยของผู้ตรวจสอบภายในต่อข้อมูลปฐมภูมิ (source data)
- การควบคุมทั่วไปและการควบคุมระบบงาน
- ความเชื่อถือที่มีต่อข้อมูล
- การมีพยานหลักฐานสนับสนุน

ขั้นตอนแรกของการทดสอบข้อมูลคือ การตรวจสอบความครบถ้วนสมบูรณ์และความถูกต้อง ซึ่งเป็นสิ่งที่สำคัญที่สุดเมื่อต้องจัดการกับการทุจริตที่อาจเกิดขึ้น เนื่องจากการขาดหายไปของข้อมูลที่ต้องบันทึกหรือการเว้นว่างข้อมูลไว้อาจบ่งชี้ว่ามีการทุจริต หรืออาจเป็นสาเหตุทำให้ไม่สามารถตรวจพบการทุจริตที่อาจเกิดขึ้น นอกจากนี้ ควรทดสอบเพิ่มเติมเพื่อให้ผู้ตรวจสอบภายในเข้าใจข้อมูลมากยิ่งขึ้นและเพื่อค้นหาสัญญาณบ่งชี้ถึงการทุจริตในข้อมูล[7]

[7] Coderre, David G. Fraud Analysis Techniques Using ACL. John Wiley & Sons, 2009.

3.2 เทคนิคการวิเคราะห์สำหรับการตรวจสอบทุจริต

มีเทคนิคการวิเคราะห์จำนวนมากที่ได้รับการพิสูจน์แล้วว่ามีประสิทธิผลสูงในการตรวจสอบทุจริต หน่วยงานตรวจสอบจึงควรพิจารณาใช้เทคนิคที่หลากหลายเหล่านี้เมื่อต้องประเมินการใช้เทคโนโลยีในการตรวจสอบทุจริต

- การคำนวณค่าตัวแปรทางสถิติ (เช่น ค่าเฉลี่ย ค่าเบี่ยงเบนมาตรฐาน ค่าสูงสุดและต่ำสุด) – เพื่อระบุธุรกรรมที่เบี่ยงเบนไปจากมาตรฐานซึ่งอาจบ่งชี้ถึงกิจกรรมการทุจริตได้
- การจัดประเภท – เพื่อหารูปแบบและความเชื่อมโยงระหว่างกลุ่มขององค์ประกอบข้อมูล
- การแบ่งค่าของตัวเลขเป็นช่วงๆ – เพื่อหาค่าที่ไม่ปกติ (ได้แก่ ค่าที่สูงหรือต่ำจนเกินไป)
- การวิเคราะห์ตัวเลขด้วยกฎของ Benford –เพื่อบ่งชี้ว่ามีตัวเลขบางจำนวนในชุดข้อมูลที่เกิดจากการสุ่ม ที่ไม่น่าจะเกิดขึ้นได้ในทางสถิติ
- รวมแหล่งข้อมูลต่างๆ เข้าด้วยกัน – เพื่อบ่งชี้ว่ามีค่าที่จับคู่กันอย่างไม่เหมาะสม เช่น ชื่อ ที่อยู่ และเลขที่บัญชีที่อยู่ในระบบที่แตกต่างกันอย่างสิ้นเชิง
- การทดสอบการทำซ้ำ– เพื่อบ่งชี้การทำธุรกรรมทางธุรกิจซ้ำทั้งอย่างง่ายและ/หรือซับซ้อน เช่น รายงานในรายละเอียดเกี่ยวกับการชำระเงิน การทำเงินเดือน การเรียกร้องเงิน หรือค่าใช้จ่ายต่างๆ
- การทดสอบข้อมูลที่ขาดหายไป – เพื่อระบุตัวเลขตามลำดับที่ถูกเว้นว่างไว้
- การรวมยอดที่เป็นตัวเลข – เพื่อตรวจสอบยอดรวมว่ามีการปลอมแปลงตัวเลขหรือไม่
- การตรวจสอบความสมเหตุสมผลของวันที่ที่ป้ อนข้อมูล– เพื่อระบุ การผ่านรายการบัญชีหรือเวลาที่ป้ อนข้อมูลซึ่งไม่เหมาะสมหรือเป็นที่น่าสงสัย

รายงานที่เปิดเผยข้อเท็จจริงในปีพ.ศ. 2551[8] ของบริษัท เอซีแอล เซอร์วิสซิส จำกัด (ACL Services Ltd.) อธิบายไว้ว่า เพื่อให้เกิดประสิทธิผลสูงสุดในการวิเคราะห์ข้อมูลการตรวจสอบทุจริต เทคโนโลยีที่ใช้จะต้องช่วยให้ผู้ตรวจสอบสามารถทำสิ่งต่อไปนี้ได้

- เปรียบเทียบข้อมูลและธุรกรรมจากระบบเทคโนโลยีสารสนเทศหลายระบบได้ (และจัดการกับช่องว่างของการควบคุมที่มักเกิดขึ้นภายในและระหว่างระบบได้)
- มีแนวทางการทำงานโดยใช้ชุดตัวชี้วัดการทุจริตที่ครอบคลุมทุกด้าน
- วิเคราะห์ธุรกรรมทั้งหมดภายในขอบเขตที่กำหนดได้
- ดำเนินการทดสอบเพื่อตรวจสอบทุจริตตามเวลาที่กำหนดไว้ และให้ข้อสังเกตเกี่ยวกับแนวโน้ม รูปแบบ และข้อยกเว้นได้ทันเวลา

[8] Analyze Every Transaction in the Fight Against Fraud: Using Technology for Effective Fraud Detection." ACL Services Ltd., 2008.

3.3 ประเภทของการทดสอบการทุจริต

เทคนิคการวิเคราะห์ข้อมูลที่อธิบายข้างต้น อาจนำไปปรับใช้กับการดำเนินงานหลากหลายด้านภายในองค์กรได้ การจัดลำดับความสำคัญของสิ่งที่ต้องตรวจสอบนั้น จำเป็นต้องดำเนินการร่วมกับกระบวนการประเมินความเสี่ยงจากการทุจริต *ตารางที่ 3 – การทดสอบการตรวจสอบทุจริต* แสดงตัวอย่างการทดสอบการตรวจสอบทุจริตที่สามารถทำได้โดยอาศัยการวิเคราะห์ข้อมูล

ตารางที่ 3 การทดสอบการตรวจสอบทุจริต

ประเภทของการทุจริต	การทดสอบเพื่อค้นหาการทุจริตประเภทนี้
ผู้ขายหรือผู้ให้บริการปลอม	● ตรวจสอบตู้ปณ. ที่ใช้เป็นที่อยู่ขององค์กรและหาความเชื่อมโยงระหว่างที่อยู่และ/หรือหมายเลขโทรศัพท์ของผู้ขายและพนักงาน ● ให้ความใส่ใจเป็นพิเศษกับผู้ขายหรือผู้ให้บริการที่มีชื่อคล้ายกัน หรือมีจำนวนผู้ขายหรือผู้ให้บริการมากกว่าหนึ่งรายที่ใช้ที่อยู่หรือหมายเลขโทรศัพท์เดียวกัน
ใบแจ้งหนี้ปลอม	● ค้นหาใบแจ้งหนี้ที่มีการทำซ้ำ ● ตรวจสอบจำนวนเงินในใบแจ้งหนี้ที่ไม่ตรงกับจำนวนเงินที่ระบุไว้ในสัญญาหรือใบสั่งซื้อ
การประมูลที่กำหนดผู้ชนะไว้แล้ว	● สรุปมูลค่าของสัญญาแยกตามผู้ขายเป็นรายๆ และเปรียบเทียบข้อมูลสรุปของผู้ขายในระยะเวลาหลายๆ ปี เพื่อพิจารณาว่าผู้ประมูลรายหนึ่งรายใดชนะการประมูลงานส่วนใหญ่หรือไม่ ● คำนวณระยะเวลาระหว่างวันที่ปิดการประมูลและวันที่ผู้ยื่นประมูลส่งเอกสารสัญญาเพื่อพิจารณาว่า ผู้ยื่นซองรายสุดท้ายมักจะชนะการประมูลอยู่เสมอหรือไม่
สินค้าที่ไม่ได้รับ	● ค้นหาปริมาณการซื้อที่ไม่ตรงกับจำนวนที่ระบุไว้ในสัญญา ● ตรวจสอบระดับสินค้าคงคลังว่าเปลี่ยนแปลงตามจำนวนสินค้าที่ควรจะได้รับหรือไม่
ใบแจ้งหนี้ซ้ำ	● สอบทานเพื่อหาเลขที่ใบแจ้งหนี้ซ้ำ วันที่ซ้ำ และจำนวนเงินในใบแจ้งหนี้ซ้ำ
ราคาซื้อที่สูงเกินไป	● เปรียบเทียบราคาซื้อกับผู้ขายหรือผู้ให้บริการหลายรายเพื่อพิจารณาว่าราคาซื้อจากผู้ขายรายนั้นสูงอย่างไม่มีเหตุผลหรือไม่
ซื้อสินค้าจำนวนมากเกินไป	● สอบทานเพื่อหาการเพิ่มขึ้นของสินค้าคงคลังที่อธิบายเหตุผลไม่ได้ ● พิจารณาว่าปริมาณวัตถุดิบที่ซื้อมาเหมาะสมกับระดับการผลิตหรือไม่ ● ตรวจสอบว่าปริมาณการสั่งซื้อที่เพิ่มขึ้นเป็นไปในทิศทางเดียวกับสัญญาก่อนหน้า หรือปีก่อนหน้า หรือเมื่อเปรียบเทียบกับโรงงานอื่นหรือไม่
การชำระเงินซ้ำ	● ค้นหาใบแจ้งหนี้ที่มีเลขที่และจำนวนเงินซ้ำกัน ● ตรวจสอบคำขอคืนเงินซ้ำจากใบแจ้งหนี้ที่มีการชำระเงินสองครั้ง

เอกสารชุดสำเนา	● ค้นหาต้นขั้วเช็คทุกใบที่มีการขึ้นเงินแล้ว ● ค้นหาเลขที่เช็คที่ขาดหายไปซ้ำอีกครั้ง
หมายเลขประจำเครื่อง (serial number) ซ้ำ	● พิจารณาว่ามีการซื้ออุปกรณ์ใหม่ที่มีราคาสูงทั้งที่บริษัทมีอุปกรณ์นั้นอยู่แล้วหรือไม่ โดยการตรวจสอบหมายเลขประจำเครื่องที่ซ้ำกันและพิจารณาว่าบุคคลเดียวกันมีส่วนเกี่ยวข้องทั้งในกระบวนการจัดซื้อและการขนส่งหรือไม่
การทุจริตเงินเดือน	● ตรวจสอบว่ายังมีรายชื่อพนักงานที่พ้นสภาพไปแล้วในบัญชีการจ่ายเงินเดือนหรือไม่ โดยเปรียบเทียบวันสิ้นสุดการจ้างและช่วงเวลาที่จ่ายเงิน และดึงรายการที่มีการจ่ายเงินทั้งหมดที่เกิดขึ้นภายหลังวันสิ้นสุดการจ้างงาน
บัญชีเจ้าหนี้	● ค้นหาธุรกรรมที่มีจำนวนเงินไม่เป็นไปตามที่ระบุไว้ในสัญญา โดยการเชื่อมโยงไฟล์บัญชีเจ้าหนี้กับสัญญาและไฟล์สินค้าคงคลัง รวมทั้งตรวจสอบวันที่ทำสัญญา ราคา จำนวนที่สั่งซื้อ จำนวนที่ระบุในใบรับสินค้า จำนวนที่ระบุในใบแจ้งหนี้ และจำนวนเงินที่จ่ายตามสัญญา

ที่มา: Computer *Aided Fraud Prevention and Detection and Detection: A Step-by-Step Guide*[9], by David Coderre

สำหรับการทดสอบเชิงวิเคราะห์ที่ต้องอาศัยการเข้าถึงและการใช้ข้อมูลส่วนบุคคลและ/หรือข้อมูลที่มีความอ่อนไหว ผู้ตรวจสอบภายในต้องใช้ความระมัดระวังเป็นพิเศษในการปกป้องข้อมูลเหล่านั้น ส่วนองค์กรก็ต้องมั่นใจว่าได้ดำเนินการประเมินความเสี่ยงด้านความเป็นส่วนตัว เมื่อมีการเข้าถึงหรือใช้ข้อมูลส่วนบุคคลเพราะมีกฎหมายควบคุมอยู่

3.4 การวิเคราะห์ข้อมูลของประชากรทั้งหมด

เพื่อให้แผนการตรวจสอบทุจริตมีประสิทธิผล ต้องใช้เทคนิคการตรวจสอบทุจริตที่กล่าวถึงข้างต้น เทียบกับ ข้อมูลของประชากรทั้งหมด แม้ว่าการสุ่มตัวอย่างข้อมูลจะเป็นวิธีการตรวจสอบที่ใช้ได้ดีและมีประสิทธิผลก็ตาม แต่ก็อาจไม่ตอบสนองวัตถุประสงค์ของการตรวจสอบทุจริตก็เป็นได้ เพราะหากทดสอบข้อมูลแค่เพียงบางส่วน ก็อาจไม่พบรายการที่ฝ่าฝืนการควบคุมและไม่พบธุรกรรมที่น่าสงสัย นอกจากนี้ ผลกระทบของความล้มเหลวในการควบคุมอาจไม่ได้รับการประเมินอย่างครบถ้วน และความผิดปกติเล็กๆ น้อยๆ ก็อาจตรวจไม่พบ ซึ่งความผิดปกติเหล่านี้อาจนำไปสู่ความเสียหายที่มีสาระสำคัญได้

การวิเคราะห์ข้อมูลโดยเทียบกับข้อมูลของประชากรทั้งหมดช่วยให้มองเห็นภาพรวมความผิดพลาดที่มีโอกาสจะเกิดขึ้นได้อย่างครบถ้วนมากขึ้น การสุ่มตัวอย่างเป็นวิธีที่มีประสิทธิผลที่สุดในการระบุปัญหาที่มีความเชื่อมโยงกันที่อยู่ในข้อมูลทั้งหมด เพราะโดยธรรมชาติแล้ว การทุจริตมักไม่เกิดขึ้นโดยปราศจากเป้าหมาย

[9] Coderre, David G., Computer Aided Fraud Prevention and Detection: A Step-by-Step Guide, John Wiley & Sons, 2009.

3.5 กลยุทธ์การใช้แผนการป้องกันและตรวจสอบทุจริต

องค์กรควรใช้วิธีการเชิงรุกเพื่อรับมือกับการทุจริตมากกว่ารอให้มีผู้มาแจ้งเบาะแส ซึ่งวิธีการที่องค์กรเลือกใช้ควรรวมถึงการประเมินความมีประสิทธิผลของการควบคุมภายในโดยการตรวจสอบภายใน ตลอดจนการวิเคราะห์ข้อมูลในระดับธุรกรรมเพื่อหาตัวบ่งชี้การทุจริต

แผนการป้องกันและตรวจสอบทุจริตควรรวมถึงการวิเคราะห์ข้อมูลในระดับต่างๆ ตั้งแต่ระดับเฉพาะกิจ ระดับที่ต้องวิเคราะห์ซ้ำ และระดับการวิเคราะห์แบบต่อเนื่อง เมื่อพิจารณาถึงตัวชี้วัดความเสี่ยงหลัก (key risk indicators: KRIs) แล้ว การทดสอบที่เกิดขึ้นแบบเฉพาะกิจจะบ่งชี้สิ่งที่ต้องตรวจสอบเพิ่มเติม หากการตรวจสอบในเบื้องต้นแสดงถึงจุดอ่อนของการควบคุมหรือข้อสงสัยว่าอาจจะเกิดการทุจริต องค์กรควรพิจารณาดำเนินการทดสอบซ้ำหรือทำการวิเคราะห์แบบต่อเนื่อง การวิเคราะห์ข้อมูลทางธุรกรรมเป็นวิธีการตรวจสอบทุจริตภายในองค์กรวิธีหนึ่งที่ใช้ได้ผลและเป็นวิธีที่มีประสิทธิผลมากที่สุด และองค์กรก็สามารถพิจารณาการใช้งานตามผลการวิเคราะห์ซึ่งพิจารณาจากประเด็นความเสี่ยงจากการทุจริต[10]

รายงาน Fraud Risk Management ของ KPMG อธิบายว่า “การติดตามดูแลธุรกรรมอย่างต่อเนื่องช่วยให้องค์กรระบุธุรกรรมที่มีโอกาสเกิดการทุจริตได้เป็นรายวัน รายสัปดาห์และรายเดือน ซึ่งต่างจากการวิเคราะห์ข้อมูลย้อนหลัง องค์กรต่างๆ มักพยายามดำเนินการติดตามดูแลโดยมุ่งเน้นที่ธุรกรรมที่อยู่ในขอบเขตที่กำหนดหรือธุรกรรมที่มีความเสี่ยงสูง”[11]

องค์กรจะสามารถตรวจสอบทุจริตได้เร็วขึ้นและลดโอกาสที่จะเกิดความเสียหายที่ร้ายแรงได้ด้วยเทคโนโลยีการวิเคราะห์ข้อมูลแบบต่อเนื่องหรือแบบที่มีการดำเนินการซ้ำ ไม่ว่าจะเป็นการตรวจสอบต่อเนื่องหรือการเริ่มต้นติดตามดูแลต่อเนื่องก็ตาม

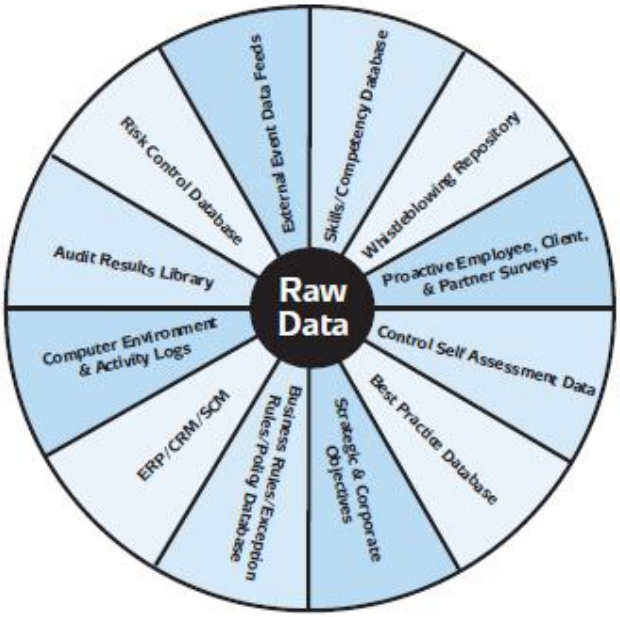
3.6 การวิเคราะห์ข้อมูลโดยใช้แหล่งข้อมูลจากภายในและภายนอก

เพื่อให้การวิเคราะห์ข้อมูลในการตรวจสอบทุจริตมีประสิทธิผล จำเป็นต้องรวมข้อมูลจากแหล่งต่างๆ ทั้งข้อมูลด้านการเงินและด้านที่ไม่ใช่ด้านการเงิน และข้อมูลจากภายในและภายนอก การใช้ข้อมูลจากแหล่งที่หลากหลายนี้จะทำให้เห็นภาพที่สมบูรณ์ในมุมมองเรื่องการทุจริตที่เกิดขึ้นภายในองค์กร *ตารางที่ 4 – แหล่งข้อมูลที่หลากหลาย* จะแสดงให้เห็นภาพรวมที่เกิดขึ้นอย่างชัดเจน

องค์กรควรใช้แหล่งข้อมูลเหล่านี้และแหล่งอื่นๆ ในการวิเคราะห์ข้อมูลการทุจริต ซึ่งรวมถึงกระบวนการสี่ขั้นตอนที่แสดงไว้ใน *ตารางที่ 5 – การวิเคราะห์ข้อมูลการทุจริต*

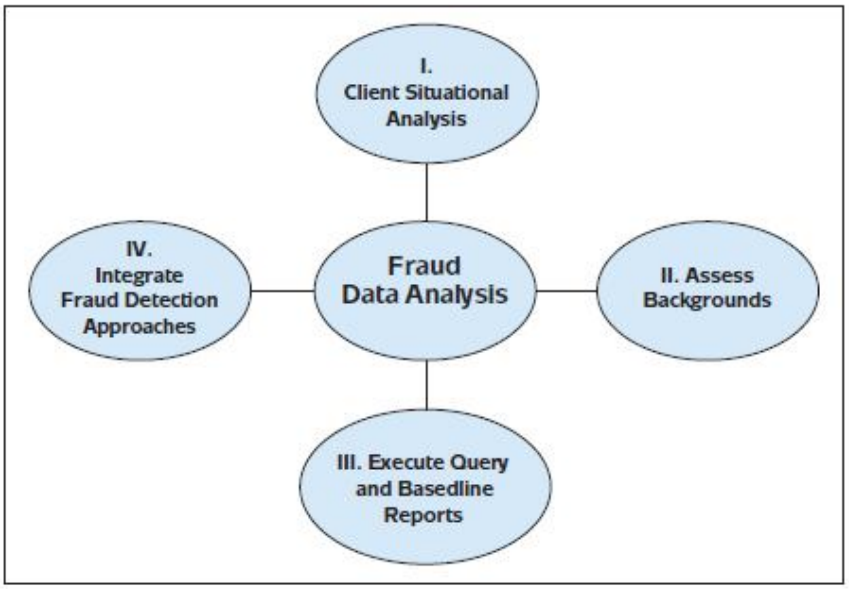
[10] “Analyze Every Transaction in the Flight Against Fraud: Using Technology for Effective Fraud Detection.” ACL Services Ltd., 2008.

[11] “Fraud Risk Management: Developing a Strategy for Prevention, Detection, and Response.” KPMG International, 2006.



ที่มา: The Buyer's Guide to Audit, Anti-Fraud, and Assurance Software[12]

ตารางที่ 4 แหล่งข้อมูลที่หลากหลาย



ตารางที่ 5 – การวิเคราะห์ข้อมูลการทุจริต

[12] Lanza, Richard B. Brooks, Dean; and Goldman, Mort. The Buyer's Guide to Audit, Anti-Fraud, and Assurance Software. Ekaros Publishing, 2008.

1. **ดำเนินการวิเคราะห์สถานการณ์**

ระบุความเสี่ยงจากการทุจริตที่สำคัญที่สุดโดยพิจารณาจากผลกระทบและความเป็นไปได้สำหรับองค์กรของตน ควรพิจารณาใช้การควบคุมภายในที่จะช่วยลดความเสี่ยงจากการทุจริต ตลอดจนแผนเพื่อศึกษาผลของการประเมินความเสี่ยงจากการทุจริต สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการดำเนินการประเมินความเสี่ยงเพื่อค้นหาการทุจริต กรุณาดูบทที่ 2

2. **ประเมินประวัติของผู้มีบทบาทหลักในการทำธุรกรรม**

โดยปกติแล้ว องค์กรจะดำเนินการตรวจสอบประวัติของพนักงานหรือผู้สมัครงานเพื่อการจ้างงานเท่านั้น องค์กรควรพิจารณาใช้ฐานข้อมูลอินเทอร์เน็ตเพื่อตรวจสอบประวัติของผู้ขายหรือผู้ให้บริการ ลูกค้าและพันธมิตรทางธุรกิจที่เกี่ยวข้องกับธุรกรรมในด้านที่มีความเสี่ยงจากการทุจริตสูง ตัวอย่างเช่น องค์กรอาจพิจารณาว่ากระบวนการจัดซื้อจัดจ้างมีความเสี่ยงสูงในการทุจริต ดังนั้น จึงอาจเลือกสอบทานผู้ขายที่มีมูลค่าของธุรกรรมสูง มีการขยายขนาดธุรกิจอย่างมากในช่วงปีที่ผ่านมา หรืออยู่ในรายงานต่างๆ ที่แสดงกิจกรรมที่มีโอกาสเกิดการทุจริต

โดยส่วนใหญ่แล้ว รัฐบาลและภาคอุตสาหกรรมในหลายๆ ประเทศจะมีแหล่งข้อมูลและรายชื่อบริษัทที่ถูกต่อต้าน (barred) คว่ำบาตร หรือถูกเฝ้าระวังในประเทศสหรัฐฯ หน่วยงาน Excluded Parties List System (www.epls.gov) จะให้ข้อมูลเกี่ยวกับผู้ที่ถูกห้ามทำสัญญากับภาครัฐ และไม่มีสิทธิได้รับความช่วยเหลือทางการเงินและผลประโยชน์อื่นจากรัฐบาลกลาง ฐานข้อมูลจากบริษัท เช่น Dun & Bradstreet และ Equifax ก็สามารถใช้เพื่อระบุประเด็นทางธุรกิจที่ส่งผลกระทบต่อบริษัทได้ เช่น การดำเนินการทางกฎหมายที่ค้างคาอยู่และ ปัญหาด้านการเงิน องค์กรควรพิจารณาแหล่งข้อมูลภายนอกที่เป็นประโยชน์เหล่านี้ หากมีการกำหนดวัตถุประสงค์และผลลัพธ์ของการตรวจสอบทุจริตอย่างชัดเจน ตัวอย่างต่อไปนี้คือข้อมูลประเภทต่างๆ ที่สามารถรวบรวมมาได้จากแหล่งข้อมูลดังกล่าวข้างต้นและใช้เพื่อประเมิน ลักษณะของการทุจริตที่อาจเกิดขึ้นกับธุรกิจ

- ที่อยู่และ/หรือหมายเลขโทรศัพท์ปลอมของบริษัท
- ผลประโยชน์ทับซ้อนของพนักงาน
- เลขประจำตัวผู้เสียภาษีปลอม
- การไม่สามารถหาหลักฐานยืนยันการมีตัวตนของบริษัทจากแหล่งข้อมูลภายนอกได้
- พนักงานเป็นผู้ขายหรือผู้ให้บริการ
- ความสัมพันธ์สามฝ่ายของพนักงาน ญาติสนิท และผู้ขาย
- บริษัทที่มีความเสี่ยง (เช่น กิจการที่มีเจ้าของคนเดียวอาจมีความเสี่ยงสูงกว่า)
- บริษัทที่เพิ่งเริ่มดำเนินธุรกิจ
- ประเด็นทางกฎหมายในอดีตหรือประเด็นพิเศษอื่นๆ.

การใช้ฐานข้อมูลภายนอกช่วยให้องค์กรมองเห็นภาพที่ชัดเจนขึ้นของผู้ร่วมทุนทางธุรกิจ (business partners) ในแง่ของโอกาสที่จะกระทำการทุจริต

3. **การตั้งคำถามที่หลากหลายและการคำนวณค่าสถิติที่เป็นเกณฑ์พื้นฐาน**

โดยพิจารณาถึงความเสี่ยงจากการทุจริตที่องค์กรได้ระบุไว้ ผู้ตรวจสอบภายในอาจตั้งคำถามและรวบรวมผลเพื่อระบุผู้ร่วมทุนทางธุรกิจ ผู้ขายหรือผู้ให้บริการ หน่วยงานในบริษัท พนักงาน และแม้กระทั่งธุรกรรมที่อาจเป็นการทุจริตได้ จากนั้นจึงสามารถคำนวณค่าสถิติที่เป็นเกณฑ์พื้นฐานสำหรับคู่ค้า หน่วยงานในบริษัท พนักงาน เวลา และอื่นๆ ได้ นอกจากนี้ ก็อาจนำกิจกรรมอื่นๆ มาเชื่อมโยงกับเกณฑ์พื้นฐานดังกล่าวเพื่อระบุข้อยกเว้นหรือสัญญาณเตือนที่มีโอกาสเป็นไปได้ซึ่งจำเป็นต้องได้รับการวิเคราะห์เพิ่มเติมต่อไป

เครื่องมือที่เป็นประโยชน์ซึ่งจะให้แนวคิดเกี่ยวกับวิธีการนำเสนอรายงานคือ Proactively Detecting Fraud Using Computer Assisted Audit Reports[13] ซึ่งเป็นผลการวิจัยของ IIA Research Foundation

สำหรับตัวอย่างบางส่วนจากรายงานดังกล่าว ได้แก่

การทุจริตการวางบิล

การทุจริตการวางบิลเกิดขึ้นเมื่อผู้กระทำการทุจริตส่งใบแจ้งหนี้ค่าสินค้าหรือบริการปลอม ใบแจ้งหนี้ที่มีมูลค่าสูงเกินจริง หรือใบแจ้งหนี้สำหรับการซื้อสินค้าที่เป็นของส่วนตัว เพื่อให้องค์กรผู้เสียหายชำระเงิน การทุจริตในลักษณะนี้แบ่งออกเป็นสามประเภทคือ

- *บริษัทปลอม* – องค์กรที่ไม่มีอยู่จริงที่ถูกตั้งขึ้นเพื่อออกใบแจ้งหนี้ปลอม
- *ผู้ขายที่ไม่ได้ร่วมทุจริต* –พนักงานจงใจชำระเงินเกินแก่ผู้ร่วมกระทำการทุจริตโดยบริษัทผู้ขายมิได้มีส่วนเกี่ยวข้องในการกระทำทุจริตนั้นๆ
- *การซื้อสินค้าที่เป็นของส่วนตัว* – การซื้อสินค้าที่เป็นของส่วนตัวโดยใช้บัญชีของบริษัท เช่น บัตรเครดิตของบริษัท

[13] Lanza, Richard B., “Proactively Detecting Fraud Using Computer Assisted Audit Reports,” the IIA Research foundation, 2003.

กระบวนการทดสอบ	รายละเอียดและการวิเคราะห์การทดสอบ	ไฟล์ข้อมูล
ระบุการชำระเงินซ้ำโดยใช้วิธีการที่หลากหลาย	สามารถกำหนดให้มีการทดสอบการชำระเงินซ้ำทั้งในส่วนของผู้ขายหรือผู้ให้บริการ เลขที่ใบแจ้งหนี้ และมูลค่าในใบแจ้งหนี้ การทดสอบที่มีความซับซ้อนมากยิ่งขึ้นจะสามารถระบุกรณีที่มีการชำระเงินตามใบแจ้งนี้ฉบับเดียวกันและมูลค่าเท่ากันแต่ชำระให้แก่ผู้ขายสองรายได้	• การชำระเงินตามใบแจ้งหนี้
สรุปยอดใบเพิ่มหนี้โดยแบ่งตามผู้ขาย ผู้ออกเอกสาร และประเภทของการจ่ายเงิน	ควรตรวจสอบใบเพิ่มหนี้ที่มีความผิดปกติ เพราะอาจแสดงถึงความพยายามปกปิดการชำระเงินที่ไม่ได้รับการอนุมัติ	• การชำระเงินตามใบแจ้งหนี้
ระบุเช็คที่ออกด้วยมือและสรุปโดยแบ่งตามผู้ขายและผู้ออกเอกสาร	เช็คที่ออกด้วยมือมีแนวโน้มจะมีการทุจริตมากกว่า ดังนั้น จึงควรได้รับการพินิจพิเคราะห์โดยละเอียด โดยเฉพาะอย่างยิ่งเมื่อพนักงานคนใดคนหนึ่งเขียนเช็คเป็นปริมาณมาก	• ทะเบียนเช็ค
ตรวจหาการซื้อที่ไม่มีใบคำสั่งซื้อและสรุปโดยแบ่งตามผู้ขายและผู้ออกเอกสาร.	การซื้อที่ไม่มีใบคำสั่งซื้อมีแนวโน้มจะมีการทุจริตมากกว่า ดังนั้นจึงควรได้รับการพิจารณาโดยละอียด โดยเฉพาะอย่างยิ่งหากใบแจ้งหนี้ไม่มีใบคำสั่งซื้อที่สอดคล้องกัน	• การชำระเงินตามใบแจ้งหนี้
จับคู่แฟ้มข้อมูลหลักเกี่ยวกับรายชื่อผู้ขายกับไฟล์ใบแจ้งหนี้ของบัญชีเจ้าหนี้	ระบุการชำระเงินแก่ผู้ขายที่อาจไม่ได้รับการอนุมัติ โดยการรวมไฟล์ผู้ขายและไฟล์ใบแจ้งหนี้หรือหมายเลขผู้ขาย โดยควรดำเนินการโดยพิจารณา "ไฟล์ที่จับคู่ไม่ได้" เพื่อให้แสดงเฉพาะหมายเลขผู้ขายที่อยู่ในไฟล์ใบแจ้งหนี้แต่ไม่ปรากฏอยู่ในไฟล์ผู้ขาย	• ทะเบียนรายชื่อผู้ขาย • การชำระเงินตามใบแจ้งหนี้
คัดกรองรายชื่อผู้ขายที่ไม่มีหมายเลขโทรศัพท์หรือเลขประจำตัวผู้เสียภาษี	ผู้ขายที่ไม่มีรายละเอียดดังกล่าวมีแนวโน้มจะมีการทุจริต จึงควรได้รับการพิจารณาตรวจสอบโดยละเอียด	• ทะเบียนรายชื่อผู้ขาย

เมื่อมีการตั้งคำถามหรือจัดทำสถิติเกณฑ์พื้นฐาน ผู้ตรวจสอบควรใช้คำถามพื้นฐาน 5 ข้อคือ ใคร ทำอะไร ทำไม ที่ไหนและเมื่อใด ผู้ตรวจสอบมืออาชีพจำนวนมากใช้วิธีการนี้เพื่อให้มองเห็นภาพรวมของสถานการณ์และสภาวะแวดล้อมทั้งหมด วิธีการใช้คำถามพื้นฐานทั้ง 5 ข้อดังกล่าวในการสอบทานการบันทึกรายการบัญชีในสมุดรายวัน (journal entries) ตามที่ได้แสดงตัวอย่างไว้ด้านล่างนี้ จะช่วยเพิ่มโอกาสในการตรวจจับสิ่งผิดปกติหรือการทุจริตจากรายการในสมุดแยกประเภททั่วไป[14]

[14] Lanza, Richard B. and Gilbet, Scott. "Maximizing Journal Entry Testing Through Automation." IT Audit, 2007.

ใครเป็นผู้บันทึกรายการบัญชีในสมุดรายวัน

- ระบุการบันทึกรายการบัญชีในสมุดรายวันที่ดำเนินการโดยบุคลากรที่ไม่ได้รับอนุญาตหรือผู้ที่ไม่มีอำนาจ

การบันทึกรายการบัญชีในสมุดรายวันมีลักษณะเป็นอย่างไร

- ระบุการบันทึกรายการบัญชีในสมุดรายวันที่ไม่เป็นไปตามมาตรฐานและที่ทำด้วยมือ (เปรียบเทียบกับการบันทึกรายการบัญชีประจำวันแบบมาตรฐานหรือโดยการใช้ระบบอัตโนมัติ เช่น ข้อมูลจากการบันทึกบัญชีเจ้าหนี้)
- ระบุการบันทึกรายการบัญชีในสมุดรายวันในบัญชีแยกประเภทเพื่อระบุลักษณะบัญชีที่เกิดซ้ำและความถี่ของการทำบัญชี (โดยพิจารณาจากการบันทึกผ่านรายการบัญชีเดบิตและเครดิต 10 ลำดับแรก)

ทำการบันทึกรายการบัญชีในสมุดรายวันเมื่อใด

- ระบุการบันทึกรายการบัญชีในสมุดรายวันในวันหยุดสุดสัปดาห์หรือวันหยุดนักขัตฤกษ์
- แบ่งประเภทกระบวนการบันทึกรายการบัญชีในสมุดรายวันป อนข้อมูลดบิตและเครดิต โดยแยกตามวัน เดือนและปี
- สรุปกระบวนการบันทึกรายการบัญชีในสมุดรายวัน ป อนข้อมูลดบิตและเครดิต ตามวัน เดือนและปี

ทำไมจึงมีกิจกรรมที่ผิดปกติในการบันทึกรายการบัญชีในสมุดรายวัน

- กลั่นกรองรายการในสมุดบัญชีแยกประเภททั่วไป (เดบิตหรือเครดิต) ที่มีมูลค่าเกินมูลค่าเฉลี่ยของบัญชีนั้นโดยอัตราส่วนร้อยละ (เริ่มพิจารณาที่ค่าที่สูงเป็นห้าเท่าของค่าเฉลี่ย)
- ระบุการบันทึกรายการบัญชีในสมุดรายวันที่มีคำอธิบายที่ใช้ภาษาที่ไม่ชัดเจน เช่น คำว่า “ส่วนเพิ่ม (plug)” คำว่า “ยอดคงเหลือ (balance)” และคำว่า “มียอดสุทธิเป็นศูนย์ (net to zero)”
- ระบุการบันทึกรายการบัญชีในสมุดรายวันที่ไม่ตัดยอดเป็นศูนย์ (เดบิต หัก เครดิต)

4. **บูรณาการวิธีต่าง ๆ ดังกล่าวให้เป็นการวิเคราะห์แบบองค์รวม**

องค์กรสามารถพัฒนารายชื่อกลุ่มเป้ าหมายในระดับผู้ร่วมทุนทางธุรกิจ ฝ ายงาน พนักงาน และ/หรือธุรกรรมโดยการรวมผลลัพธ์ของกระบวนการตามที่อธิบายไว้ในขั้นที่ 3 ประกอบกับใช้วิธีการให้คะแนน เมื่อดำเนินการจัดทำรายชื่อนั้น บริษัทควรพิจารณาระดับความต้องการที่เฉพาะเจาะจง นอกเหนือจากการศึกษากิจกรรมที่ผิดปกติด้วย

วิธีหนึ่งในการให้คะแนนกิจกรรมคือ การให้คะแนนผลลัพธ์แต่ละข้อที่ประกอบด้วยหุ้นส่วนธุรกิจ/ธุรกรรม แล้วจึงให้น้ำหนักแก่คะแนนดังกล่าวโดยพิจารณาจากปริมาณการดำเนินการที่เกี่ยวข้องกับหุ้นส่วนธุรกิจ/ธุรกรรม ซึ่งสามารถอธิบายได้ดีที่สุดโดยการใช้ตัวอย่างบัญชีแยกประเภทด้านบนและให้คะแนนกิจกรรมดังต่อไปนี้

ขั้นที่ 1 – ให้ 1 คะแนนแก่การบันทึกรายการบัญชีในสมุดรายวันที่ปรากฏอยู่ในการตรวจสอบข้อใดข้อหนึ่งต่อไปนี้

1. การบันทึกรายการบัญชีในสมุดรายวันที่ไม่เป็นไปตามมาตรฐานหรือที่ทำด้วยมือ
2. การบันทึกรายการบัญชีที่ถูกระงับลงในสมุดรายวัน โดยแยกตามบุคคลที่ทำการบันทึกข้อมูลและเลขที่บัญชีที่เกี่ยวข้อง
3. มูลค่าธุรกรรมบัญชีแยกประเภททั่วไปที่มากกว่ามูลค่าเฉลี่ยของบัญชีนั้นโดยอัตราส่วนร้อยละ
4. การบันทึกรายการบัญชีในสมุดรายวันที่มีคำอธิบายที่ใช้ภาษาที่ไม่ชัดเจน
5. การบันทึกรายการบัญชีในสมุดรายวันที่ไม่ตัดยอดสุทธิเป็นศูนย์

ขั้นที่ 2 – รวมคะแนนที่ได้ในขั้นที่ 1 เพื่อหาคะแนนรวม เช่น ให้คะแนน 3 คะแนนแก่การบันทึกรายการบัญชีในสมุดรายวันที่ตรงกับเงื่อนไขการตรวจสอบข้อ 1 3 และ 5 ในขั้นที่ 1

ขั้นที่ 3 –นำคะแนนรวมของการบันทึกรายการที่ได้จากขั้นที่ 2 ไปคูณกับมูลค่าเดบิตของการบันทึกรายการที่เกี่ยวข้อง เพื่อหาคะแนนที่ให้ค่าน้ำหนักแล้ว เช่น การบันทึกรายการบัญชีในสมุดรายวันที่ได้คะแนน 3 คะแนนจากขั้นที่ 2 โดยมีมูลค่าเดบิตรวม 100,000 เหรียญสหรัฐ จะได้รับคะแนนที่ให้ค่าน้ำหนักแล้ว 300,000 เหรียญสหรัฐ (3 x 100,000)

ขั้นที่ 4 –การบันทึกรายการบัญชีในสมุดรายวันจะถูกแบ่งตามคะแนนรวม ตามขั้นที่ 2 และการบันทึกรายการที่ได้คะแนนรวมสูงสุด 20 อันดับแรกจะถูกแสดงไว้ในรายงาน จากนั้นจึงแยกการบันทึกรายการบัญชีในสมุดรายวันตามคะแนนที่ให้น้ำหนักแล้วตามขั้นที่ 3 และแสดงผลการบันทึกรายการบัญชีในสมุดรายวันที่ได้คะแนนรวมสูงสุด 20 อันดับแรกในรายงาน

แม้ว่าจะสามารถสอบทานรายงานการบันทึกรายการบัญชีในสมุดรายวันแต่ละกรณีแยกกันได้ แต่การสอบทานร่วมกันจะก่อให้เกิดประสิทธิภาพสูงกว่า เนื่องจากผู้ตรวจสอบภายในจะสามารถมุ่งเน้นไปที่การบันทึกรายการที่ผิดปกติหรือมีแนวโน้มที่จะผิดปกติมากที่สุดได้ ดังนั้น หากการบันทึกรายการบัญชีในสมุดรายวันดังกล่าวปรากฏอยู่ในรายงานที่มีความน่าสงสัยหลายฉบับ ก็มีแนวโน้มจะมีความผิดปกติมากกว่า หรืออาจเกี่ยวข้องกับการบริหารไม่ได้ดำเนินการตามขั้นตอนอย่างเหมาะสม

4. บทบาทของ CAE ในการรับมือกับการทุจริตด้านเทคโนโลยีสารสนเทศ

วัตถุประสงค์ของบทนี้คือ การให้แนวทางแก่ CAE ในการสื่อสารกับคณะอนุกรรมการตรวจสอบเกี่ยวกับความเสี่ยงจากการทุจริตด้านเทคโนโลยีสารสนเทศ ตลอดจนการตั้งคำถามเพื่อช่วยเพิ่มความเข้าใจเกี่ยวกับความเสี่ยงจากการทุจริตด้านเทคโนโลยีสารสนเทศภายในองค์กรและบทบาทของผู้ตรวจสอบภายใน ข้อมูลที่เกี่ยวข้องกับการทุจริตด้านเทคโนโลยีสารสนเทศที่ควรพิจารณาเพื่อรายงานให้คณะอนุกรรมการตรวจสอบทราบ จะครอบคลุมถึงรายละเอียดของแนวคิดต่างๆ บทนี้ยังได้กล่าวถึงคำถาม 20 ข้อเกี่ยวกับการทุจริตด้านเทคโนโลยีสารสนเทศและให้คำแนะนำถึงนโยบายการสอบสวนการทุจริตว่า ควรครอบคลุมถึงเรื่องใดบ้างเพื่อช่วยเพิ่มความเข้าใจแก่ผู้ตรวจสอบภายในเกี่ยวกับวิธีการที่องค์กรรับมือกับความเสี่ยงจากการทุจริต

4.1 คณะอนุกรรมการตรวจสอบ

ความสัมพันธ์ระหว่าง CAE และคณะอนุกรรมการตรวจสอบควรรวมถึงการรายงานกิจกรรมการตรวจสอบภายในที่เกี่ยวข้องกับความเสี่ยงจากการทุจริตด้านเทคโนโลยีสารสนเทศและการประเมินความเสี่ยงดังกล่าว การตระหนักอยู่เสมอว่า องค์กรและอุตสาหกรรมกำลังเผชิญกับสถานการณ์ใด จะช่วยเพิ่มความสามารถของ CAE ในการจัดการความเสี่ยงจากการทุจริตด้านเทคโนโลยีสารสนเทศร่วมกับคณะอนุกรรมการตรวจสอบได้

CAE ควรหารือกับคณะอนุกรรมการตรวจสอบเกี่ยวกับการทุจริตด้านเทคโนโลยีสารสนเทศหรือการทุจริตที่เกิดจากเทคโนโลยีในเรื่องใด ส่วนใหญ่แล้ว ก็เป็นเรื่องเดียวกับการรายงานสถานการณ์เกี่ยวกับการทุจริตทั่วไปต่อผู้บริหารระดับอาวุโสและคณะอนุกรรมการตรวจสอบ Practice Guide ของ IIA ที่ว่าด้วยเรื่อง การตรวจสอบภายในและการทุจริต (Internal Auditing and Fraud) ได้ให้ข้อมูลเชิงลึกเกี่ยวกับแนวทางการสื่อสารกับคณะกรรมการ นอกจากนี้ คณะอนุกรรมการตรวจสอบอาจต้องการคำอธิบายที่ให้รายละเอียดมากขึ้นเกี่ยวกับเทคโนโลยีหรืองานด้านเทคโนโลยีสารสนเทศที่อาจได้รับผลกระทบ เพื่อให้เข้าใจผลกระทบและความเสี่ยงต่อองค์กรมากยิ่งขึ้น ดังนั้น CAE ต้องมีความคุ้นเคยและสามารถสื่อสารกับคณะอนุกรรมการตรวจสอบว่า องค์กรมีวิธีการจัดการและควบคุมทรัพยากรด้านเทคโนโลยีสารสนเทศที่สำคัญอย่างไรและบทบาทของการตรวจสอบภายในที่เกี่ยวข้องคืออะไร

CAE อาจหารือกับคณะอนุกรรมการตรวจสอบเกี่ยวกับการทุจริตด้านเทคโนโลยีสารสนเทศในเรื่องต่อไปนี้

- บทบาทของการตรวจสอบภายในในการสอบสวนการทุจริตด้านเทคโนโลยีสารสนเทศ
- การดำเนินการตรวจสอบการทุจริตทั้งหมดในด้านเทคโนโลยีสารสนเทศ
- กระบวนการประเมินความเสี่ยงจากการทุจริตด้านเทคโนโลยีสารสนเทศ
- การทุจริตด้านเทคโนโลยีสารสนเทศหรือผลประโยชน์ทับซ้อนและผลของแผนการติดตามดูแลที่เกี่ยวข้องกับการปฏิบัติตามข้อกำหนดด้านกฎหมาย จรรยาบรรณและ/หรือจริยธรรม

- โครงสร้างองค์กรที่เกี่ยวข้องกับกิจกรรมการตรวจสอบภายในเพื่อการจัดการกับการทุจริตด้านเทคโนโลยีสารสนเทศ
- ความร่วมมือของกิจกรรมการตรวจสอบการทุจริตด้านเทคโนโลยีสารสนเทศกับผู้สอบบัญชีรับอนุญาต
- การประเมินภาพรวมของสภาพแวดล้อมของการควบคุมการทุจริตในองค์กรด้านเทคโนโลยีสารสนเทศ
- มาตรการด้านการเพิ่มผลผลิตและด้านงบประมาณของกิจกรรมการตรวจสอบภายในที่เกี่ยวข้องกับการทุจริตด้านเทคโนโลยีสารสนเทศ
- ใช้เกณฑ์เปรียบเทียบกิจกรรมการตรวจสอบภายในที่เกี่ยวข้องกับการทุจริตด้านเทคโนโลยีสารสนเทศกับบริษัทอื่น

4.2 คำถาม 20 ข้อเกี่ยวกับการทุจริตที่ CAE ควรถาม

CAE ไม่ควรลังเลที่จะถามคำถามเกี่ยวกับการทุจริต การหารืออย่างทันเวลาและเหมาะสมกับบุคลากรทุกระดับในองค์กร ซึ่งรวมถึงคณะอนุกรรมการตรวจสอบในเรื่องการทุจริต แสดงถึงบทบาทเชิงรุกของการตรวจสอบภายใน คำถามเกี่ยวกับการทุจริตด้านเทคโนโลยีสารสนเทศที่ CAE ควรถามโดยทั่วไปแล้วมีดังนี้

1. องค์กรมีโครงสร้างการกำกับดูแลการทุจริตที่มีการมอบหมายความรับผิดชอบในเรื่องการสอบสวนการทุจริตด้านเทคโนโลยีสารสนเทศหรือไม่
2. องค์กรมีนโยบายรับมือกับเหตุการณ์ทุจริตด้านเทคโนโลยีสารสนเทศหรือไม่ (สำหรับข้อมูลเพิ่มเติม ดู *เรื่องที่ควรรวมอยู่ในนโยบายการสอบสวนการทุจริต*)
3. องค์กรได้ระบุกฎหมายและระเบียบข้อบังคับเกี่ยวกับการทุจริตด้านเทคโนโลยีสารสนเทศในขอบเขตอำนาจศาลของพื้นที่ที่ดำเนินธุรกิจอยู่หรือไม่
4. แผนการจัดการกับทุจริตด้านเทคโนโลยีสารสนเทศขององค์กรรวมถึงการประสานงานกับการตรวจสอบภายในหรือไม่
5. องค์กรมีสายด่วนรับแจ้งการทุจริตซึ่งจะแจ้งให้ผู้ที่อยู่ในระดับที่เหมาะสมได้รับทราบถึงข้อกังวลเกี่ยวกับการทุจริตที่เกี่ยวข้องกับทรัพยากรด้านเทคโนโลยีสารสนเทศหรือไม่
6. กฎบัตรการตรวจสอบได้กล่าวถึงบทบาทและหน้าที่รับผิดชอบของผู้ตรวจสอบภายในที่เกี่ยวข้องกับการทุจริตด้านเทคโนโลยีสารสนเทศหรือไม่
7. มีการมอบหมายความรับผิดชอบในการตรวจจับ ป้องกันรับมือ และความตระหนักในเรื่องการทุจริตด้านเทคโนโลยีสารสนเทศภายในองค์กรหรือไม่

8. ผู้บริหารและ CAE ได้แจ้งเรื่องการทุจริตด้านเทคโนโลยีสารสนเทศให้คณะอนุกรรมการตรวจสอบรับทราบจนถึงปัจจุบันหรือไม่
9. ผู้บริหารได้ส่งเสริมให้เกิดความตระหนักในเรื่องการทุจริตด้านเทคโนโลยีสารสนเทศและจัดให้มีการฝึกอบรมภายในองค์กรหรือไม่
10. ผู้บริหารเป็นผู้นำในการประเมินความเสี่ยงจากการทุจริตด้านเทคโนโลยีสารสนเทศและรวมการตรวจสอบภายในไว้ในกระบวนการประเมินหรือไม่
11. มีการนำผลการประเมินความเสี่ยงจากการทุจริตด้านเทคโนโลยีสารสนเทศไปใช้ในกระบวนการวางแผนการตรวจสอบหรือไม่
12. มีการสร้างความตระหนักรู้ในเรื่องการทุจริตด้านเทคโนโลยีสารสนเทศ ตลอดจนให้การฝึกอบรมในเรื่องดังกล่าวแก่ผู้ตรวจสอบภายในเป็นระยะๆ หรือไม่
13. มีการจัดหาเครื่องมืออัตโนมัติให้แก่ผู้ที่รับผิดชอบเรื่องการป้องกันการตรวจจับ และการสอบสวนการทุจริตด้านเทคโนโลยีสารสนเทศหรือไม่
14. ผู้บริหารได้ระบุประเภทของความเสี่ยงจากการทุจริตด้านเทคโนโลยีสารสนเทศที่มีโอกาสเกิดขึ้นได้ในขอบเขตความรับผิดชอบของตนเองไว้หรือไม่
15. ผู้บริหารและ CAE ทราบหรือไม่ว่า จะขอคำแนะนำเรื่องการทุจริตด้านเทคโนโลยีสารสนเทศจากองค์กรที่มีความเชี่ยวชาญได้จากที่ใด
16. ผู้บริหารและผู้ตรวจสอบภายในรับทราบหน้าที่ของตนที่เกี่ยวข้องกับการทุจริตด้านเทคโนโลยีสารสนเทศหรือไม่
17. ผู้บริหารได้สร้างการควบคุมที่เหมาะสมเพื่อป้องกันตรวจจับ และสอบสวนการทุจริตด้านเทคโนโลยีสารสนเทศหรือไม่
18. ผู้บริหารมีทักษะที่เหมาะสมในการดำเนินการสอบสวนการทุจริตด้านเทคโนโลยีสารสนเทศหรือไม่
19. ผู้บริหารและผู้ตรวจสอบภายในได้ประเมินประสิทธิภาพและประสิทธิผลของการควบคุมการทุจริตด้านเทคโนโลยีสารสนเทศเป็นระยะหรือไม่
20. เอกสารเกี่ยวกับการสอบสวนการทุจริตด้านเทคโนโลยีสารสนเทศและเอกสารสนับสนุนต่างๆ ได้รับการปกป้องและเก็บรักษาไว้อย่างเหมาะสมหรือไม่

เรื่องที่ควรรวมอยู่ในนโยบายการสอบสวนการทุจริต

1. จะเริ่มสอบสวนการทุจริตเมื่อไรและอย่างไร
2. ข้อกำหนดในการจัดทำเอกสารประกอบการสอบสวนการทุจริต
3. วิธีการเลือกทีมงานที่จะดำเนินการสอบสวน
4. กระบวนการสำหรับการเพิ่มผู้เชี่ยวชาญแก่ทีมงาน
5. วิธีการประเมิน ประเมินค่า และกระชับการควบคุมภายใน
6. จะเพิ่มระดับการสอบสวนได้เมื่อไรและอย่างไร
7. ความสม่ำเสมอและความสอดคล้องในการดำเนินการให้แน่ใจว่าผู้กระทำผิดได้รับการปฏิบัติอย่างเท่าเทียมกัน
8. คำแนะนำว่าองค์กรเต็มใจจะดำเนินการสอบสวนไปถึงระดับใด
9. ช่องทางการสื่อสารที่ใช้ก่อน ระหว่าง และภายหลังการสอบสวน
10. แนวทางเกี่ยวกับขอบเขตความพยายามในการกู้สถานการณ์กลับคืน

เกี่ยวกับกรอบการปฏิบัติงานวิชาชีพตรวจสอบภายในระดับสากล

(The International Professional Practices Framework - IPPF)

กรอบการปฏิบัติงานวิชาชีพตรวจสอบภายในระดับสากล หรือ IPPF คือกรอบแนวคิดที่รวบรวมแนวทางการปฏิบัติงานที่เชื่อถือได้ซึ่งเผยแพร่โดยสมาคมผู้ตรวจสอบภายใน IPPF นี้ประกอบด้วย

แนวทางบังคับใช้ (Mandatory Guidance)

ความสอดคล้องกับหลักการที่ได้กำหนดไว้ในแนวทางบังคับใช้ เป็นสิ่งจำเป็นและมีความสำคัญอย่างยิ่งสำหรับการปฏิบัติงานวิชาชีพตรวจสอบภายใน แนวทางนี้พัฒนาขึ้นตามกระบวนการที่ผ่านการกลั่นกรองความถูกต้องเชื่อถือได้เป็นอย่างดี รวมถึงได้มีการเผยแพร่ร่างกรอบการปฏิบัติงานนี้ สู่สาธารณชนเพื่อรับฟังความคิดเห็นจากผู้มีส่วนได้เสีย องค์ประกอบหลักที่สำคัญของ IPPF นี้ประกอบไปด้วย 3 ส่วน คือ คำจำกัดความของการตรวจสอบภายใน (Definition of Internal Auditing) ประมวลจรรยาบรรณ (Code of Ethics) และมาตรฐานสากลการปฏิบัติงานวิชาชีพตรวจสอบภายใน (*International Standards for the Professional Practice of Internal Auditing*)

องค์ประกอบ	**คำจำกัดความ**
คำจำกัดความ	คำจำกัดความของการตรวจสอบภายในกล่าวถึงวัตถุประสงค์พื้นฐาน ลักษณะงาน และขอบเขตของงานตรวจสอบภายใน
ประมวลจรรยาบรรณ	ประมวลจรรยาบรรณกล่าวถึงหลักการและความประพฤติที่พึงปฏิบัติของผู้ตรวจสอบภายในและองค์กรที่เกี่ยวข้องกับการปฏิบัติงานตรวจสอบภายใน ประมวลจรรยาบรรณนี้บรรยายถึงข้อกำหนดในการปฏิบัติงานและความประพฤติของผู้ตรวจสอบภายในที่คาดหวังในขั้นต่ำ มากกว่าการปฏิบัติงานเฉพาะอย่าง
มาตรฐานสากล	*มาตรฐานสากล*มุ่งเน้นในหลักการและให้กรอบในการปฏิบัติงานและการส่งเสริมงานตรวจสอบภายใน *มาตรฐาน*นี้เป็นข้อกำหนดที่ต้องปฏิบัติซึ่งประกอบด้วย • แถลงการณ์ของข้อกำหนดพื้นฐานสำหรับการปฏิบัติงานวิชาชีพตรวจสอบภายในและการประเมินความมีประสิทธิผลของการปฏิบัติงานนั้นๆ ข้อกำหนดนี้สามารถนำมาปรับใช้ได้อย่างเป็นสากลทั้งในระดับองค์กรและระดับบุคคล • การตีความ ซึ่งอธิบายคำ (term) หรือแนวความคิด (concept) ที่ปรากฏอยู่ในแถลงการณ์นั้นๆ ทั้งแถลงการณ์และการตีความแถลงการณ์นั้นเป็นสิ่งที่ผู้ประกอบวิชาชีพจำเป็นที่จะต้องให้ความสนใจเพื่อทำความเข้าใจและสามารถนำ*มาตรฐานสากล*ไปประยุกต์ใช้ได้อย่างถูกต้อง นอกจากนี้ ใน *มาตรฐานสากล* ยังมีการใช้คำซึ่งได้อธิบายความหมายเฉพาะไว้ในภาคคำศัพท์ของ IPPF ด้วย

แนวทางที่แนะนำให้ต้องนำไปใช้ (Strongly Recommended Guidance)

แนวทางที่แนะนำให้ต้องนำไปใช้นี้ได้รับการรับรองจากสมาคมผู้ตรวจสอบภายใน (IIA) โดยผ่านกระบวนการพิจารณาอนุมัติอย่างเป็นทางการ แนวทางนี้อธิบายถึงแนวปฏิบัติสำหรับการนำคำจำกัดความของการตรวจสอบภายใน ประมวลจรรยาบรรณ และ*มาตรฐานฯ* ไปใช้อย่างมีประสิทธิผล องค์ประกอบทั้ง 3 ของ IPPF ที่ได้รับการแนะนำให้ต้องนำไปใช้ คือ เอกสารแสดงความคิดเห็น (Position Papers) ข้อแนะนำในการนำมาตรฐานไปใช้ (Practice Advisories) และแนวปฏิบัติ (Practice Guides)

องค์ประกอบ	**คำจำกัดความ**
เอกสารแสดงความคิดเห็น	เอกสารแสดงความคิดเห็นจะช่วยให้ผู้ที่มีความสนใจในงานตรวจสอบภายในในวงกว้าง ซึ่งรวมถึงผู้ที่ไม่ได้อยู่ในสายวิชาชีพตรวจสอบภายใน ได้ทำความเข้าใจถึงประเด็นที่สำคัญเกี่ยวกับการกำกับดูแล ความเสี่ยง หรือการควบคุม และช่วยอธิบายบทบาทและความรับผิดชอบที่เกี่ยวข้องกับการตรวจสอบภายในด้วย
ข้อแนะนำในการนำมาตรฐานไปใช้	ข้อแนะนำในการนำมาตรฐานไปใช้จะช่วยให้ผู้ตรวจสอบภายในสามารถประยุกต์ใช้คำจำกัดความของการตรวจสอบภายใน ประมวลจรรยาบรรณและมาตรฐานสากล รวมถึงส่งเสริมแนวปฏิบัติที่ดีด้วย ซึ่งข้อแนะนำนี้จะอธิบายถึงแนวทางการปฏิบัติงาน วิธีการปฏิบัติงาน และข้อพิจารณาในการปฏิบัติงานตรวจสอบภายใน แต่ไม่ได้อธิบายขั้นตอนหรือกระบวนการปฏิบัติงานโดยละเอียด ข้อแนะนำนี้รวมถึงแนวปฏิบัติที่เกี่ยวข้องกับประเด็นในระดับสากล ระดับประเทศ หรือในระดับอุตสาหกรรมเฉพาะอย่าง และภารกิจเฉพาะ รวมถึงประเด็นทางกฎหมายหรือข้อบังคับต่าง ๆ
แนวปฏิบัติ	แนวปฏิบัติจะให้แนวทางโดยละเอียดในการดำเนินกิจกรรมการตรวจสอบภายใน ซึ่งรวมถึงขั้นตอนและกระบวนการปฏิบัติงานโดยละเอียด เช่น เครื่องมือและเทคนิค (tool and technique) แนวการตรวจสอบ และแนวการปฏิบัติงานโดยละเอียดตามขั้นตอน รวมไปถึงตัวอย่างผลงานตรวจสอบที่ต้องส่งมอบ

แนวทางฉบับนี้อยู่ภายใต้กรอบการปฏิบัติงานวิชาชีพตรวจสอบภายในระดับสากล

สำหรับเอกสารแนวทางที่ประกาศใช้อื่นๆ สามารถค้นหาเพิ่มเติมได้ที่ www.theiia.org/guidance/