มาตรฐานการตรวจสอบสารระบบสนเทศ: CISA (Certified Information System Auditor: CISA)

รวบรวมโดย

คุณเจือทิพย์ นันทะสาร [46654067]

คุณธนิพรรณ สมร่าง [46654166]

คุณธาราทิพย์ อร่ามเจริญ [46654190]

คุณพรชัย เอี่ยมเศรษฐกุล [46654620]

คุณไพรัช หอมทอง [46654356]

คุณวิทยาศักดิ์ รุจิวรกุล [46654414]

คุณอมรินทร์ เทียนประยูร [46654620]

เสนอ

รศ.ดร.ครรชิต มาลัยวงศ์

ราชบัณฑิต สาขาวิชาคอมพิวเตอร์

ประกอบวิชา 214552: Managing Information Technology

ประจำภาคเรียนที่ 1 ปีการศึกษา 2547

คำนำ

ระบบสารสนเทศมีใช้อยู่ในทุกๆ องค์กร มากบ้างน้อยบ้างตามแต่ขนาดขององค์กรนั้นๆ และความต้องการใช้ เมื่อมีการใช้เทคโนโลยีต่างๆ เพิ่มมากขึ้น ความซับซ้อนของระบบก็เพิ่มขึ้นเป็นเงาตามตัว ทำให้ต้องมีการกำหนดมาตรฐานเพื่อให้ระบบสามารถทำงานร่วมกันได้อย่างมีประสิทธิภาพ สำหรับประเทศไทยแล้ว การจะให้องค์กรเป็นบรรษัทภิบาลนั้น สิ่งหนึ่งที่ขาดไม่ได้คือ การตรวจสอบ (Audit) และมาตรฐานสำหรับการตรวจสอบระบบสารสนเทส มาตรฐาน CISA หรือ Certified Information System Auditor เป็นมาตรฐานหนึ่งที่น่าความสนใจเป็นอย่างยิ่ง

เอกสารฉบับนี้ จัดทำขึ้นเพื่อให้ผู้อ่านได้ทำความเข้าใจกับมาตรฐานการตรวจสอบระบบสารสนเทศ – CISA ว่า CISA คืออะไร และมีหลักการเป็นอย่างไร พร้อมทั้งมีรายละเอียดของแหล่งความรู้เพื่อให้ผู้อ่านสามารถศึกษาและทำความเข้าใจเพิ่มเติมได้ หากเอกสารฉบับนี้มีข้อผิดพลาดประการใด ผู้จัดทำขออภัยไว้ ณ ที่นี้ด้วย

คณะผู้จัดทำเอกสาร

สค. 2547

สารบัญ

มาตรฐานสำหรับผู้ตรวจสอบด้านเทคโนโลยีสารสนเทศ (IT & IS AUDITOR)

ในยุค ICT การใช้งานระบบสารสนเทศเป็นเรื่องสำคัญ และ จำเป็นสำหรับทุกองค์กร เรียกได้ว่าระบบคอมพิวเตอร์ได้ถูกนำมาใช้ในการประมวลผล, การนำเสนอข้อมูล และอื่นๆ อีกมากมาย จนเราต้องใช้งานคอมพิวเตอร์ทุกวันอย่างหลีกเลี่ยงไม่ได้

จากการที่เรานำระบบ IT มาใช้ในชีวิตประจำวันของการทำงานในองค์กร จึงมีความจำเป็นที่ต้องมีฝ่ายหรือบุคลากรที่จะมาตรวจสอบด้าน IT ซึ่งเรามักเรียกว่า **"IT Auditor"** หรือ **"IS Auditor"** โดยทั่วไปแล้ว จะมีทั้ง Internal Audit (ฝ่ายตรวจสอบภายในองค์กรเอง) และ External Audit (ผู้ตรวจสอบที่มาจากองค์กรที่เชื่อถือได้)

ผู้ตรวจสอบภายในที่ได้รับการยอมรับโดยทั่วไปเราเรียกว่า **CIA (Certified Internal Auditor)** ซึ่งทางสมาคมผู้ตรวจสอบภายใน หรือ IIAT นั้นได้มีการจัดสอบ เป็นประจำทุกปี ปีละ 2 ครั้ง (ข้อมูลเพิ่มเติมดูได้ที่ www.theiiat.or.th) ยกตัวอย่างบริษัทที่จดทะเบียนในตลาดหลักทรัพย์ ต้องแต่งตั้งคณะกรรมการกำกับงานตรวจสอบ หรือ Audit Committee ขึ้นเพื่อดูแลให้บริษัทมีระบบตรวจสอบภายในที่มีประสิทธิภาพเป็นต้น

วุฒิบัตร CIA นั้น สามารถรับรองความรู้ความสามารถของผู้ที่สอบผ่าน CIA ว่าเป็น "Professional" ในงานที่ตนเองทำอยู่ เช่นเดียวกับการยอมรับใน CPA (Certified Public Accountant) หรือ "ผู้สอบบัญชีรับอนุญาต" ทั้ง CIA และ CPA นั้น ยังไม่ได้มุ่งไปที่การตรวจสอบระบบสารสนเทศ (IT & IS AUDIT) โดยตรง เมื่อเราพูดถึงระบบสารสนเทศที่มีความเกี่ยวข้องกับการใช้งานเทคโนโลยีเครือข่าย ระบบโครงสร้างพื้นฐานด้าน IT เช่น Router, Switching, Remote Access, ระบบป้องกันด้าน Security เช่น Firewall, IDS รวมทั้ง Application Server ต่างๆ เช่น Proxy Server , Mail Server หรือ WEB Server เป็นต้น

ผู้ตรวจสอบด้าน IT และ IS จึงจำเป็นต้องวัดความรู้ทางด้านเทคนิค ประกอบกับ ความรู้ทางด้านการตรวจสอบไปด้วยกัน ในเมืองไทยมี **"สมาคมผู้ตรวจสอบและควบคุมระบบสารสนเทศ-ภาคพื้นกรุงเทพ"** เรียกโดยย่อว่า **ISACA-BANGKOK CHAPTER** ที่ทำการจัดสอบวัดความรู้ผู้ตรวจสอบด้าน IT&IS หรือเรียกว่า **"CISA"** หรือ **"Certified Information System Auditor"**

ความเป็นมาของ CISA

ก่อตั้งครั้งแรกในสหรัฐอเมริกาเมื่อปี 1978 โดยมีเป้าหมายหลัก เพื่อพัฒนา บรรทัดฐาน ในการประเมิน ความสามารถ ในการ Conduct Information System Audit, Security and Control Review และให้การสนับสนุน และพัฒนา ความสามารถของ CISA ด้วย Methodology ใหม่ๆ เพื่อให้สามารถ ปฏิบัติงาน ได้มาตรฐาน ระดับสากล ปัจจุบัน

IS Auditor หรือ IS security and Control profession มีบทบาทสำคัญ กับองค์กร มากขึ้น ทุกขณะ เนื่องจากการปฏิบัติธุรกิจจะพึ่งพา การประมวลผลข้อมูล และการเชื่อมโยง เครือข่ายต่างๆ มากขึ้น โดยที่ความเสี่ยงต่าง ๆ ก็เพิ่มมากขึ้น เช่นกัน ซึ่งตลอดระยะเวลา 21 ปี **CISA จึงเป็น Program แรก และโปรแกรมเดียว ซึ่งให้ Certificate สำหรับ Professional IS AUDIT and CONTROL และเป็นที่ยอมรับ ในระดับสากล** ซึ่งการจัดสอบ CISA จะมีขึ้น ทุกเดือนมิถุนายน ของทุกปี

คุณสมบัติของผู้เป็น CISA ก็มีกติกาดังนี้

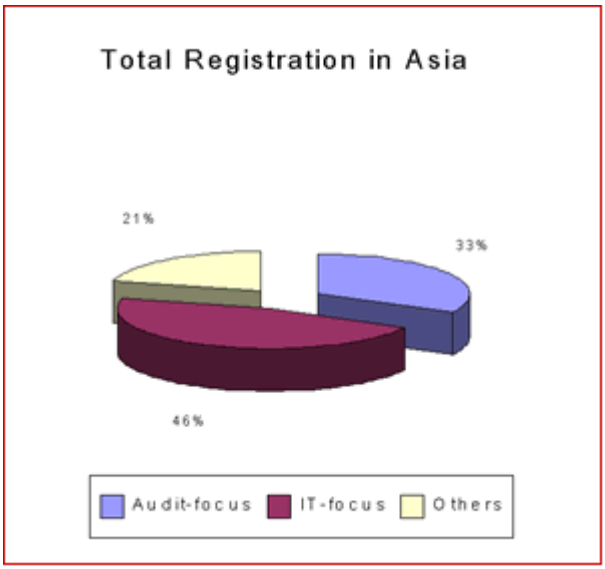
1. ต้องสอบผ่าน CISA EXAMINATION โดยได้คะแนนมากกว่าหรือเท่ากับ 75 คะแนน ซึ่งคะแนน ดังกล่าว คิดจากคะแนน ของผู้สอบทั้งหมดทั่วโลก
2. ต้องปฏิบัติงานตาม Code of Professional Ethic ของการเป็น CISA
3. ต้องมีประสบการณ์เกี่ยวกับ IS Auditing, Control หรือ Security Work Experience อย่างน้อย 5 ปี

จำนวนผู้สมัครสอบและผู้เป็น CISA:

ซึ่งในปี 1999 มีผู้เข้าสอบทั่วโลก สูงถึง 5,086 ราย และมีผู้สอบผ่าน จำนวน 2,715 ราย ซึ่งจากสถิติ ที่ผ่านมา ผู้ที่ทำการทดสอบ มิได้ จำกัดเฉพาะ IS auditor เท่านั้น ยังมี IS Security and Control Professional, IT professional, Professor, Higher Education student ซึ่งเป็นผู้ที่มีคุณสมบัติ ที่สามารถสอบได้ **ในประเทศไทย ปัจจุบันมีผู้สอบ CISA ผ่านแล้วทั้งสิ้นจำนวน 16 ท่าน** ซึ่งนับว่าเป็นจำนวนน้อย เมื่อเทียบกับความต้องการของ IS security professional

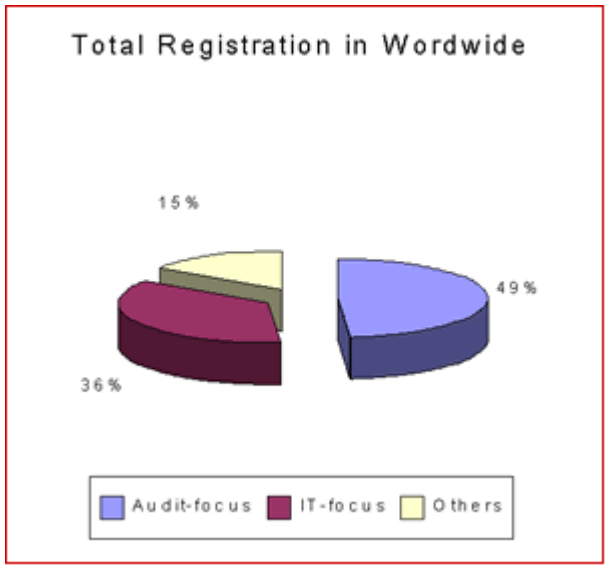
สถิติการสมัครสอบ CISA ในภูมิภาคเอเชียและของโลก ณ วันที่ 21 มีนาคม 2545

จำนวนผู้สมัครสอบ CISA ในภูมิภาคเอเชีย



จำนวนผู้สมัคร	
Audit-focus	1,366 (32.8%)
IT-focus	1,922 (46.2%)
Others	872 (21.0%)
Total	4,160

จำนวนผู้สมัครสอบ CISA ทั่วโลก



จำนวนผู้สมัคร	
Audit-focus	3,869 (48.5%)
IT-focus	2,899 (36.3%)
Others	1,210 (15.2%)
Total	**7,976**

หมายเหตุ

Audit-focus are Audit Director, General Auditor, IS Auditor, External Auditor, Internal Auditor

IT-focus are CIO, IS Director, IS Security Director/Mgr/Staff, IS Manager, IS Consultant, IS Vendor/Supplier, IS Educator/Student

Others are CEO, CFO, Non-specified

หลักการตรวจสอบระบบสารสนเทศ (IT Audit) อย่างมีประสิทธิภาพในทางปฏิบัติ

การตรวจสอบระบบสารสนเทศในปัจจุบันนี้ ถือเป็นเรื่องสำคัญที่ทุกองค์กรต้องปฏิบัติ ทั้งการตรวจสอบภายใน (Internal Audit) โดยพนักงานตรวจสอบขององค์กรเองโดยเฉพาะ ตลอดจนการตรวจสอบจากภายนอก (External Audit) เช่น การตรวจสอบจากบริษัทแม่ในต่างประเทศ หรือ การตรวจสอบจากหน่วยงานที่มีหน้าที่ในการควบคุม เช่น สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (กลต.) มีหน้าที่ตรวจสอบบริษัทหลักทรัพย์ หรือ ธนาคารแห่งประเทศไทยมีหน้าที่ตรวจสอบธนาคารพาณิชย์ เป็นต้น

หลักการในการตรวจสอบระบบสารสนเทศที่ถูกต้องก็คือ **ต้องมีการประเมินความเสี่ยง (Risk Assessment)** ขององค์กรก่อน ซึ่งมีขั้นตอนสำคัญที่ต้องปฏิบัติ คือ

- การระบุปัจจัยที่มีผลทำให้เกิดความเสี่ยง
- การระบุความเสี่ยงที่มีโอกาสเกิดขึ้น (Risk Identification)
- การวิเคราะห์ความเสี่ยง (Risk Analysis)
- การบริหารจัดการกับความเสี่ยง (Risk Management)

การตรวจสอบระบบสารสนเทศต้องพิจารณาเรื่องของการควบคุม (Control) ซึ่งต้องมีการจัดการอย่างถูกต้อง
การตรวจสอบการควบคุมแบ่งออกเป็น 3 ประเภทใหญ่ๆ คือ

1. การควบคุมแบบป้องกันล่วงหน้า (Preventive Control)
2. การควบคุมแบบค้นหาประวัติเหตุการณ์ที่เกิดขึ้น (Detective Control)
3. การควบคุมแบบแก้ไขปัญหาจากเหตุการณ์ที่เกิดขึ้น (Corrective Control)

IT Auditor ควรจะพิจารณาการควบคุม (Control) ไปพร้อมๆกันทั้ง 3 มุมมอง คือ

1. มุมมองทางด้านการบริหารจัดการ (Administrative Control)
2. มุมมองทางด้านเทคนิค (Technical Control)
3. มุมมองทางด้านกายภาพ (Physical Control)

ปัญหาของการตรวจสอบระบบสารสนเทศ

ปัญหาที่แท้จริงของการตรวจสอบระบบสารสนเทศในปัจจุบัน คือ การขาดบุคลากรที่มีความรู้และประสบการณ์ในการตรวจสอบด้านสารสนเทศโดยเฉพาะ หรือ บุคลากรที่มีอยู่ยังขาดการอบรมความรู้ใหม่ๆทางด้านเทคนิค เช่น

1. ขาดความรู้ด้าน Vulnerability Assessment และ Penetration Testing
2. ขาดความรู้พื้นฐานทางด้านเครือข่าย เช่น ISO OSI Layer Model, TCP/IP Protocol Suite
3. ขาดความรู้เกี่ยวกับการใช้งานระบบปฏิบัติการพื้นฐาน คือ Microsoft Windows และ Unix/Linux ตลอดจนความรู้พื้นฐานในการใช้งานอุปกรณ์เครือข่าย Router หรือ Switching ซึ่ง IT Auditor ควรมีความรู้พื้นฐานในระดับ CCNA (Cisco Certified Network Associate)
4. ขาดความรู้ทางด้านความปลอดภัยข้อมูล

IT Auditor ควรเข้าใจ Concept ของ CIA TRIAD (Confidentiality, Integrity and Availability), การทำงานของ Firewall และ IDS ในบริเวณ Network Perimeter ขององค์กร ตลอดจนวิธีการบุกรุกของ Hacker และ การทำงานของ Virus

ดังนั้น IT Auditor นอกจากควรจะมี **CISA Certification** เพื่อแสดงถึงความรู้ในด้าน IT Audit Process แล้ว ก็ควรจะมีความรู้พื้นฐานทางด้านเทคนิคด้วย ทั้งด้านระบบเครือข่ายและระบบปฏิบัติการที่ตนเองต้องเข้าไปตรวจสอบ ทางแก้ปัญหาในเชิงบูรณาการก็คือ IT Auditor ต้องเข้ารับการฝึกอบรมทางด้านเทคนิคเพิ่มเติม หรือ หาความรู้เพิ่มด้วยตนเองจากการติดตามข่าวสารเทคโนโลยีด้านความปลอดภัยใหม่ๆอยู่ตลอดเวลา เพื่อให้ทันกับยุคที่การสื่อสารไร้พรมแดน และ ภัยอินเตอร์เน็ต ไม่ว่าจะเป็น Hacker และ Virus ที่นับวันจะทวีความรุนแรงมากขึ้น

มาตรฐาน แนวทาง และกระบวนการสำหรับผู้ตรวจสอบและควบคุมระบบสารสนเทศ
(IS Standards, Guidelines and Procedures for Auditing and Control Professionals)

จรรยาบรรณแห่งวิชาชีพ (Code of Professional Ethics)

ผู้ที่เป็นสมาชิกของสมาคมและผู้ที่เป็น CISA จะต้องปฏิบัติตามจรรยาบรรณแห่งวิชาชีพด้านการตรวจสอบและควบคุมระบบสารสนเทศดังนี้

1. ให้การสนับสนุนการจัดตั้งและการนำไปปฏิบัติ ของมาตรฐาน ขั้นตอนการปฏิบัติ และการควบคุมที่เกี่ยวกับระบบสารสนเทศ
2. ปฏิบัติตามมาตรฐานการตรวจสอบระบบสารสนเทศที่ยอมรับโดยสมาคมฯ
3. ให้บริการแก่ผู้ว่าจ้าง ผู้ถือหุ้น ลูกค้า และสาธารณชนด้วยความรู้จริงและซื่อสัตย์ และไม่ร่วมในกิจกรรมใดๆที่ขัดต่อศีลธรรมและกฎหมาย
4. รักษาความลับของข้อมูลที่ได้รับทราบมาระหว่างการปฏิบัติหน้าที่ และไม่ใช้ข้อมูลดังกล่าวเพื่อหาประโยชน์ส่วนตัวหรือให้ข้อมูลแก่ผู้อื่นหรือองค์กรอื่นที่ไม่สมควรได้
5. ปฏิบัติหน้าที่อย่างเป็นอิสระและมีเป้าหมาย และควรหลีกเลี่ยงการรับงานไม่สามารถหรืออาจไม่สามารถปฏิบัติงานได้อย่างเป็นอิสระ
6. รักษาความรู้ความสามารถที่จำเป็นในการปฏิบัติงานการตรวจสอบระบบสารสนเทศ โดยการมีส่วนร่วมในกิจกรรมที่พัฒนาด้านวิชาชีพ
7. ใช้ความระมัดระวังและละเอียดถี่ถ้วนในการได้มาซึ่งเอกสารหลักฐานและข้อเท็จจริงที่จะนำมาซึ่งการสรุปผลการตรวจสอบอย่างถูกต้องและการให้ข้อเสนอแนะที่เหมาะสม
8. แจ้งให้ผู้ที่เกี่ยวข้องทราบถึงผลการตรวจสอบ
9. สนับสนุนการให้ความรู้ความเข้าใจแก่ผู้บริหาร ลูกค้า และสาธารณชน ด้านการตรวจสอบและด้านระบบสารสนเทศ
10. รักษามาตรฐานระดับสูงในการปฏิบัติงานและการปฏิบัติตน ทั้งในกิจกรรมด้านวิชาชีพและส่วนตัว

ความสัมพันธ์ ของ มาตรฐานกับแนวทางและกระบวนการ (Relationship of Standards to Guidelines and Procedures)

มาตรฐานการตรวจสอบระบบสารสนเทศแบ่งออกเป็น 8 กลุ่ม 12 ข้อ ซึ่งเป็นข้อบังคับสำหรับรายงานการตรวจสอบและสิ่งที่ค้นพบของผู้ที่ได้รับประกาศนียบัตร IS Auditing and Guidelines เป็นตัวชี้แนวทางที่ผู้ตรวจสอบจะปฏิบัติตามพร้อมทั้งเข้าใจว่าอาจจะมีบางสถานการณ์ที่ผู้ตรวจสอบอาจจะไม่ปฏิบัติตามแนวทาง ในกรณีนี้มันเป็นความรับผิดชอบของผู้ตรวจสอบที่จะตัดสินว่าจะใช้วิธีใด เพื่อให้งานสำเร็จ

ตัวอย่างของ Procedure แสดงถึงขั้นตอนการทำงานของผู้ตรวจสอบระบบสารสนเทศ และมีข้อมูลมากกว่า Guidelines ตัวอย่างต่างๆถูกสร้างขึ้นตามมาตรฐานของการตรวจสอบระบบสารสนเทศและ Guidelines และได้ให้ข้อมูลตามมาตรฐานการตรวจสอบระบบ ในบางครั้งอาจจะมีการสร้าง best practice ของกระบวนการการทำงานเพื่อให้ปฏิบัติตาม

การประมวลภาพรวม (Codification)

เรานำตัวเลขสามหลักมาใช้กำหนดมาตรฐาน ซึ่งกำหนดมาตรฐานออกเป็น 8 ประเภท โดยที่มาตรฐานสำหรับ IS Audit จะเริ่มต้นด้วยเลข 0, มาตรฐานสำหรับ IS Control Professionals เริ่มต้นด้วยเลข 5 ส่วนหมายเลขของมาตรฐานของเอกสารเป็นเลขอีกสามหลักถัดไป และสามหลักสุดท้ายเกี่ยวกับ guideline ส่วนกระบวนการจะถูกแยกไว้ต่างหากโดยเรียงลำดับจากวันที่ ที่ออก

Standard Category	Standard	Guideline
000	.000	.000

ตัวอย่างเช่น เอกสารหมายเลข 060.020.040 เป็น Guideline ซึ่งบอกแนวทางไปที่กลุ่มมาตรฐานข้อที่ 6 ซึ่งเป็น Performance of Audit Work และเป็นข้อที่สองที่อยู่ในกลุ่มนี้ และเป็นแนวทางข้อที่สี่ของ Evidence Procedure จะถูกกำหนดหมายเลขแยกออกมาโดยเฉพาะโดยจะเรียงตามลำดับวันที่ ที่ออก โดยจะเริ่มจาก 1

วิธีนำไปใช้ (Use)

ในการ Audit ประจำปี ผู้ทำการ audit ควรจะดำเนินการสัมภาษณ์ตามมาตรฐานที่ได้มีการกำหนดไว้ล่วงหน้า หรืออาจจะดำเนินการตามมาตรฐานของ ISACA ได้เช่นกัน

เอกสารอิเลคทรอนิคส์ (Electronic Copies)

เอกสารมาตรฐาน แนวทางและกระบวนการ ทั้งหมดของ ISACA ได้เผยแพร่ไว้ในเวปไซต์ของ ISACA ที่ www.isaca.org/standards

ภาพรวมของมาตรฐานการตรวจสอบระบบสารสนเทศ (IS Auditing Standards Overview)

โดยทั่วไปการตรวจสอบระบบสารสนเทศและทักษะในการตรวจสอบนั้นต้องทำตามมาตรฐานที่ได้กำหนดไว้ วัตถุประสงค์ของ Information System Audit and Control Association (ISACA) คือเพื่อที่จะทำให้เกิดมาตรฐานที่นำไปใช้ได้ทั่วไป เพื่อให้ตรงกับทรรศนะขององค์กร การพัฒนาและการเผยแพร่มาตรฐานการตรวจสอบระบบสารสนเทศเป็นส่วนที่สำคัญในการสนับสนุนวิชาชีพของกลุ่มที่ทำการตรวจสอบ Framework สำหรับมาตรฐานการตรวจสอบระบบสารสนเทศนั้นมีระดับการแนะนำที่หลากหลาย

มาตรฐาน เป็นการระบุความต้องการที่บังคับสำหรับการตรวจสอบระบบสารสนเทศและรายงานที่ ISACA ซึ่งกล่าวถึง

- การตรวจสอบของผู้ที่ทำการตรวจสอบระบบสารสนเทศนั้นมีระดับการตรวจสอบอย่างน้อยตามที่ได้ระบุไว้ในจรรยาบรรวิชาชีพของรหัส ISACA สำหรับผู้ตรวจสอบระบบสารสนเทศ
- การจัดการและกลุ่มผู้เชี่ยวชาญที่เกี่ยวข้อง

คำแนะนำ มีการระบุคำแนะนำในการใช้มาตรฐานการตรวจสอบระบบสารสนเทศ ผู้ตรวจสอบระบบสารสนเทศควรจะคำนึงถึงว่าควรจะทำอย่างไรถึงจะประสบความสำเร็จในการเอามาตรฐานไปใช้ โดยการใช้การตัดสินใจที่เชี่ยวชาญให้เป็นประโยชน์ และการเตรียมตัวเพื่อแสดงเหตุผลสำหรับทางออก วัตถุประสงค์ของคำแนะนำการตรวจสอบระบบสารสนเทศคือเพื่อที่จะหาสารสนเทศให้มากขึ้นเพื่อที่จะนำไปใช้กับมาตรฐานการตรวจสอบระบบสารสนเทศ

กระบวนการ จะมีตัวอย่างกระบวนการซึ่งผู้ตรวจสอบระบบสารสนเทศควรที่จะทำตามในการตรวจสอบ เอกสารกระบวนการนั้นมีข้อมูลเกี่ยวกับว่าควรทำอย่างไรเพื่อที่จะทำได้ตามมาตรฐานที่กำหนดไว้เมื่อทำการตรวจสอบงานระบบสารสนเทศ แต่ไม่ได้กำหนดสิ่งที่ต้องทำเอาไว้ วัตถุประสงค์ของกระบวนการตรวจสอบระบบสารสนเทศคือเพื่อที่จะหาสารสนเทศให้มากขึ้นเพื่อที่จะนำไปใช้กับมาตรฐานการตรวจสอบระบบสารสนเทศ

CobiT ทรัพยากรทางด้านเทคโนโลยีสารสนเทศควรที่จะถูกใช้เพื่อก่อให้เกิดการปฏิบัติที่ดีที่สุด ซึ่งสิ่งเหล่านี้ได้ถูกกำหนดโดยกระบวนการการจัดการทางด้านเทคโนโลยีสารสนเทศซึ่งระบุไว้ใน CobiT Framework CobiT มุ่งถึงการใช้ทรัพยากรทางด้านธุรกิจและการจัดการทางด้านเทคโนโลยีสารสนเทศ รวมถึงผู้ที่ทำการตรวจสอบระบบสารสนเทศ ดังนั้นการใช้ CobiT ทำให้เข้าใจถึงวัตถุประสงค์ทางธุรกิจ การสื่อสารในแง่ของการปฏิบัติที่ดีที่สุดและคำแนะนำที่เกิดขึ้นรวมถึงการทำตามมาตรฐานที่อ้างถึง ซึ่ง CobiT ได้กล่าวถึง

- Control Objective: ระดับสูงและรายระเอียดที่ระบุโดยทั่วไปของการควบคุมในขั้นต่ำ
- Control Practice: การปฏิบัติที่มีเหตุผลและการนำคำแนะนำไปใช้ในการควบคุมวัตถุประสงค์
- Audit Guideline: เป็นคำแนะนำสำหรับการควบคุมในแต่ละส่วนเพื่อที่จะเกิดความเข้าเข้าใจ การประเมินในแต่ละส่วนให้เกิดความสอดคล้องและทำให้ความเสี่ยงที่ได้รับการควบคุมนั้นไม่เกิดขึ้น
- Management Guideline: คำแนะนำในการประเมินในการพัฒนากระบวนการเทคโนโลยีสารสนเทศ โดยการใช้ Maturity model, Metric และ Critical Success Factor

Glossary สามารถดูได้ในเว็บ ISACA www.isaca.org/glossary คำของการตรวจสอบและพิจารณาสามารถใช้สับเปลี่ยนกันได้

Disclaimer ISACA ได้ออกแบบคำแนะนำในระดับขั้นต่ำที่ต้องการเพื่อให้ตรงกับที่กำหนดไว้ในรหัส ISACA ของจรรยาบรรณวิชาชีพสำหรับผู้ตรวจสอบระบบสารสนเทศ ISACA ทำให้ไม่มีการอ้างถึงว่าการใช้หลักตามนี้จะทำให้เกิดผลที่ประสบความสำเร็จอย่างแน่นอน การเผยแพร่จะไม่คำนึงถึงกระบวนการที่เหมาะสมและการทดสอบหรือนอกจากกระบวนการอื่นและการทดสอบที่มีเหตุผลโดยตรงที่จะได้ผลลัพธ์เดียวกัน ในการกำหนดกระบวนการหรือการทดสอบร่วมกัน การควบคุมขึ้นอยู่กับการตัดสินใจของผู้ตรวจสอบตามสภาพแวดล้อมของระบบจริงๆหรือสภาพของเทคโนโลยีสารสนเทศ

IS Auditing Standards & Guideline – ออกโดย Information Systems Audit and Control Association

010 Audit Charter

010.010 Responsibility, Authority and Accountability

หน้าที่, อำนาจ, และความรับผิดชอบของงานการตรวจสอบระบบสารสนเทศจะต้องทำเป็นเอกสารอย่างเหมาะสมอยู่ในเอกสารที่เป็นทางการของการตรวจสอบหรือในเอกสารข้อตกลง

010.010.010 Audit Charter Effective 1 September 1999

010.010.020 Outsourcing of IS Activities to Other Organizations Effective 1 September 1999

020 Independence

020.010 Professional Independence

ผู้ตรวจสอบระบบสารสนเทศต้องเป็นอิสระต่อผู้ถูกตรวจสอบทั้งทางด้านทัศนะคติ และทางด้านภาพลักษณ์ในทุกๆกรณีที่เกี่ยวข้องกับการตรวจสอบ

020.010.010 Effect of Nonaudit Role on the IS Auditor's Independence Effective 1 July 2002

020.020 Organizational Relationship

หน้าที่การตรวจสอบระบบสารสนเทศจะต้องมีอิสระต่อส่วนที่จะถูกตรวจสอบเพื่อให้เกิดความสำเร็จอย่างไม่ลำเอียง

020.020.010 Organizational Relationship and Independence Effective 1 September 2000

030 Professional Ethics and Standards

030.010 Code of Professional Ethics

ผู้ตรวจสอบระบบสารสนเทศจะต้องยึดติดกับ Code of Professional Ethics ของ ISACA

030.010.010 Irregularities and Illegal Acts Effective 1 July 2002

030.020 **Due Professional Care**

การปฏิบัติการและการดูแลของมืออาชีพโดยมาตรฐานการตรวจสอบจะต้องถูกนำไปใช้ในทุกๆส่วนของงานการตรวจสอบ

030.020.010 Audit Considerations for Irregularities Effective 1 March 2000

030.020.020 Due Professional Care Effective 1 September 1999

040 **Competences**

040.010 **Skills and Knowledge**

ผู้ตรวจสอบระบบสารสนเทศต้องมีความสามารถทางด้านเทคนิค มีทักษะ และความรู้ที่จำเป็นในการทำงานการตรวจสอบ

040.020 **Continuing Professional Education**

ผู้ตรวจสอบระบบสารสนเทศต้องรักษาระดับความสามารถทางด้านเทคนิคตลอดจนการศึกษาระดับมืออาชีพต่อไป

050 **Planning**

050.010 **Audit Planning**

ผู้ตรวจสอบระบบสารสนเทศจะต้องวางแผนงานการตรวจสอบระบบสารสนเทศเพื่อให้บรรลุวัตถุประสงค์ในการตรวจสอบและเหมาะสมกับมาตรฐานการตรวจสอบแบบมืออาชีพ

050.010.010 Materiality Concepts for Auditing Information Systems Effective 1 September 1999

050.010.020 Planning Revised Effective 1 March 2002

050.010.030 Use of Risk Assessment in Audit Planning Effective 1 September 2000

050.010.040 Effect of Third Parties on an Organization's IT Controls Effective 1 March 2002

060 **Performance of Audit Work**

060.010 **Supervision**

พนักงานการตรวจสอบระบบสารสนเทศจะต้องได้รับการแนะนำอย่างถูกต้องเพื่อให้ความมั่นใจว่าจะทำให้บรรลุวัตถุประสงค์ของการตรวจสอบและตรงตามมาตรฐานการตรวจสอบ

.010 Enterprise Resource Planning (ERP) Systems Review Effective 1 August 2003

.020 Mobile Computing Effective 1 September 2004

060.020 **Evidence**

ในระหว่างการตรวจสอบ ผู้ตรวจสอบระบบสารสนเทศต้องได้รับหลักฐานสำคัญที่เพียงพอ,เชื่อถือได้และมีประโยชน์เพื่อให้บรรลุวัตถุประสงค์ของหารตรวจสอบอย่างมีประสิทธิภาพ การค้นพบและการสรุปของการตรวจสอบจะเกิดจากการวิเคราะห์ที่เหมาะสม และการแปลความจากหลักฐานนั้นๆ

060.020.010 Audit Documentation Effective 1 September 1999

060.020.020 Application Systems Review Effective 1 November 2001

060.020.030 Audit Evidence Requirement Effective 1 December 1998

060.020.040 Audit Sampling Effective 1 March 2000

060.020.050 IT Governance Effective 1 July 2002

060.020.060 Effect of Pervasive IS Controls Effective 1 March 2000

060.020.070 Use of Computer Assisted Audit Techniques (CAATs) Effective 1 December 1998

060.020.080 Using the Work of Other Auditors and Experts Effective 1 June 1998

060.020.090 Business-to-consumer (B2C) E-commerce Review Effective 1 August 2003

060.020.100 System Development Life Cycle (SDLC) Review Effective 1 August 2003

060.020.110 Internet Banking Effective 1 August 2003

060.020.120 Review of Virtual Private Networks Effective 1 July 2004

060.020.130 Business Process Reengineering (BPR) Project Reviews Effective 1 July 2004

060.020.140 Computer Forensics Effective 1 September 2004

060.020.150 Business Continuity Planning (BCP) Review Effective 1 September 2004

070 **Reporting**

070.010 **Report Content and Form**

ผู้ตรวจสอบระบบสารสนเทศจะต้องจัดทำรายงานในรูปแบบที่เหมาะสม และตรงตามเป้าหมายโดยแสดงความสำเร็จของงานการตรวจสอบ รายงานการตรวจสอบต้องแสดงขอบเขต, วัตถุประสงค์, ระยะเวลาที่ครอบคลุมของงานการตรวจสอบที่ทำ รายงานจะแสดงถึงองค์กร, ผู้รับ และข้อกำหนดและการเวียนเอกสารต่างๆ รายงานจะแสดงถึงสิ่งที่ค้นพบ ข้อสรุปและข้อแนะนำ ที่ผู้ตรวจสอบระบบสารสนเทศค้นพบ

070.010.010 Reporting Effective 1 January 2003

080 **Follow-Up Activities**

080.010 **Follow-Up**

ผู้ตรวจสอบระบบสารสนเทศจะต้องร้องขอและประเมินสารสนเทศที่เหมาะสมจากการค้นพบที่ผ่านมา และสรุป ข้อชี้แนะต่างๆ เพื่อบอกถึงการกระทำที่เหมาะสมที่ได้ทำไปแล้วในช่วงเวลาที่ผ่านมา

Effective Date

มาตรฐานเหล่านี้จะมีผลใช้ต่อผู้ตรวจสอบระบบสารสนเทศในระยะเวลา เริ่มจากวันที่ 25 กรกฎาคม 1997

Index of IS Auditing Procedures

1.	IS Risk Assessment	effective 1 July 2002
2.	Digital Signatures	effective 1 July 2002
3.	Intrusion Detection	effective 1 August 2003
4.	Viruses and other Malicious Logic	effective 1 August 2003
5.	Control Risk Self-assessment	effective 1 August 2003
6.	Firewalls	effective 1 August 2003
7.	Irregularities and Illegal Acts	effective 1 November 2003
8.	Security Assessment—Penetration Testing and Vulnerability Analysis	effective 1 September 2004

บรรณานุกรม

1. จาก: หนังสือ eWeek Thailand ปักษ์แรก เดือนเมษายน 2547 Update Information: 24 กุมภาพันธ์ 2547
2. จาก: หนังสือ eLeader Thailand ปีที่ 15 ฉบับที่168 ประจำเดือนกุมภาพันธ์ 2546
   Update Information: 21 มีนาคม 2546
3. http://www.acisonline.net/article_prinya_itauditor.htm
4. http://www.isaca-bangkok.org/association/isacabkk/cisa.html
5. http://www.theiiat.or.th/
6. http://www.isaca.org