การติดตามและควบคุมการใช้งานฐานข้อมูล

การติดตามตรวจสอบและควบคุมการใช้งานฐานข้อมูลเป็นขบวนการรักษาความปลอดภัยที่ดีอย่างหนึ่ง การตรวจสอบข้อมูลอย่างสม่ำเสมอเพื่อให้มั่นใจว่ากฎ ระเบียบ มาตรฐานที่ได้กำหนดไว้ได้มีการใช้งานจริง องค์กรส่วนใหญ่จะมีกลุ่มคนที่ทำหน้าที่ตรวจสอบแยกจากกลุ่มผู้ใช้และพัฒนาระบบ การตรวจสอบนี้มักจะทำทุกส่วนที่เกี่ยวข้องตั้งแต่ระบบคอมพิวเตอร์ รวมถึงคู่มือการใช้งานและคู่มือระบบด้วย

1.วัตถุประสงค์ในการติดตามและควบคุมการใช้งานฐานข้อมูล

วัตถุประสงค์ในการติดตามและควบคุมการใช้งานฐานข้อมูลเพื่อ

1.1 เพื่อให้มั่นใจว่าข้อมูลนำเข้าถูกต้อง ผู้ตรวจสอบจะตรวจสอบว่ามีการตรวจสอบข้อมูลนำเข้าเบื้องต้นครบถ้วนหรือไม่ รวมทั้งมีการป้องกันในระดับระบบจัดการฐานข้อมูลและโปรแกรมดีเพียงพอหรือไม่

1.2 เพื่อให้มั่นใจว่ากระบวนการทำงานถูกต้อง การตรวจสอบจะรวมถึงพิธีปฏิบัติ และรายละเอียดในการทำงานของระบบงานทุกขั้นตอน

1.3เพื่อป้องกันการเปลี่ยนแปลงแก้ไขโปรแกรมโดยไม่มีสิทธิ เมื่อระบบใช้งานจริงแล้ว ผู้ตรวจสอบจะทำการควบคุมไม่ให้มีการแก้ไขโปรแกรมเพื่อความปลอดภัยของระบบ

1.4 ตรวจสอบการใช้งานและสิทธิการใช้งานของผู้ใช้งาน เพื่อให้มั่นใจว่าไม่มีผู้ใช้งานที่ไม่มีสิทธิอยู่ในระบบและสิทธิต่างๆได้ถูกกำหนดไว้ถูกต้องเพื่อให้มั่นใจว่าคู่มือต่างๆ ได้รับการปรับปรุงให้ทันสมัยอยู่เสมอ

2.การติดตามและตรวจสอบการใช้งานข้อมูล

การตรวจสอบทุกด้านข้างต้นจะต้องทำอย่างมีประสิทธิภาพ โดยผู้ตรวจสอบอาจสุ่มตรวจเป็นระยะ ไม่มีการแจ้งล่วงหน้า หรืออาจจะกำหนดการตรวจเป็นตารางแน่นอนและต้องทำอย่างสม่ำเสมอ ทั้งนี้การตรวจเกี่ยวกับระบบฐานข้อมูลจำเป็นต้องติดต่อประสานงานกับผู้บริหารฐานข้อมูลอย่างใกล้ชิด ส่วนมากจะเริ่มตั้งแต่การร่วมออกแบบระบบฐานข้อมูลด้วย

ผู้บริหารฐานข้อมูลมีหน้าที่ในการที่จะต้องเก็บบันทึกการใช้งานต่างๆ ตามที่ผู้ตรวจสอบต้องการ ทั้งนี้ขึ้นอยู่กับความเหมาะสมว่าจะใช้บันทึกการปฏิบัติงานที่มักจะมีมาพร้อมกับระบบจัดการฐานข้อมูล หรือจะพัฒนาขึ้นเองเป็นส่วนหนึ่งในการพัฒนาระบบงาน

3. การควบคุมการใช้งานฐานข้อมูล

การควบคุมการใช้งานฐานข้อมูลเป็นส่วนหนึ่งในการรักษาความปลอดภัย การควบคุมการใช้งานฐานข้อมูลอาจแยกออกเป็น 2 ด้าน ได้แก่ การควบคุมทางกายภาพ (physical control) และการควบคุมการเข้าถึงข้อมูล (access control)

3.1.การควบคุมทางกายภาพ เป็นการควบคุมในส่วนภายนอกระบบฐานข้อมูล การควบคุมในส่วนนี้เป็นการควบคุมและป้องกันความเสียหายโดยทั่วไป ได้แก่

-การป้องกันภัยจากน้ำท่วม ไฟไหม้ ภัยจากระบบไฟฟ้าเสียหาย
-การล็อกห้องคอมพิวเตอร์อย่างหนาแน่นเมื่อไม่มีการใช้งานแล้ว การใช้ยามเฝ้า
-เก็บข้อมูลที่ทำการสำรองไว้ในสถานที่ต่างหาก เช่น ในบริเวณที่ห่างไกลจากระบบคอมพิวเตอร์ที่มีอยู่ เพื่อเป็นการป้องกันภัยที่อาจเกิดขึ้นและอาจทำลายระบบไปพร้อมกับระบบสำรองข้อมูล เช่นการเกิด ไฟไหม้หรือน้ำท่วม เป็นต้น
-การวางแผนล่วงหน้าในกรณีฉุกเฉิน(contingency plan)โดยการใช้ระบบสำรองข้อมูล(back up disk) สำหรับการทำข้อมูลสำรองอย่างสม่ำเสมอเพื่อใช้ในกรณีที่ระบบเกิดความเสียหายไม่สามารถเรียกคืนได้ ตรวจสอบกระบวนการทำสำรองข้อมูลอย่างสม่ำเสมอ เพื่อดูว่ากระบวนการนั้นได้ทำการสำรองข้อมูลไว้อย่างถูกต้องและครบถ้วน
-ต้องทำลายข้อมูลหรือลบข้อมูลที่ไม่ใช้แล้วอย่างปลอดภัย และไร่ร่องรอย ซึ่งอาจทำได้ โดยการลบหลายๆครั้ง หรือใช้เทคนิคอย่างอื่นเข้าช่วย มิใช่เพียงแต่งเขียนข้อมูลใหม่ทับซ้ำลงไปเท่านั้น เนื่องจากว่าการกระทำเช่นนี้ไม่สามารถทำลายข้อมูลเก่าให้หมดไปได้อย่างไร่ร่องรอย เพราะอาจมีการใช้เทคนิคชนิดพิเศษต่างๆมาทำการอ่านข้อมูลเก่าที่ถูกทับไว้ได้
-สื่อที่ใช้ในการบันทึกข้อมูลเมื่อต้องการจะทิ้งหรือไม่ต้องการแล้วต้องทำลายให้ดี เพื่อป้องกันการแอบนำสื่อเหล่านั้นกลับมาอ่านข้อมูลที่หลงเหลืออยู่ได้
-มีโปรแกรมที่สามารถเก็บสำรองข้อมูลไว้ได้โดยอัตโนมัติและสม่ำเสมอ โดยไม่ต้องใช้ผู้ดูแลระบบมาทำการเก็บสำรองข้อมูลด้วยตนเองเพราะเกิดความไม่สม่ำเสมอ โดยไม่ต้องใช้ผู้ดูแลระบบมาทำการเก็บสำรองข้อมูลด้วยตนเองเพราะอาจเกิดความไม่สม่ำเสมอและข้อผิดพลาดได้

3.2.การควบคุมการเข้าถึงระบบ ควรมีการควบคุมความปลอดภัยในการเข้าถึงระบบซอฟต์แวร์และฮาร์ดแวร์ของระบบฐานข้อมูล และส่วนอื่นๆ ที่เกี่ยวข้องกับการทำงาน โดยมีการควบคุมดังนี้
-ควบคุมความปลอดภัยโดยระบบปฏิบัติการ(operating system controls)หรือระบบจัดการฐานข้อมูล ควรมีการควบคุมสิทธิการเข้าถึงและการใช้ข้อมูลในส่วนต่างๆภายในระบบคอมพิวเตอร์ของผู้ใช้ การมีระบบบันทึกเหตุการณ์ต่างๆในระบบ(security log)ไว้โดยอัตโนมัติเพื่อใช้เป็นหลักฐานการตรวจสอบ(audit trail)
-ควบคุมความปลอดภัยในการเข้าถึงระบบฮาร์ดแวร์อาจควบคุมโดย เทคโนโลยีทางฮาร์ดแวร์ได้มีการออกแบบสถาปัตยกรรมขั้นพื้นฐานในการรักษาความปลอดภัยที่สามารถควบคุมการเข้าถึงระบบได้อย่างดี เช่น การใช้สมาร์ดการ์ดในการควบคุมการใช้ การใช้วงจรเฉพาะกิจเชื่อมต่อกับหน่วยความจำ เพื่อตรวจสอบ ป้องกัน และกำจัดเวลาในการใช้ เป็นต้น
-ผู้ใช้แต่ละคนจะต้องมีชื่อผู้ใช้(user name) และรหัสผ่าน(password) ที่แตกต่างกันออกไปในแต่ละคน
-ระบบการตรวจสอบ จะต้องมีหลักฐานการตรวจสอบ(audit trial) จะต้องบันทึกว่าผู้ใช้เป็นใคร ทำอะไร จากที่ไหน และทำสำเร็จหรือไม่จะต้องบันทึกการเข้าสู่ระบบของผู้ใช้(events logging)แฟ้มข้อมูลของระบบตรวจสอบจะต้องได้รับการปกป้องและตรวจสอบเสมอ

-ควบคุมการเข้าถึงข้อมูลโดยต้องจำแนกแยกแยะสิทธิในการกระทำต่อส่วนต่างๆของระบบและจำแนกแยกแยะระหว่างผู้ใช้กลุ่มต่างๆ เช่น ผู้ใช้กลุ่มใดมีสิทธิในการใช้ระบบแฟ้มข้อมูล (file system) มีการแบ่งหน่วยความจำ (shared memory)

-มีโปรแกรมที่สามารถเก็บสำรองข้อมูลไว้ได้โดยอัตโนมัติและสม่ำเสมอ โดยไม่ต้องใช้ผู้ดูแลระบบมาทำการเก็บสำรองข้อมูลด้วยตนเองเพราะอาจเกิดความไม่สม่ำเสมอและข้อผิดพลาดได้

-ควบคุมความปลอดภัยในการเข้าถึงระบบเครือข่าย การรักษาความปลอดภัยของข้อมูลในระบบเครือข่ายนั้นจะต้องทำให้ทั่วถึงทั้งระบบ จะทำเฉพาะจุดใดจุดหนึ่งไม่ได้ สิ่งที่ต้องควบคุมก็คือ ความลับของข้อมูลที่ส่งผ่านในระบบเครือข่าย และการตรวจสอบความถูกต้องของผู้ใช้ รวมถึงการตรวจสอบความถูกต้องของระบบคอมพิวเตอร์ที่จะเข้ามาทำการเชื่อมต่อเข้าสู่ระบบเครือข่าย การรักษาความปลอดภัยต้องคำนึงถึง การควบคุมการอนุญาตให้เข้ามาในระบบ(access control) การตรวจสอบความถูกต้องระบบคอมพิวเตอร์ในระบบเครือข่าย(authentication in distribute system) การรักษาความถูกต้องของข้อมูลที่ส่งผ่านระบบเครือข่าย (data integrity) และการใช้ตัวป้องกันการบุกรุกหรือกำแพงไฟ(firewall)ในการรักษาความปลอดภัยของระบบเครือข่าย

-ควบคุมการอนุญาตให้เข้ามาในระบบเครือข่าย เป็นการป้องกันการเข้าระบบโดยผ่านช่องทางหรือพอร์ต (port) ต่างๆที่มีอยู่ในระบบ โดยใช้ฮาร์ดแวร์และซอฟต์แวร์และการกำหนดระดับสิทธิในการเข้าถึงข้อมูลที่ต่างกัน เช่น กำหนดสิทธิในการเข้าถึงข้อมูลบางส่วนเท่านั้นสำหรับผู้ที่มีสิทธิหรือสามารถเพียงแค่ในการอ่านข้อมูลเท่านั้น แต่ไม่มีสิทธิในการเปลี่ยนแปลงแก้ไขข้อมูล เป็นต้น

-การตรวจสอบความถูกต้องของระบบคอมพิวเตอร์ในระบบเครือข่าย(authentication in distribute system) เป็นการป้องกันการปลอมแปลงจากระบบคอมพิวเตอร์ที่ไม่ได้รับอนุญาตให้เข้ามาในระบบได้ ต้องมีวิธีในการการตรวจสอบความถูกต้องของระบบที่มาต่อเชื่อม โดยการตรวจสอบรหัสผ่านเพื่อใช้ในการตรวจสอบเซอร์ฟเวอร์(server) จากระบบอื่นๆที่จะเข้ามาทำการต่อเชื่อมได้

-การรักษาความถูกต้องของข้อมูลที่ส่งผ่านระบบเครือข่าย(data integrity)โดยการนำวิธีการติดต่อสื่อสารที่มีขั้นตอนและรูปแบบที่แน่นอนระหว่างระบบคอมพิวเตอร์ภายในเครือข่าย เช่น การใช้โพรโตคอล (protocol) มาตราฐาน การใช้ลายเซ็นอิเล็กทรอนิกส์(digital signature) การใช้ตัวป้องกันการบุกรุกหรือกำแพงไฟ (firewall)ในการรักษาความปลอดภัยของระบบเครือข่าย โดยใช้กำแพงไฟเป็นเครื่องมือในการตรวจสอบหรือปิดกั้นการเชื่อมต่อของข้อมูลจากระหว่างภายนอกระบบเครือข่ายกับภายในระบบเครือข่าย

ที่มา http://www.srisangworn.go.th/home/databaselearnx/ms1t2-12.htm