

สรุปการบรรยาย ครั้งที่ 1 (เช้า)
หลักสูตร e-Government Exchange Program
วันที่ 5 กันยายน 2557

หัวข้อการบรรยาย: **The Principles for Cloud Computing**

โดย คุณวิบูลย์ ภัทรพิบูล ผู้อำนวยการฝ่ายให้คำปรึกษา สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน)

ประเด็นการบรรยาย

1. ICT Trend
2. Risk Management
3. Service Level Agreement
4. ISO/IEC
5. CSA
6. Cloud Definition Framework
7. G-Cloud
8. EGA

ความก้าวหน้าทางเทคโนโลยีในยุคปัจจุบัน อันได้แก่

- WEB-SCALE IT
- SMART MACHINES
- 3D PRINTING
- THE ERA OF PERSONAL CLOUD
- SOFTWARE-DEFINED ANYTHING
- MOBILE DEVICE DIVERSITY AND MANAGEMENT
- MOBILE APPS AND APPLICATIONS
- THE INTERNET OF EVERYTHING
- HYBRID CLOUD & IT AS A SERVICE BROKER
- CLOUD/CLIENT ARCHITECTURE

นโยบายการบริหารความเสี่ยงในด้านต่างๆ ที่จะใช้ประกอบกับการดำเนินงาน อันได้แก่



- ความพร้อมในการทำงาน
- ประสิทธิภาพ
- การปฏิบัติตามข้อกำหนด
- ความปลอดภัยของข้อมูล

หลักการเบื้องต้นของข้อตกลงระดับบริการ หรือ (Service Level Agreement – SLA) อาทิเช่น

- RPO : Recovery Point Objective (การยอมรับการสูญหายของข้อมูล)
- RTO : Recovery time objective (ระยะเวลาที่ระบบกลับมาใช้งานได้)
- RPO/RTO Classes มีผลกับงบประมาณในเรื่องการบริหารจัดการ
- Disaster Recovery Site (DR Site)

ความสำคัญในการตัดสินใจในการเลือก DR Site ที่มีอยู่หลายรูปแบบ ได้แก่

1. Hot Site หมายถึง ระบบสำรองที่จะสามารถทำงานได้ทันที ที่ระบบหลักมีปัญหา มีลักษณะเช่นเดียวกับ Mirror Site ซึ่งหมายความว่าเรามีระบบสำรองที่ทำงานเหมือนระบบจริง ติดตั้งอยู่อีกสถานที่หนึ่งมีการเชื่อมต่อเครือข่ายถึงกันและปรับปรุงข้อมูลแบบเรียลไทม์
2. Warm Site หมายถึง ระบบสำรองที่สามารถทำงานได้ก็ต่อเมื่อ มีการติดตั้งข้อมูลที่อัปเดต ที่ได้จากการทำสำรองข้อมูล ต้องดำเนินการติดตั้ง อัปเดตข้อมูล ฐานข้อมูล หรือระบบงานบ้าง ถึงจะใช้งานได้ ปกติก็ประมาณ 1 วัน
3. Cold Site หมายถึง การจัดเตรียมสถานที่ และอุปกรณ์เบื้องต้นในระดับหนึ่ง ถ้ามีปัญหาจำเป็นจะต้องจัดซื้อระบบคอมพิวเตอร์เข้ามา และทำการติดตั้งใหม่ทั้งหมดไซต์แบบนี้ 3-5 วัน จึงจะสามารถใช้งานได้
4. Standby Site จัดการเฉพาะสถานที่ แต่ยังมีได้ดำเนินการใดๆ
5. Nothing ไม่มีการจัดเตรียมระบบสำรองใดๆ

ความจำเป็นที่ผู้บริหารต้องนำแนวการปฏิบัติของมาตรฐานสากลต่างๆเข้ามาเพื่อช่วยในการดำเนินงาน โดยมาตรฐานที่สำคัญๆ ได้แก่

- ISO/IEC 27001 Information Security Management Systems

เน้นในเรื่องความปลอดภัยด้านสารสนเทศ ทั้งด้าน Physical และ Logical โดยคำนึงถึงความเสี่ยงที่อาจเกิดขึ้นจากสารสนเทศ เช่น แสกเกอร์ ไวรัส หรือความเสี่ยงที่อันอาจก่อให้เกิดผลกระทบต่อองค์กร

- ISO/IEC 20000-1 Information Technology Service Management

เป็นแนวทางในการพัฒนางานบริการทางด้านไอที ซึ่งสามารถนำไปประยุกต์ใช้ได้ทั้งในองค์กรขนาดใหญ่และขนาดเล็ก โดยมีเป้าหมายในการเพิ่มประสิทธิภาพและปรับปรุงการให้บริการ ลดต้นทุน ในการดำเนินงาน และสร้างความพึงพอใจให้กับลูกค้า

- ISO 22301 Business Continuity Management Systems

มาตรฐานความปลอดภัยที่ช่วยลดความเสี่ยงด้านเทคโนโลยีสารสนเทศ ระบบสารสนเทศขององค์กรมีความจำเป็นอย่างยิ่งที่จะต้องเตรียมพร้อมและศึกษาถึงมาตรฐานทางการรักษาความปลอดภัยระบบสารสนเทศ

หน่วยงานที่ดูแลงานทางการรักษาความปลอดภัยของการทำงานในเทคโนโลยี Cloud (Cloud Security Alliance (CSA))

เป็นหน่วยงานทำหน้าที่วิจัยและเผยแพร่ความรู้ในประเด็นด้านความมั่นคงปลอดภัยของระบบการประมวลผลแบบกลุ่มเมฆ (Cloud Security) การให้ cloud computing นั้นก็มีความเสี่ยงจากภัยคุกคามเช่นเดียวกับการใช้เทคโนโลยีอื่นๆ โดยทาง CSA หรือ Cloud Security Alliance

รูปแบบของเทคโนโลยี (Cloud Definition Framework)

- Characteristics
- Service Models
- Deployment Models

ทำไมต้องใช้บริการ คลาวด์ภาครัฐ (Why G-Cloud)

- ประหยัดงบประมาณ
- ลดการบริหารจัดการด้านโครงสร้างพื้นฐานต่างๆ
- การบริหารทรัพยากรบุคคลที่ดีขึ้น
- EGA สามารถช่วยเหลือได้ทันที
- มาตรฐานการดำเนินงานระดับสากล

ก้าวต่อไปของหน่วยงานภาครัฐ

- ความสามารถในการดำเนินงานที่ไม่มีอุปสรรคทางด้านภัยพิบัติต่างๆ (Disaster recovery Site)
- การให้บริการภาคประชาชนที่เข้าถึงได้สะดวก (Government Application Center)
- การบูรณาการข้อมูลของหน่วยงานภาครัฐที่สมบูรณ์ (Open Data)
- การบริหารจัดการข้อมูลภาครัฐเพื่อประชาชน (Big Data)
- การดำเนินงานของหน่วยงานภาครัฐที่เป็นประโยชน์ในระบบงานต่างๆ (Smart)

ประเด็นสอบถามในระหว่างการบรรยาย และได้รับการอธิบายจากวิทยากรเรียบร้อยแล้ว

- สอบถามเกี่ยวกับการดำเนินงานด้าน Service Level Agreement – SLA ในหน่วยงานภาครัฐ
- สอบถามประเด็นเรื่องการคำนวณในเรื่อง RPO : Recovery Point Objective (การยอมรับการสูญหายของข้อมูล) และ RTO : Recovery time objective (ระยะเวลาที่ระบบกลับมาใช้งานได้)