ขั้นตอนปฏิบัติสำหรับการจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย และการเตรียมความพร้อมของหน่วยงาน

กำพล ศรธนะรัตน์

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์

(ก.ล.ต.)

ก.ล.ต. กับการนำ IT มาใช้งาน

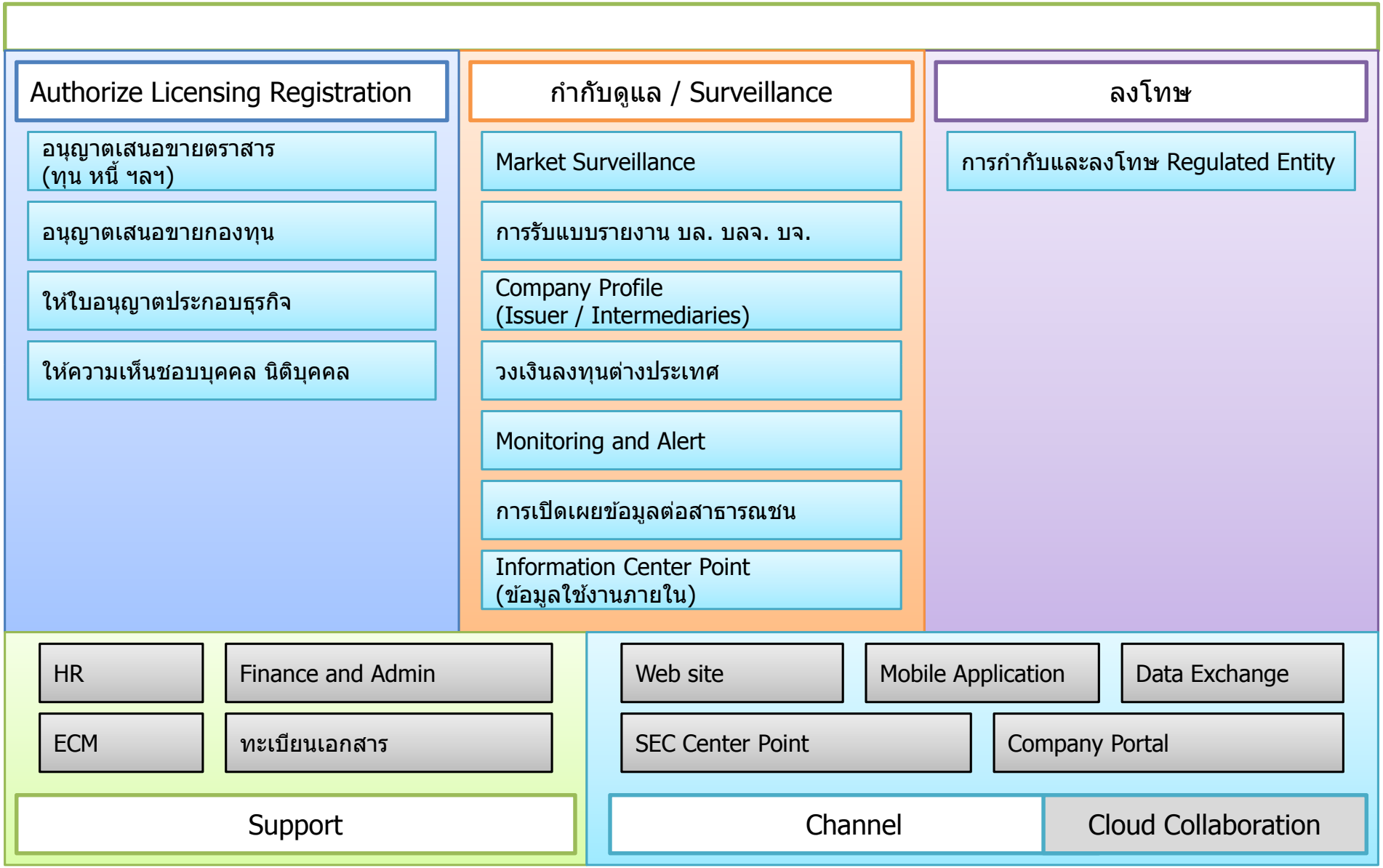
- บทบาทในการกำกับดูแลและพัฒนาตลาดทุน
- Mission – “Possibility Provider”
- Portfolio Workload
- GRC Framework
- Enterprise Architecture

Portfolio Workload

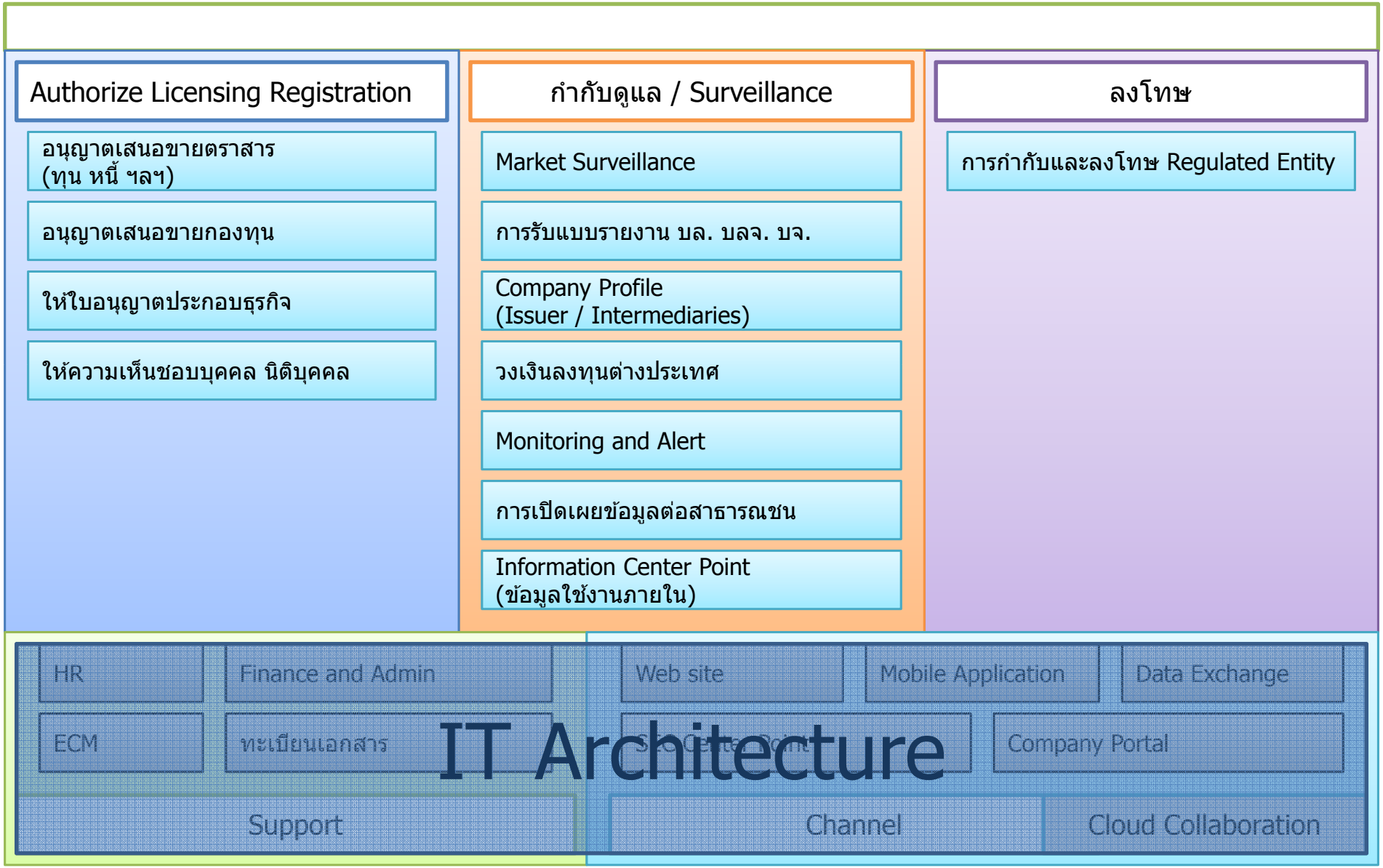
Information Provider (25%)		Application Development (40%)		Infrastructure (35%)	
Project (60%)	Operation (40%)	Project (60%)	Operation (40%)	Project (30%)	Operation (70%)

GRC Framework

Enterprise Architecture



Enterprise Architecture



กระบวนการจัดทำนโยบายและแนวปฏิบัติ

ความต้องการของกฎหมาย (พ.ร.ฎ. ภายใต้มาตรา 35)

- กำหนดเอกสารอิเล็กทรอนิกส์ ให้มีลักษณะ ครบถ้วนอ้างอิงภายหลังได้ กำหนดอายุของเอกสาร ต้องระบุตัวเจ้าของข้อมูลและรับรองข้อมูลได้ ต้องแจ้งการตอบรับว่าได้ดำเนินการ
- กำหนดนโยบายและแนวปฏิบัติเพื่อความมั่นคงปลอดภัยของสารสนเทศ อย่างน้อย 3 เรื่องได้แก่ Access Control, BCP , Risk Assessment and Compliance (3 of 11)
- กำหนดนโยบายและแนวทางปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล

กระบวนการจัดทำนโยบายและแนวปฏิบัติ (ต่อ)

ความต้องการของกฎหมาย (พ.ร.ฎ. ภายใต้มาตรา 35)

- กำหนดเอกสารอิเล็กทรอนิกส์ ให้มีลักษณะ ครบถ้วนอ้างอิงภายหลังได้ กำหนดอ[illegible] ต้องแจ้งการตอบรับว่าได้ดำเนินการ

  Done with Infrastructure Development

- กำหนดนโยบายและแนวปฏิบัติเรื่องความปลอดภัยของสารสนเทศ อย่างน้อยเรื่องที่เกี่ยวกับ Access Control, BCP , Risk Assessment (3 of 11)

  2544 / 2546/ 2555

  ผ่านความเห็นชอบของคณะกรรมการธุรกรรม 16 ธ.ค. 2553

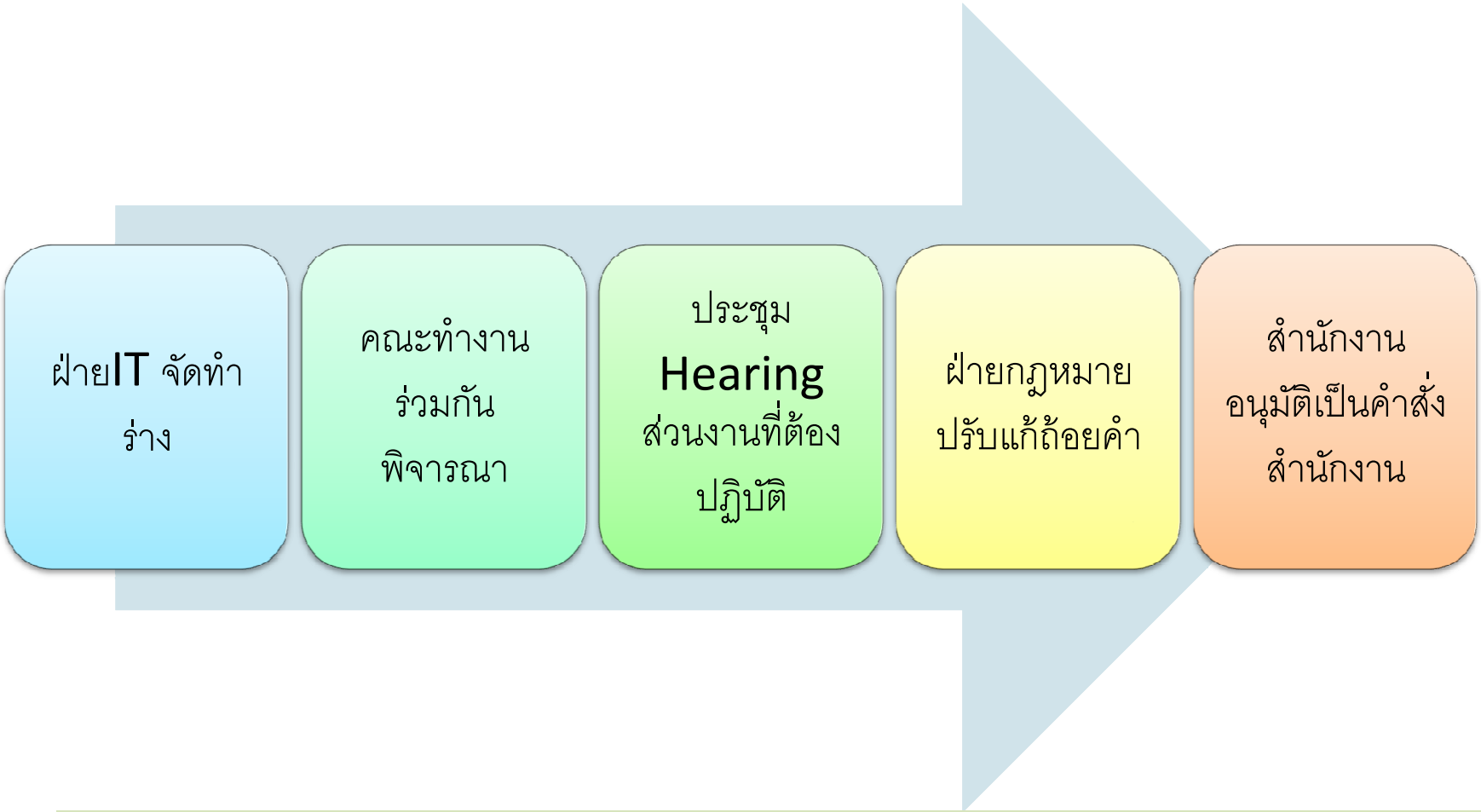
- กำหนดนโยบาย[illegible]ส่วนบุคคล

  Done and published on website

ขั้นตอนการทำและการเตรียมความพร้อม

- แต่งตั้งคณะทำงานจากทุกส่วนงาน โดยมีฝ่ายIT และฝ่ายกฎหมายเป็นทีมเลขา และฝ่ายตรวจสอบกิจการภายใน เป็นผู้สังเกตการณ์
- ประชุม หารือ อภิปราย จากต้นร่างที่ฝ่ายIT จัดทำขึ้นตามแนวทางของ ISO/IEC 17799, 27001, 27002 เพื่อให้มั่นใจว่า
  - สอดคล้องตาม Best Practice และ
  - สามารถปฏิบัติได้จริง
- ร่างสุดท้าย ฝ่ายกฎหมายปรับปรุงการใช้คำให้ครอบคลุมตามเจตนารมณ์
- ประกาศเป็นคำสั่งสำนักงาน กรณีละเมิดหรือกระทำผิด ถือเป็นผิดวินัยพนักงาน และผิดตามกฎหมายอื่นแล้วแต่กรณี

เพื่อให้รองรับ พ.ร.ฎ. ภายใต้มาตรา 25



ระยะเวลาดำเนินการ ประมาณปีเศษ เพื่อให้มีนโยบายและแนวปฏิบัติที่สอดคล้องกับมาตรฐาน และสามารถปฏิบัติได้จริง ภายใต้บริบทการทำงานของสำนักงาน

มุมมอง / ทัศนคติ

- เป็นงานต่อเนื่อง – continuing process
  - มีการ monitor/enforce การใช้งานให้สอดคล้องกับแนวปฏิบัติ
  - ออก security awareness อย่างสม่ำเสมอ
    - ตามข่าว/ภัย ที่เกิดใหม่
    - การเปลี่ยนแปลงของเทคโนโลยี
    - การหมุนเวียนของคน
  - สร้าง risk-aware culture ผ่านการ monitor แบบ proactive
  - Log consolidation and analysis / daily and monthly activities – sense and respond
  - Top management Involvement
  - Good infrastructure and PPT

DISCUSSION

KUMPOL AT SEC DOT OR DOT TH