**รายงานผลการจัดลำดับความสำคัญที่หน่วยงานกำหนดความต้องการขั้นต้นร่วมกัน**
**ตามกรอบการทำงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ของประเทศไทย**
**(Thailand's National Cloud Security Framework)**

---

จากการส่งแบบสอบถามเกี่ยวกับการเตรียมความพร้อมของหน่วยงานด้าน Cloud Security ตามกรอบการทำงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ของประเทศไทย (Thailand's National Cloud Security Framework) ไปยังหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ผู้เชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สถาบันการศึกษา หน่วยงานกำหนดนโยบาย ผู้ให้บริการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และผู้ให้บริการคลาวด์ทั้งภายในและต่างประเทศ โดยหน่วยงานที่ต้องตอบแบบสอบถามฯ ถูกจัดประเภทตามบทบาทหน้าที่หรือความเกี่ยวข้องกับมาตรฐานความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567 รวม 7 กลุ่ม ได้แก่

1. คณะกรรมการระดับชาติที่เกี่ยวข้องกับดิจิทัลหรือไซเบอร์ (ไม่มีผู้ตอบแบบสอบถาม)
2. ผู้ใช้บริการคลาวด์ (Cloud Service Customer) (มีผู้ตอบแบบสอบถาม 210 หน่วยงาน)
3. ผู้ให้บริการคลาวด์ (Cloud Service Provider) (มีผู้ตอบแบบสอบถาม 13 หน่วยงาน)
4. หน่วยงานตรวจสอบและให้การรับรอง (Certification Bodies) (มีผู้ตอบแบบสอบถาม 1 หน่วยงาน)
5. ผู้ให้บริการด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Provider) (มีผู้ตอบแบบสอบถาม 10 หน่วยงาน)
6. หน่วยงานควบคุมหรือกำกับดูแล (Regulator) (มีผู้ตอบแบบสอบถาม 14 หน่วยงาน)
7. หน่วยงานกำหนดนโยบาย (Policy maker) (มีผู้ตอบแบบสอบถาม 4 หน่วยงาน)

และหน่วยงานอื่น ๆ ที่ไม่ได้มีการระบุข้อมูลในแบบสอบถามฯ ทั้ง 7 กลุ่ม มีผู้ตอบแบบสอบถามจำนวน 27 หน่วยงาน ประกอบด้วย 1) หน่วยงานของรัฐ 2) หน่วยงานภายใต้การกำกับของรัฐ 3) หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) 4) ทั้งหน่วยงานของรัฐ และหน่วยงาน Regulator 5) สถาบันการศึกษา 6) ผู้ให้บริการคลาวด์เฉพาะภายในหน่วยงาน 7) ผู้ตรวจประเมินภายนอกของระบบคลาวด์ 8) ผู้ตรวจสอบภายในองค์กร 9) หน่วยงานฝ่ายเทคโนโลยีสารสนเทศหรือผู้ที่เกี่ยวข้อง 10) กลุ่มงานปฏิบัติการและบริการลูกค้า 11) ไม่ใช่ทั้ง CSC และ CSP 12) ไม่มีระบบคลาวด์ และ 13) ไม่ทราบ และ 14) ไม่ระบุ

โดย สกมช. ได้นำผลจากแบบสอบถามฯ มาวิเคราะห์และจัดลำดับความสำคัญเพื่อจัดทำแผนบูรณาการในการขับเคลื่อนการดำเนินงานตามมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของระบบคลาวด์ (ระยะเวลา 5 ปี) ก่อนที่จะใช้บังคับต่อไป ซึ่งแบบสอบถามดังกล่าวได้ถูกจัดส่งไปยังหน่วยงาน รวมทั้งสิ้น จำนวน 507 หน่วยงาน พบว่า มีหน่วยงานที่ตอบแบบสอบถามกลับมา รวมทั้งสิ้น จำนวน 279 หน่วยงาน สามารถสรุปผลแบบสอบถามฯ ตามลำดับความสำคัญที่หน่วยงานกำหนดความต้องการขั้นต้นร่วมกัน ตามกรอบการทำงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ของประเทศไทย (Thailand's National Cloud Security Framework) ได้ดังนี้

สรุปรายการความต้องการขั้นต้นในขั้นกำหนดความต้องการร่วมกัน (Mutually Identify the Preliminary National Cloud Security Requirements) คือสิ่งที่หน่วยงานจำเป็นต้องใช้ในการนำมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ไปสู่การปฏิบัติเพื่อให้สามารถบรรลุผลได้อย่างมีประสิทธิภาพ และประสิทธิผล มีรายละเอียดดังต่อไปนี้

A. หลักเกณฑ์และวิธีการแบ่งความรับผิดชอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับการประมวลผลคลาวด์

B. หลักเกณฑ์และวิธีการตรวจรับรองโดยการประเมินตนเอง (Self-assessment)

C. หลักเกณฑ์และวิธีการตรวจรับรองโดยหน่วยงานควบคุมหรือกำกับดูแล (Attestation)

D. หลักเกณฑ์และวิธีการตรวจรับรองโดยหน่วยงานให้บริการตรวจรับรอง (Certify Body)

E. หลักเกณฑ์และวิธีการตรวจรับรองโดย สกมช. ให้กับหน่วยงานให้บริการตรวจรับรอง

F. แนวปฏิบัติประกอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567

G. คำอธิบายเพิ่มเติมเกี่ยวกับคำศัพท์ที่ใช้ใน ประกาศ กมช. เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567

H. ความสอดคล้องระหว่าง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567 กับมาตรฐานสากล

I. เครื่องมือ และเอกสารต้นแบบ (Templates)

J. บุคลากรผู้ทำหน้าที่ตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ (Cloud Security Auditor) และผู้ปฏิบัติงานด้านความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ (Cloud Security Professional)

K. แพลตฟอร์มกลางหรือระบบฐานข้อมูลเพื่อสนับสนุนหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

L. กรอบการบริหารความเสี่ยงทางไซเบอร์ต่อระบบคลาวด์ (Cloud Security Risk Management Framework) สำหรับหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Risk Management Framework for Cloud Security)

M. โมเดลสถาปัตยกรรมด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์

N. เอกสาร White Paper เพื่ออธิบายประกาศ คำสั่ง หลักเกณฑ์และวิธีการเพื่อปฏิบัติตามมาตรฐานคลาวด์

O. ทีมเฉพาะกิจจาก สกมช. เพื่อดำเนินการและประสานงานในการแก้ไขปัญหาและอุปสรรคต่าง ๆ

P. เครื่องมือประเมินผลการปฏิบัติตามมาตรฐาน (Compliance Assessment Tools)

Q. คู่มือแนวปฏิบัติ (Guideline Manuals) ที่ปรับใช้ตามประเภทข้อมูล (Security Categorization)

R. ฐานข้อมูลผู้ให้บริการคลาวด์ที่ผ่านการรับรอง (Certified CSP Directory)

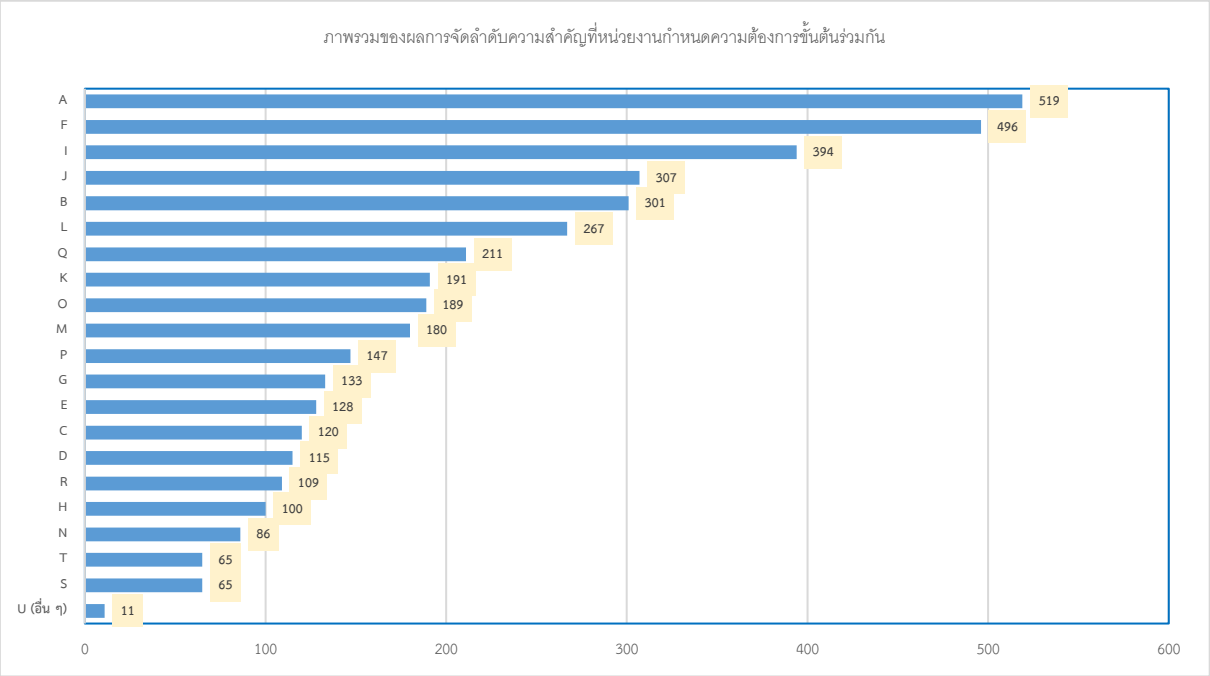
S. แนวทางการปฏิบัติด้าน Data Residency & Localization

T. แพลตฟอร์มการรับรองและอัพเดตมาตรฐานสำหรับ CSP/CSC (Certification Portal)

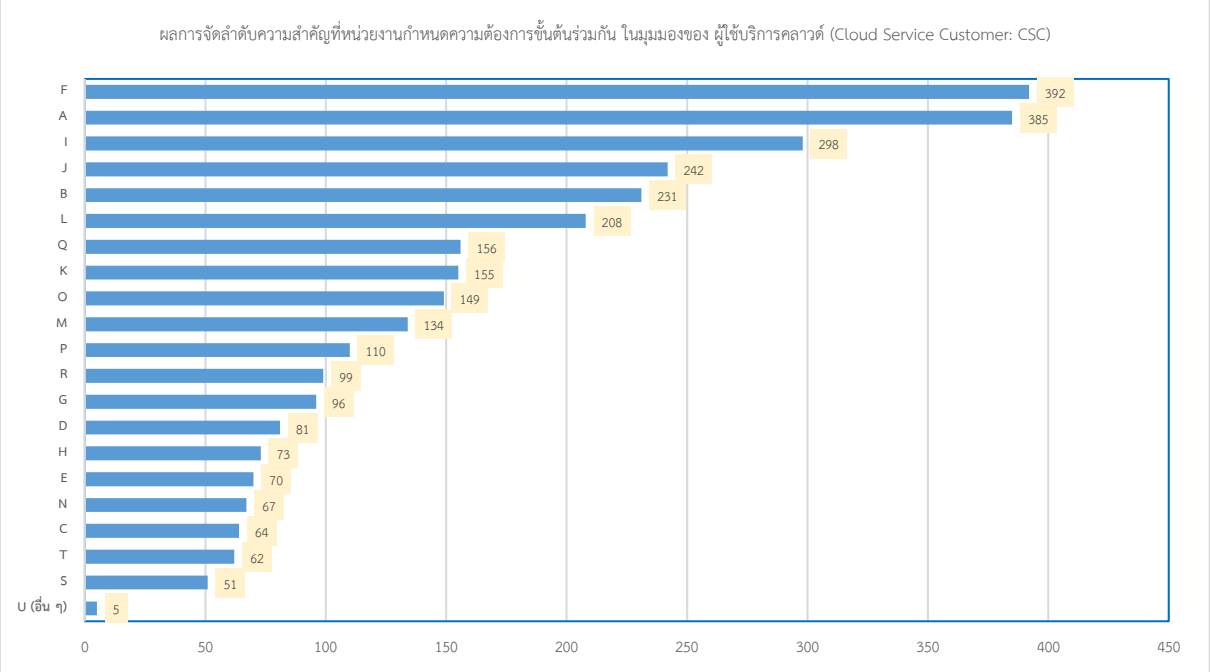
U. อื่น ๆ

โดยมีหน่วยงานที่ร่วมตอบแบบสอบถามฯ ได้เลือกรายการตามความต้องการขั้นต้นในขั้นกำหนดความต้องการร่วมกันมา 5 ลำดับ (A - T) ซึ่งความต้องการนี้ คือสิ่งที่หน่วยงานจำเป็นต้องใช้ โดยเริ่มจากปัจจัยที่สำคัญที่สุดในการนำมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ ไปสู่การปฏิบัติเพื่อให้สามารถบรรลุผลได้อย่างมีประสิทธิภาพ ซึ่งใช้หลักเกณฑ์ในการให้คะแนนและจัดลำดับความสำคัญนี้อาศัยการให้ค่าน้ำหนักตามลำดับที่หน่วยงานซึ่งตอบแบบสอบถามฯ ได้ระบุ โดยลำดับที่ 1–5 มีค่าน้ำหนักเท่ากับ 5, 4, 3, 2 และ 1 ตามลำดับ และกรณีที่มีการระบุเกิน 5 ลำดับ ให้รายการตั้งแต่ลำดับที่ 6 เป็นต้นไปมีค่าน้ำหนักเทียบเท่าลำดับที่ 5 (1 คะแนน) จากนั้นนำคะแนนของแต่ละตัวเลือกที่ได้จากหน่วยงานซึ่งตอบแบบสอบถามฯ ทั้งหมดมารวม แล้วเรียงลำดับผลคะแนนรวมจากมากไปหาน้อย ทั้งนี้ ในกรณีคะแนนรวมเท่ากันให้พิจารณาจำนวนครั้งที่ได้รับลำดับที่ 1 มากกว่าเป็นอันดับก่อน และหากยังเท่ากันให้พิจารณาจำนวนการปรากฏรวมถัดไป โดยยึดเฉพาะตัวอักษร A - T ที่ปรากฏจริงในคำตอบ ส่วนรายการที่ว่างหรืออยู่นอกเกณฑ์จะไม่ถูกนำมาคิดคะแนน

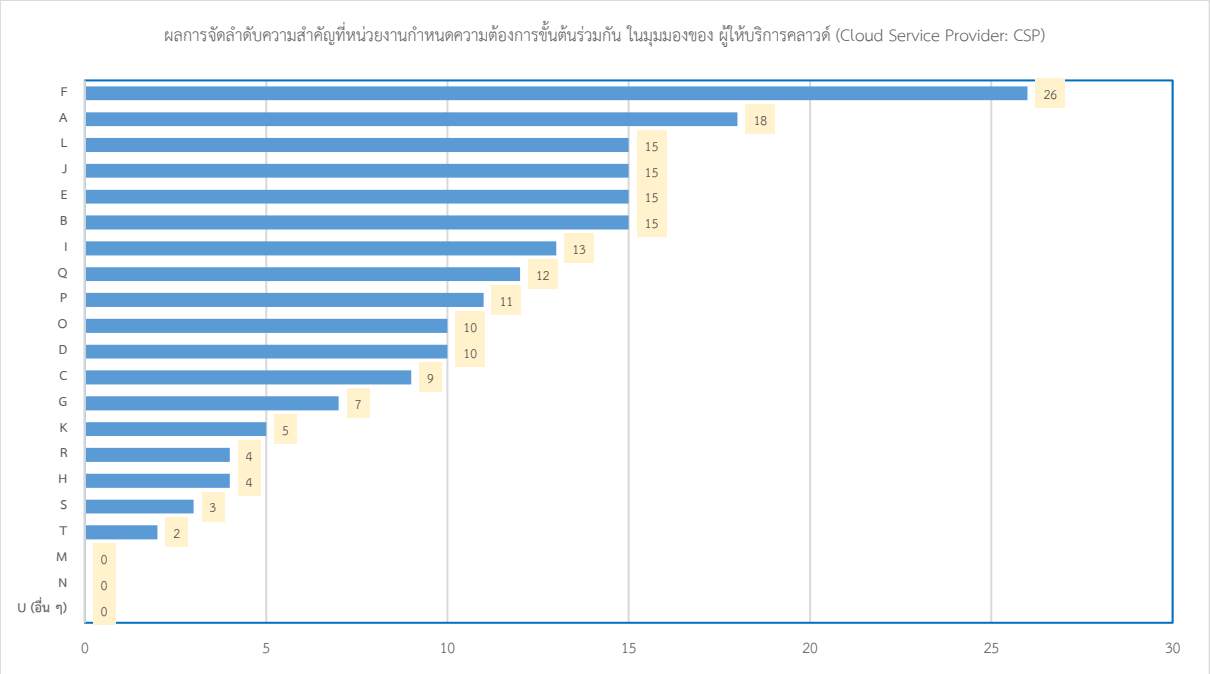
**แผนภูมิที่ 1** : แสดงภาพรวมของผลการจัดลำดับความสำคัญที่หน่วยงานกำหนดความต้องการขั้นต้นร่วมกัน



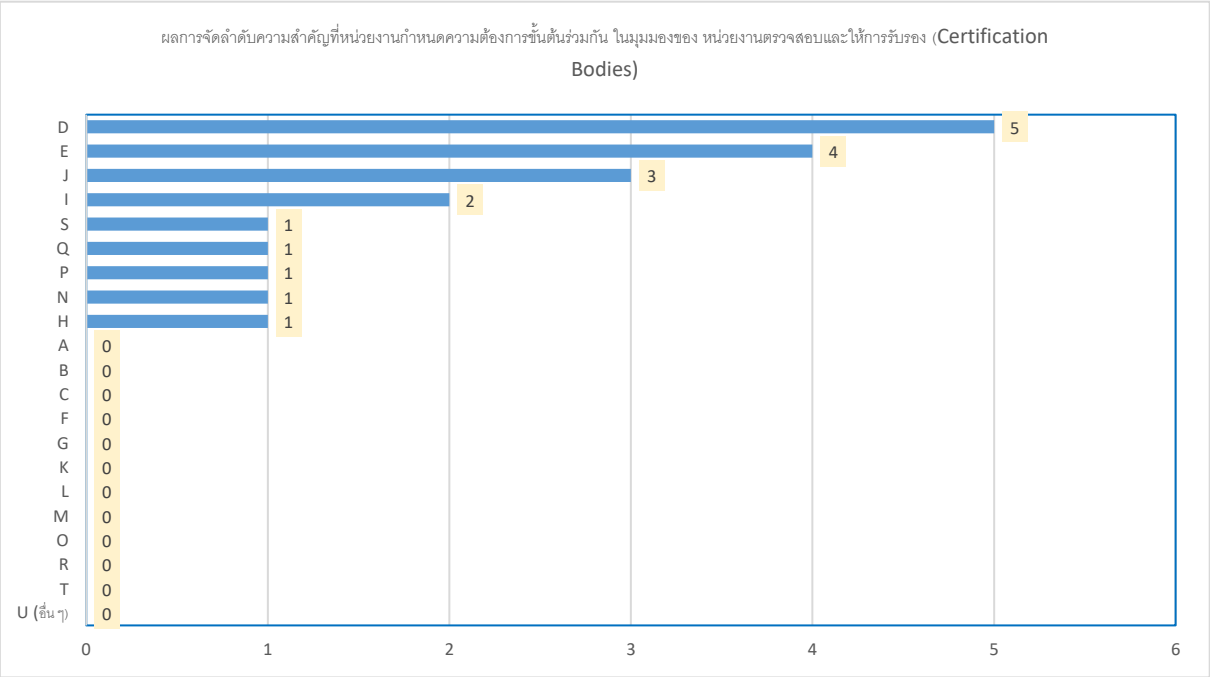

**แผนภูมิที่ 2** : แสดงผลการจัดลำดับความสำคัญที่หน่วยงานกำหนดความต้องการขั้นต้นร่วมกัน ในมุมมองของผู้ใช้บริการคลาวด์ (Cloud Service Customer)



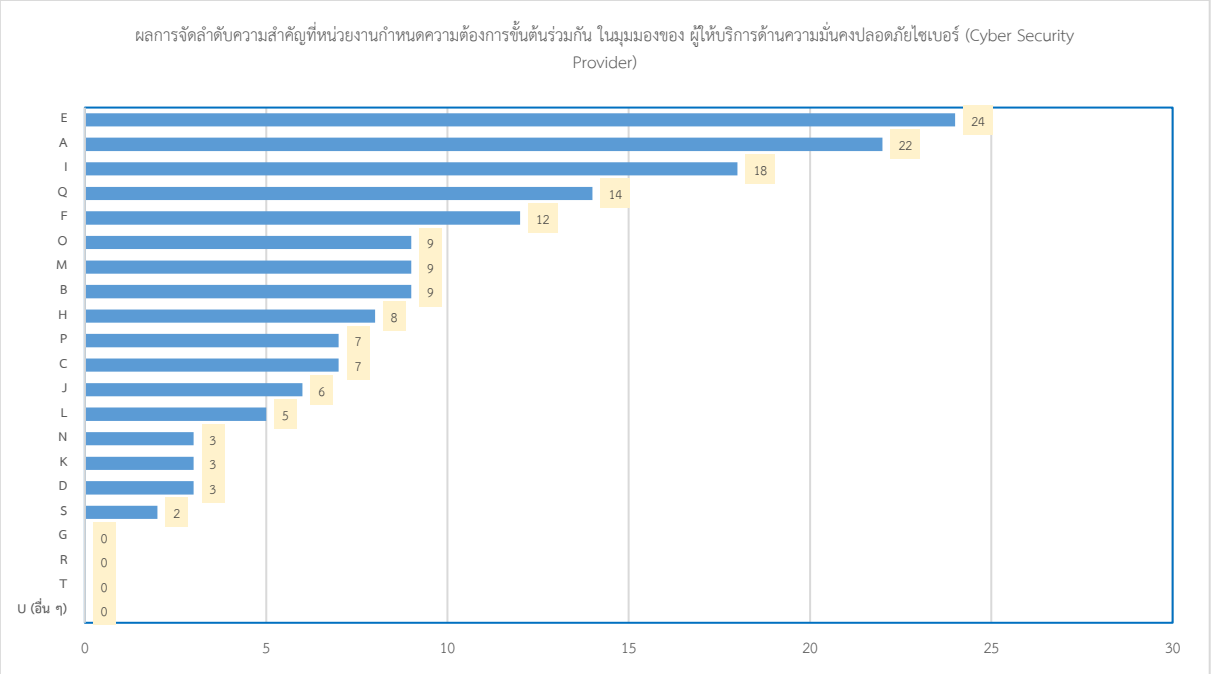
**แผนภูมิที่ 3** : แสดงผลการจัดลำดับความสำคัญที่หน่วยงานกำหนดความต้องการขั้นต้นร่วมกัน ในมุมมองของผู้ให้บริการคลาวด์ (Cloud Service Provider)



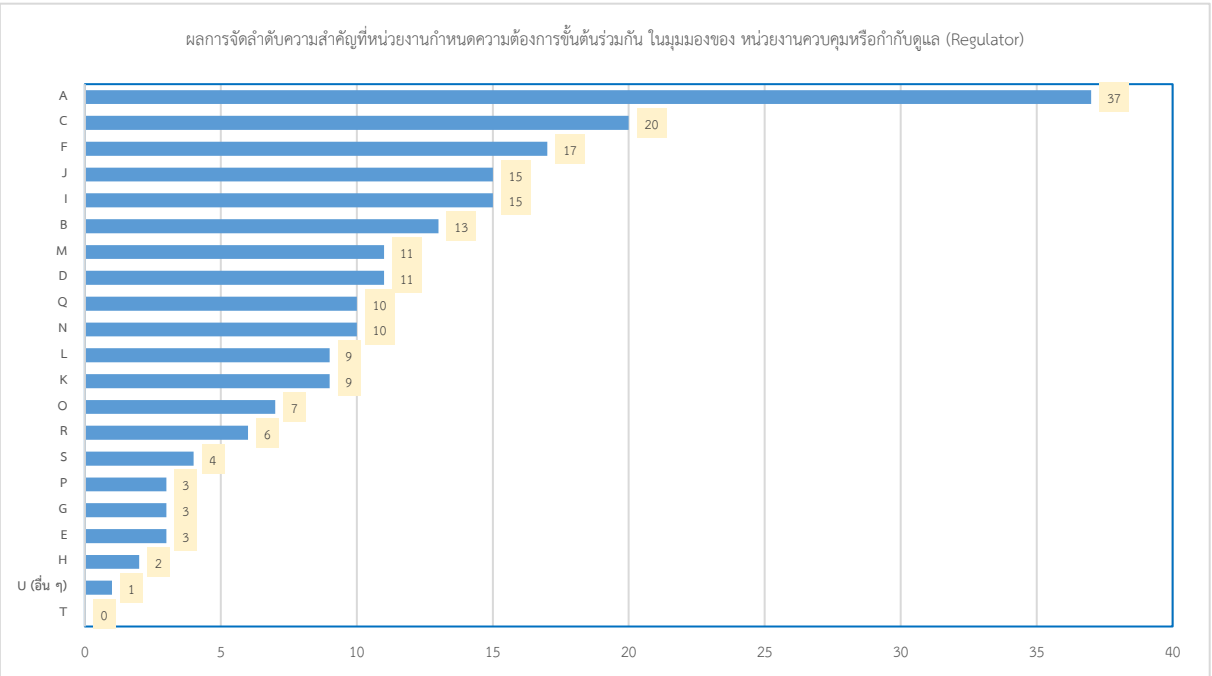

**แผนภูมิที่ 4** : แสดงผลการจัดลำดับความสำคัญที่หน่วยงานกำหนดความต้องการขั้นต้นร่วมกัน ในมุมมองของหน่วยงานตรวจสอบและให้การรับรอง (Certification Bodies)



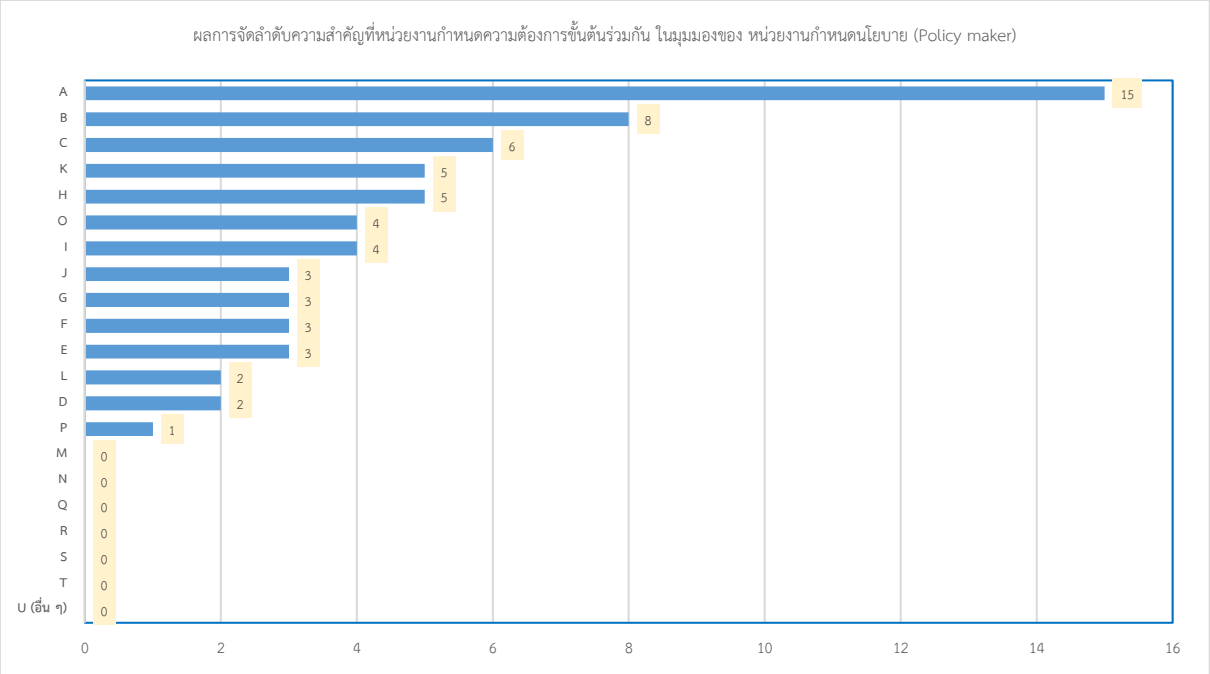
**แผนภูมิที่ 5** : แสดงผลการจัดลำดับความสำคัญที่หน่วยงานกำหนดความต้องการขั้นต้นร่วมกัน ในมุมมองของผู้ให้บริการด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Provider)



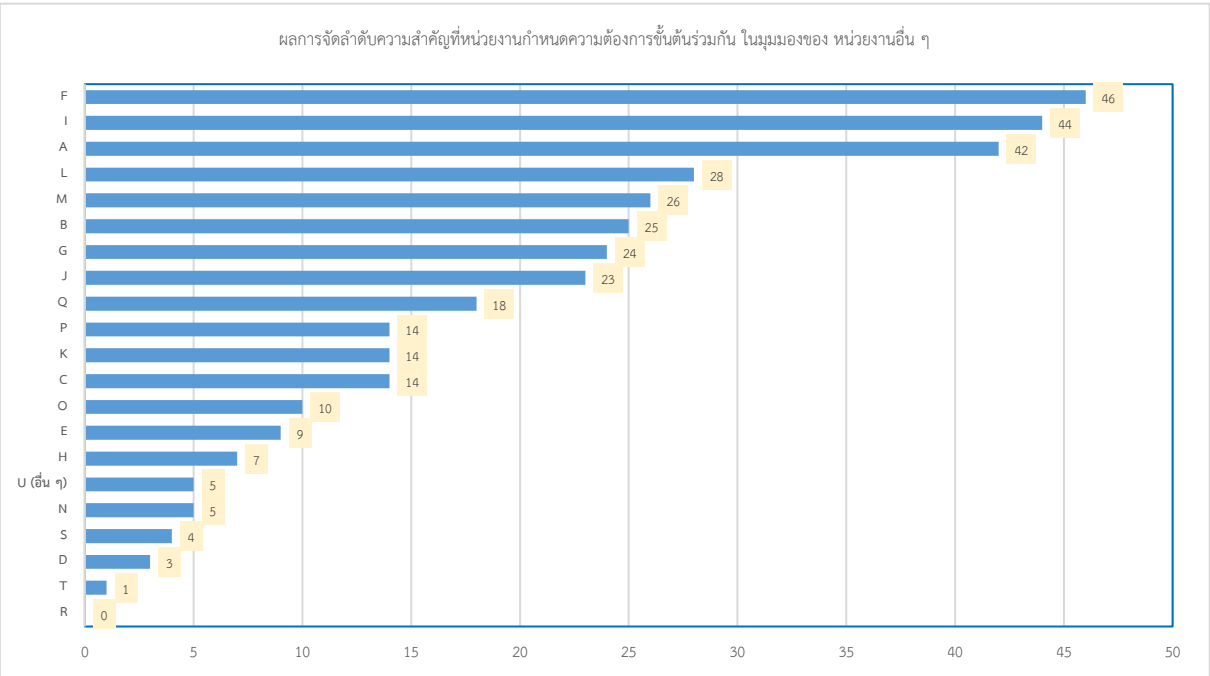

**แผนภูมิที่ 6** : แสดงผลการจัดลำดับความสำคัญที่หน่วยงานกำหนดความต้องการขั้นต้นร่วมกัน ในมุมมองของหน่วยงานควบคุมหรือกำกับดูแล (Regulator)



**แผนภูมิที่ 7** : แสดงผลการจัดลำดับความสำคัญที่หน่วยงานกำหนดความต้องการขั้นต้นร่วมกัน ในมุมมองของหน่วยงานกำหนดนโยบาย (Policy maker)




**แผนภูมิที่ 8** : แสดงผลการจัดลำดับความสำคัญที่หน่วยงานกำหนดความต้องการขั้นต้นร่วมกัน ในมุมมองของหน่วยงานอื่น ๆ



ทั้งนี้ สกมช. จะนำผลการจัดลำดับความสำคัญที่หน่วยงานกำหนดความต้องการขั้นต้นร่วมกันตามกรอบการทำงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ของประเทศไทย มาใช้พิจารณาจัดทำแผนบูรณาการเพื่อขับเคลื่อนการดำเนินการ ตามมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567 ซึ่งเป็นแผนระยะ 5 ปี เพื่อให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ผู้ให้บริการคลาวด์ทั้งภายในและต่างประเทศ และหน่วยงานอื่นๆ ที่เกี่ยวข้อง สามารถดำเนินการตามมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567 ได้ต่อไป

**********