CYFENCE
Securing your Business

การสร้างความตระหนัก ในการรักษาความมั่นคงปลอดภัยสารสนเทศ

วิทยากร
คุณ อุมารัตน์ โพธิ์ชัย

วิทยากร
คุณ จันทกานต์ ผลผล

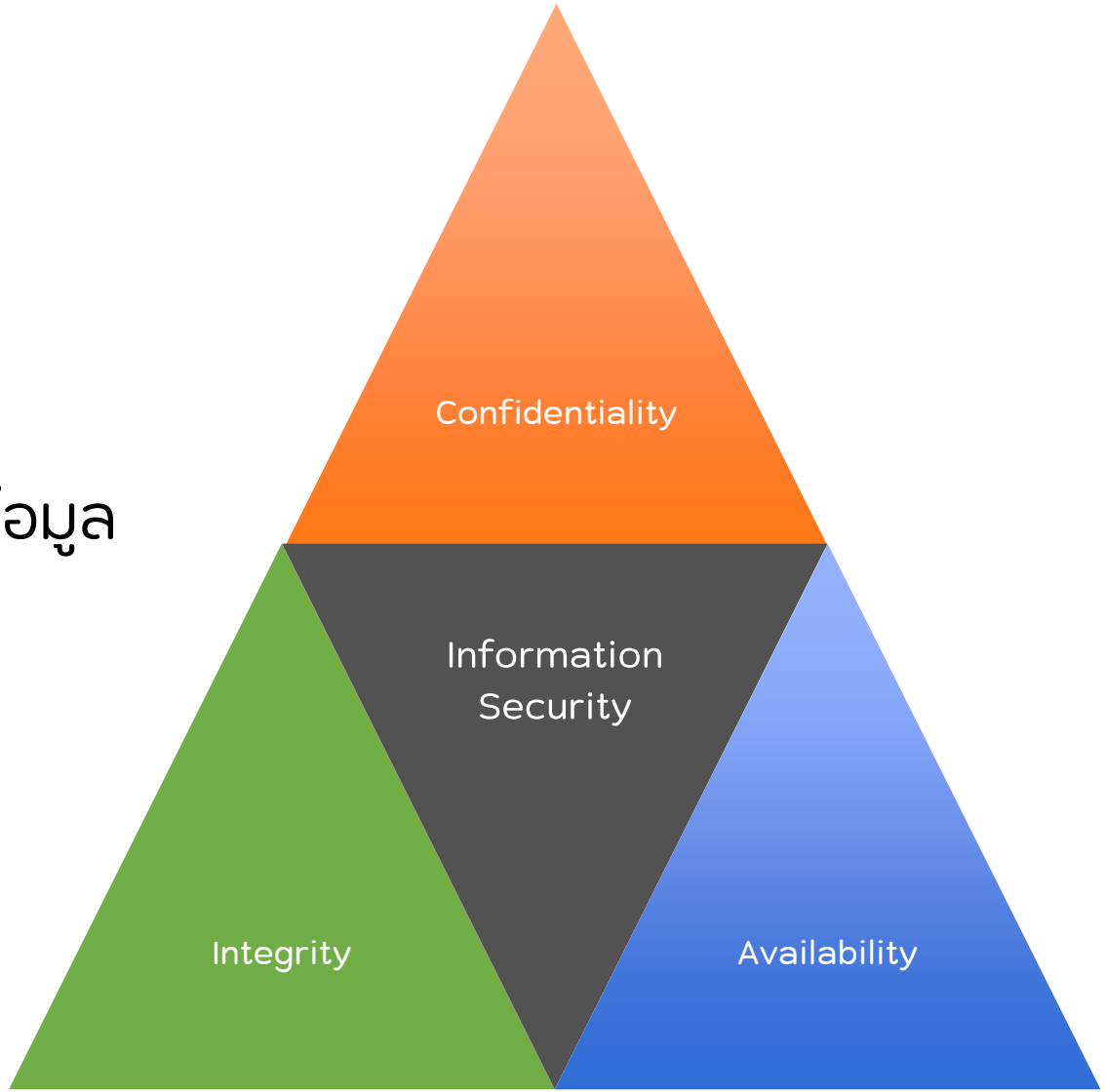
Information Security Management System (ISMS)

CIA Model

Confidentiality – การรักษาความลับ

Integrity – ความถูกต้อง/ความสมบูรณ์ของข้อมูล

Availability – ความพร้อมใช้งาน



ISO/IEC 27001 : 2022

The new ISO/IEC 27001:2022 revision was published on the **25th of October 2022**

Information Technology – Security techniques – Code of practice for information security controls

2013

Name Changed

Information security, cybersecurity and privacy protection – Information security controls

2022

Benefits of ISO 27001

ลดโอกาสที่จะเกิดเหตุการณ์ความเสี่ยงด้านเทคโนโลยีสารสนเทศ

ลดผลกระทบและการสูญเสียจากเหตุการณ์ความเสี่ยง

เพิ่มประสิทธิภาพของการรักษาความลับ ความถูกต้อง และความพร้อมใช้ของข้อมูล

เพิ่มศักยภาพการทำงานให้กับบุคลากรในองค์กร

เพิ่มความสอดคล้องของการปฏิบัติตามกฎหมาย อาทิ พ.ร.บ.ไซเบอร์ และ PDPA

สร้างภาพลักษณ์และความน่าเชื่อถือให้กับองค์กร

ISO/IEC 27001: 2022 Structure

Clauses: Mandatory Processes

- 4. Context of Organization
- 5. Leadership
- 6. Planning
- 7. Support
- 8. Operation
- 9. Performance Evaluation
- 10. Improvement

Annex A: Controls (A.5 – A.8)

4 Categories

- Organisational
- People
- Physical
- Technological

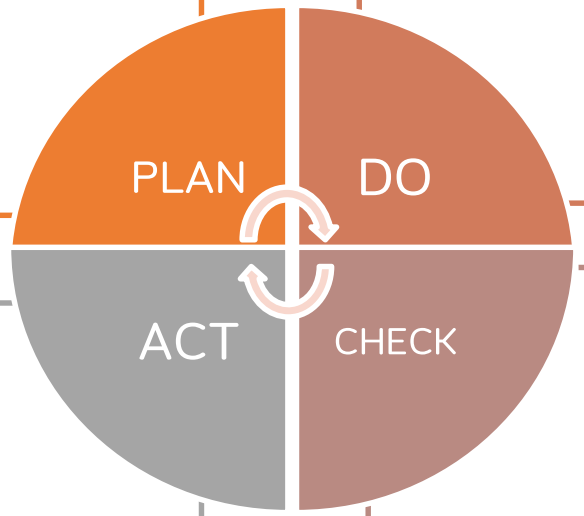
93 Controls

CYFENCE
Securing your Business

Deming Cycle (PDCA)

- 4. Context
- 5. Leadership
- 6. Planning
- 7. Support

- 8. Operation



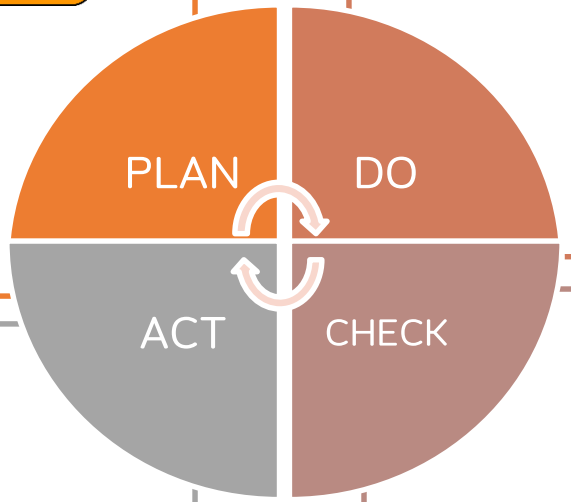
- 10. Improvement

- 9. Performance Evaluation:

CYFENCE
Securing your Business

Deming Cycle (PDCA)

- การวิเคราะห์บริบทองค์กร
- การสนับสนุนโดยผู้บริหารระดับสูง
- การกำหนดวัตถุประสงค์ รวมถึงความเสี่ยงและโอกาส
- การสนับสนุนด้านทรัพยากรและบุคลากรที่มีความรู้ความสามารถ รวมถึงจัดทำเอกสารที่จำเป็น



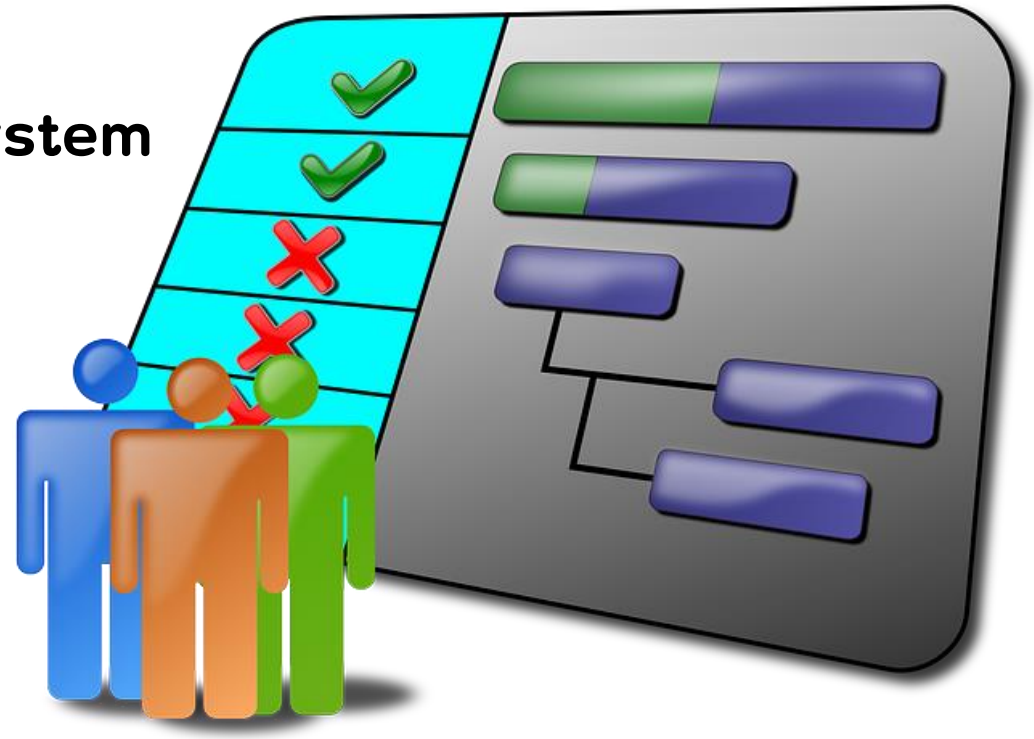
- การดำเนินการตามแผนที่วางไว้ ซึ่งรวมถึงการประเมินความเสี่ยงและการจัดการความเสี่ยง

- การแก้ไขสิ่งที่ไม่สอดคล้องและหาแนวทางป้องกันไม่ให้เกิดซ้ำ รวมถึงปรับปรุงอย่างต่อเนื่อง

- การเฝ้าระวัง วัดผล วิเคราะห์และประเมิน รวมถึงการประเมินภายในเพื่อตรวจสอบความสอดคล้องของกระบวนการ

Clause 4: Context of Organization

1. Understand the organization
2. Understand the needs and expectations
3. Determine the scope of ISMS
4. Information security management system
    - Establish
    - Implement
    - Maintain
    - Continual Improvement



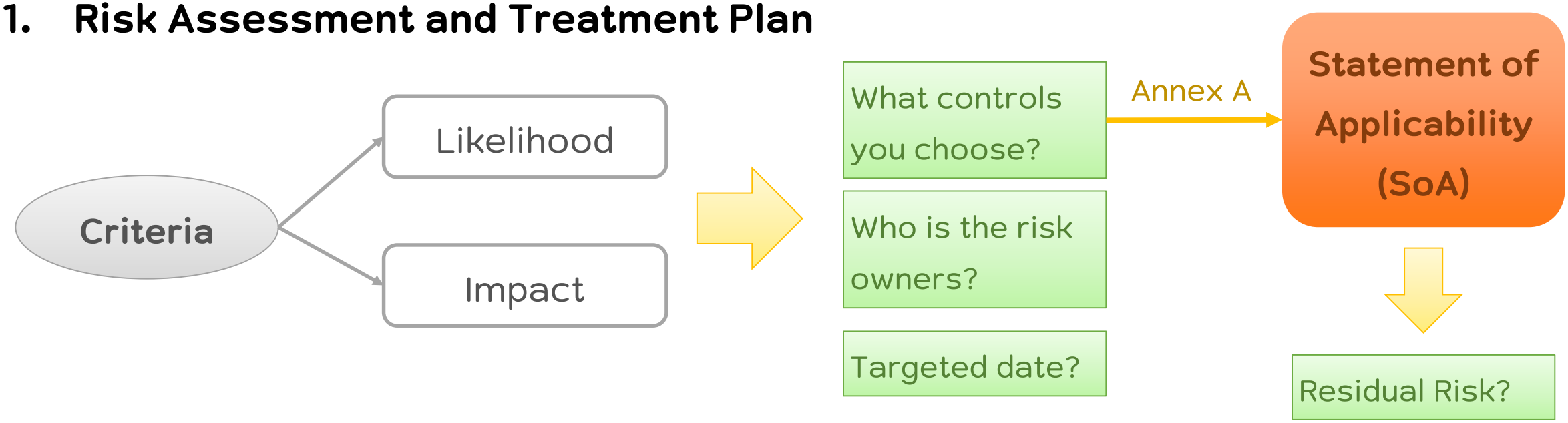
Clause 5: Leadership

What are the roles of top management?

- Policy
- Resources
- Leadership
- Continual improvement
- Information Security Awareness
- Task and responsibility Assignment

Clause 6: Planning

1. Risk Assessment and Treatment Plan



2. Objective and Plan

- Resources
- Who takes responsibility?
- How long will it take to reach goals?

Clause 7: Support

Resources

Competence

Awareness

Communication

Documented Information

CYFENCE
Securing your Business

Clause 8: Operation

- Operational Planning and Controls
- Risk Assessment
- Risk Treatment

CYFENCE
Securing your Business

Clause 9: Performance Evaluation

Monitoring, Measurement, Analysis, Evaluation

- KPI
  - ➢ When
  - ➢ Who

Internal Audit

- IA Checklist
- IA Plan
- IA Report
  - ➢ Conformity/ Nonconformity

Management Review

- ISMS Committee Meeting Report
  - ➢ Status
  - ➢ Change
  - ➢ Result
  - ➢ Interested Parties
  - ➢ Risk Assessment and Treatment Plan
  - ➢ Opportunities for Improvement

nt CYFENCE Securing your Business

Clause 10: Improvement

Is there any nonconformity?

What is the corrective action?

How to improve continuously?

Documented Information

ISO/IEC 27001 Major Changes Summary

- Introduced **Clause 6.3 Planning of changes**
- Controls in Annex A are **grouped into 4 main Categories** (Organizational, People, Physical, and Technological) instead of the previous 14.
- The total number of Annex A controls was reduced from **114 to 93**
- **11 new controls** added to in Annex A

Organizational	Physical	Technological
• Threat intelligence • Information security for use of cloud services • ICT readiness for business continuity	• Physical security monitoring	• Configuration management • Information deletion • Data masking • Data leakage prevention • Monitoring activities • Web filtering • Secure coding

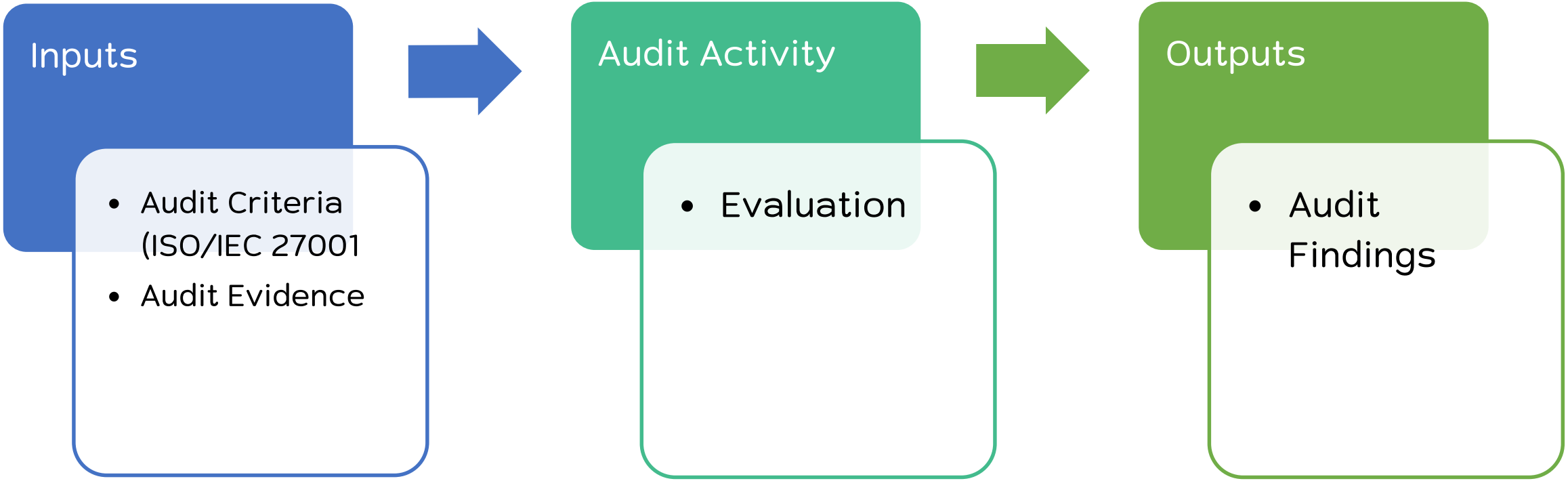
การตรวจประเมินสำหรับขอรับรอง ISO/IEC 27001

รูปแบบการตรวจประเมิน

First-party Audits	• การตรวจประเมินภายใน (Internal Audit) ขององค์กรโดยเจ้าหน้าที่หรือหน่วยงานตรวจประเมินภายใน • ตรวจเพื่อประเมินประสิทธิภาพการดำเนินงานหรือความสอดคล้องกับข้อกำหนด
Second-party Audits	• การตรวจประเมินภายนอก (External Audit) โดยผู้มีส่วนได้ส่วนเสีย • ตรวจเพื่อประเมินว่าการดำเนินงานขององค์กรสอดคล้องกับความต้องการของผู้ใช้บริการ หรือผู้มีส่วนได้ส่วนเสียหรือไม่
Third-party Audits	• การตรวจประเมินภายนอก (External Audit) โดยหน่วยงานอิสระ อาทิ หน่วยรับรอง ISO/IEC 27001 (Certification Body) • ตรวจเพื่อขอใบรับรองมาตรฐาน อาทิ มาตรฐาน ISO/IEC 27001

nt CYFENCE Securing your Business

กระบวนการตรวจประเมิน



การเตรียมความพร้อมสำหรับตรวจประเมินขอการรับรอง มาตรฐาน ISO/IEC 27001:2022

1. กำหนดขอบเขตของการตรวจประเมิน
2. จัดเตรียมเอกสารที่เกี่ยวข้องกับกระบวนการ ISMS
3. จัดเตรียมบุคลากรที่จะทำหน้าที่รับผิดชอบกระบวนการ ISMS
4. จัดทำ Audit Program เพื่อควบคุมการปฏิบัติงานให้เป็นไปตามแผนการตรวจประเมิน
5. ในการตรวจประเมินแต่ละครั้ง ต้องกำหนดช่วงเวลา สถานที่ และวิธีการตรวจตรวจประเมินไว้ล่วงหน้า รวมถึงเตรียมบุคลากรและผู้บริหารให้มีความพร้อมสำหรับการตรวจประเมิน
6. หากเป็นการตรวจประเมินครั้งแรก หรือต้องการเปลี่ยนเวอร์ชันของมาตรฐาน ISO/IEC 27001 ควรประเมิน Gap analysis เพื่อระบุว่าข้อกำหนดใดที่ยังไม่ได้ดำเนินการ

บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)

National Telecom Public Company Limited

www.cyfence.com | Contact Center 1888