

## Phụ lục A

(Quy định)

### Các mục tiêu kiểm soát và biện pháp kiểm soát tham chiếu

Các mục tiêu kiểm soát và biện pháp kiểm soát được liệt kê trong Bảng A.1 dưới đây được dẫn xuất trực tiếp và liên kết với các điều từ Điều 5 đến Điều 18 trong tiêu chuẩn ISO/IEC 27002:2013 và sẽ được sử dụng trong bối cảnh của 6.1.3.

#### Bảng A.1 – Các mục tiêu kiểm soát và biện pháp kiểm soát

**Có 14 Nhóm (số hiệu từ A5 đến A18) trong Phụ lục A của tiêu chuẩn 27001:2013.**

- A.5** Information security policies (Chính sách ATTT)
- A.6** Organization of information security (Tổ chức ATTT)
- A.7** Human resource security (An toàn nguồn lực con người)
- A.8** Asset Management (Quản lý tài sản)
- A.9** Access Control (Kiểm soát truy cập)
- A.10** Cryptography (Mật mã)
- A.11** Physical and environmental security (An toàn vật lý và môi trường)
- A.12** Operations security (An toàn vận hành)
- A.13** Communications security (An toàn truyền thông)
- A.14** System acquisition, development and maintenance (Tiếp nhận, phát triển và bảo trì hệ thống)
- A.15** Supplier relationships (Quan hệ với nhà cung cấp)
- A.16** Information security incident management (Quản lý sự cố ATTT)
- A.17** Information security aspects of business continuity management (Các khía cạnh ATTT trong quản lý hoạt động liên tục)
- A.18** Compliance (Sự tuân thủ)

14 Nhóm	35 Yêu cầu	114 Điều
<b>A.5</b>	<b>A.5.1</b>	<b>A.5.1.1 và A.5.1.2</b> (2 Điều)
<b>A.6</b>	<b>A.6.1 và A.6.2</b>	<b>A.6.1.1, A.6.1.2,..., A.6.1.5</b> (5 Điều) <b>A.6.2.1 và A.6.2.2</b> (2 Điều)
<b>A.7</b>	<b>A.7.1, A.7.2 và A.7.3</b>	<b>A.7.1.1 và A.7.1.2</b> (2 Điều) <b>A.7.2.1, A.7.2.2 và A.7.2.3</b> (3 Điều) <b>A.7.3.1</b> (1 Điều)

<b>A.8</b>	<b>A.8.1, A.8.2 và A.8.3</b>	A.8.1.1, A.8.1.2,..., A.8.1.4 (4 Điều) A.8.2.1, A.8.2.2 và A.8.2.3 (3 Điều) A.8.3.1, A.8.3.2 và A.8.3.3 (3 Điều)
<b>A.9</b>	<b>A.9.1, A.9.2, A.9.3 và A.9.4</b>	A.9.1.1 và A.9.1.2 (2 Điều) A.9.2.1, A.9.2.2,..., A.9.2.6 (6 Điều) A.9.3.1 (1 Điều) A.9.4.1, A.9.4.2,..., A.9.4.5 (5 Điều)
<b>A.10</b>	<b>A.10.1</b>	A.10.1.1 và A.10.1.2 (2 Điều)
<b>A.11</b>	<b>A.11.1 và A.11.2</b>	A.11.1.1, A.11.1.2,..., A.11.1.6 (6 Điều) A.11.2.1, A.11.2.2,..., A.11.2.9 (9 Điều)
<b>A.12</b>	<b>A.12.1, A.12.2, A.12.3, A.12.4, A.12.5, A.12.6 và A.12.7</b>	A.12.1.1, A.12.1.2,..., A.12.1.4 (4 Điều) A.12.2.1 (1 Điều) A.12.3.1 (1 Điều) A.12.4.1, A.12.4.2,..., A.12.4.4 (4 Điều) A.12.5.1 (1 Điều) A.12.6.1 và A.12.6.2 (2 Điều) A.12.7.1 (1 Điều)
<b>A.13</b>	<b>A.13.1 và A.13.2</b>	A.13.1.1, A.13.1.2 và A.13.1.3 (3 Điều) A.13.2.1, A.13.2.2,..., A.13.2.4 (4 Điều)
<b>A.14</b>	<b>A.14.1, A.14.2 và A.14.3</b>	A.14.1.1, A.14.1.2 và A.14.1.3 (3 Điều) A.14.2.1, A.14.2.2,..., A.14.2.9 (9 Điều) A.14.3.1 (1 Điều)
<b>A.15</b>	<b>A.15.1 và A.15.2</b>	A.15.1.1, A.15.1.2 và A.15.1.3 (3 Điều) A.15.2.1 và A.15.2.2 (2 Điều)
<b>A.16</b>	<b>A.16.1</b>	A.16.1.1, A.16.1.2,..., A.16.1.7 (7 Điều)
<b>A.17</b>	<b>A.17.1 và A.17.2</b>	A.17.1.1, A.17.1.2 và A.17.1.3 (3 Điều) A.17.2.1 (1 Điều)
<b>A.18</b>	<b>A.18.1 và A.18.2</b>	A.18.1.1, A.18.1.2,..., A.18.1.5 (5 Điều) A.18.2.1, A.18.2.2 và A.18.2.3 (3 Điều)

## 1) **A.5** INFORMATION SECURITY POLICIES

: NHÓM A.5 có 1 Yêu cầu (A.5.1), 1 Mục tiêu (Objective) và 2 Biện pháp kiểm soát (control)

Objective	A.5.1
Control	A.5.1.1 và A.5.1.2

## 2) **A.6 ORGANIZATION OF INFORMATION SECURITY**

: NHÓM A.6 có 2 Yêu cầu (A.6.1 và A.6.2), 2 Mục tiêu (Objective) và 7 BPKS (control)

Objective	A.6.1 và A.6.2
Control	A.6.1.1, A.6.1.2, A.6.1.3, A.6.1.4, A.6.1.5 A.6.2.1 và A.6.2.2

## 3) **A.7 HUMAN RESOURCE SECURITY**

: NHÓM A.7 có 3 Yêu cầu (A.7.1, A.7.2 và A.7.3) có 3 Mục tiêu (Objective) và 6 BPKS (control)

Objective	A.7.1, A.7.2 và A.7.3
Control	A.7.1.1, A.7.1.2 A.7.2.1, A.7.2.2 và A.7.2.3 A.7.3.1

## 4) **A.8 ASSET MANAGEMENT**

: NHÓM A.8 có 3 Yêu cầu (A.8.1, A.8.2 và A.8.3) có 3 Mục tiêu (Objective) và 10 BPKS (control)

Objective	A.8.1, A.8.2 và A.8.3
Control	A.8.1.1, A.8.1.2, A.8.1.3, A.8.1.4 A.8.2.1, A.8.2.2 và A.8.2.3 A.8.3.1, A.8.3.2, và A.8.3.3

## 5) **A.9 ACCESS CONTROL**

: NHÓM A.9 có 4 Yêu cầu (A.9.1, A.9.2, A.9.3 và A.9.4) có 4 Mục tiêu (Objective) và 14 BPKS

Objective	A.9.1, A.9.2, A.9.3 và A.9.4
Control	A.9.1.1 và A.9.1.2 A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.5 và A.9.2.6 A.9.3.1 A.9.4.1, A.9.4.2, A.9.4.3, A.9.4.4, và A.9.4.5

## 6) **A.10 CRYPTOGRAPHY**

: NHÓM A.10 có 1 Yêu cầu (A.10.1), 1 Mục tiêu (Objective) và 2 BPKS (control)

Objective	A.10.1 và A.10.2
Control	A.10.1.1 và A.10.1.2

**7)A.11 PHYSICAL AND ENVIRONMENTAL SECURITY**

**: NHÓM A.11 có 2 Yêu cầu (A.11.1 và A.11.2) có 2 Mục tiêu (Objective) và 15 BPKS (control)**

<b>Objective</b>	<b>A.11.1 và A.11.2</b>
<b>Control</b>	<b>A.11.1.1, A.11.1.2 và A.11.1.3, A.11.1.4, A.11.1.5 và A.11.1.6 A.11.2.1, A.11.2.2, A.11.2.3, A.11.2.4, A.11.2.5, A.11.2.6, A.11.2.7, A.11.2.8, A.11.2.9</b>

**8)A.12 OPERATIONS SECURITY**

**: NHÓM A.12 có 7 Yêu cầu (A.12.1,..., A12.7) , 7 Mục tiêu (Objective) và 14 BPKS (control)**

<b>Objective</b>	<b>A.12.1, A.12.2, A.12.3, A.12.4, A.12.5, A.12.6 và A.12.7</b>
<b>Control</b>	<b>A.12.1.1, A.12.1.2, A.12.1.3 và A.12.1.4 A.12.2.1 A.12.3.1 A.12.4.1, A.12.4.2 và A.12.4.3 và A.12.4.4 A.12.5.1 A.12.6.1 và A.12.6.2 A.12.7.1</b>

**9)A.13 COMMUNICATIONS SECURITY**

**: NHÓM A.13 có 2 Yêu cầu (A.13.1 và A.13.2), 2 Mục tiêu (Objective) và 7 BPKS (control)**

<b>Objective</b>	<b>A.13.1 và A.13.2</b>
<b>Control</b>	<b>A.13.1.1, A.13.1.2 và A.13.1.3 A.13.2.1, A.13.2.2 và A.13.2.3 và A.13.2.4</b>

**10)A.14 SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE**

**: NHÓM A.14 có 3 Yêu cầu (A.14.1, A.14.2 và A.14.3), 3 Mục tiêu (Objective) và 13 BPKS**

<b>Objective</b>	<b>A.14.1, A.14.2 và A.14.3</b>
<b>Control</b>	<b>A.14.1.1, A.14.1.2 và A.14.1.3 A.14.2.1, A.14.2.2, A.14.2.3, A.14.2.4, A.14.2.5, A.14.2.6, A.14.2.7, A.14.2.8,A.14.2.9 A.14.3.1</b>

11)**A.15**      **SUPPLIER RELATIONSHIPS**

: **NHÓM A.15** có 2 Yêu cầu (A.15.1 và A.15.2), 2 Mục tiêu (Objective) và 5 BPKS (control)

Objective	A.15.1 và A.15.2
Control	A.15.1.1, A.15.1.2 và A.15.1.3 A.15.2.1 và A.15.2.2

12)**A.16**      **INFORMATION SECURITY INCIDENT MANAGEMENT**

: **NHÓM A.16** có 1 Yêu cầu (A.16.1), 1 Mục tiêu (Objective) và 7 BPKS (control)

Objective	A.16.1
Control	A.16.1.1, A.16.1.2, A.16.1.3, A.16.1.4, A.16.1.5, A.16.1.6 và A.16.1.7

13)**A.17**      **INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT**

: **NHÓM A.17** có 2 Yêu cầu (A.17.1 và A.17.2), 2 Mục tiêu (Objective) và 4 BPKS (control)

Objective	A.17.1 và A.17.2
Control	A.17.1.1, A.17.1.2 và A.17.1.3 A.17.2.1

14)**A.18**      **COMPLIANCE**

: **NHÓM A.18** có 2 Yêu cầu (A.18.1 và A.18.2), 2 Mục tiêu (Objective) và 8 BPKS (control)

Objective	A.18.1 và A.18.2
Control	A.18.1.1, A.18.1.2, A.18.1.3, A.18.1.4 và A.18.1.5 A.18.2.1, A.18.2.2 và A.18.2.3

./.