ICT as Tool of Compliance

Chester Que
CEO, Achieve Without Borders

Business Units

IT Networks

- Hardware - Enterprise network routers, switches, and WiFi APs
- High Availability Networks
- Security Infrastructure
- IT Security Management
- CCTV
- Voice Over IP / IP-PBX Systems

Business Units

ORACLE + NETSUITE

Microsoft

AWB CLOUD SOLUTIONS

Philippine HRIS + Payroll • Warehouse • Cloud Migration
Web + Mobile Development • Systems Integration

IT Solutions

- Enterprise Resource Planning (ERP)
- Localized Human Resource Information System (HRIS)
- Custom Business Applications
- Website and Web Applications
- Mobile Applications

Business Units

IT and Business Services

- IT Process Outsourcing
- MIS Consulting
- Security Solutions Special Projects
- Data Privacy Act Continuing Compliance

Data Privacy Act of the Philippines

AWB Objective is to increase DPA Compliance

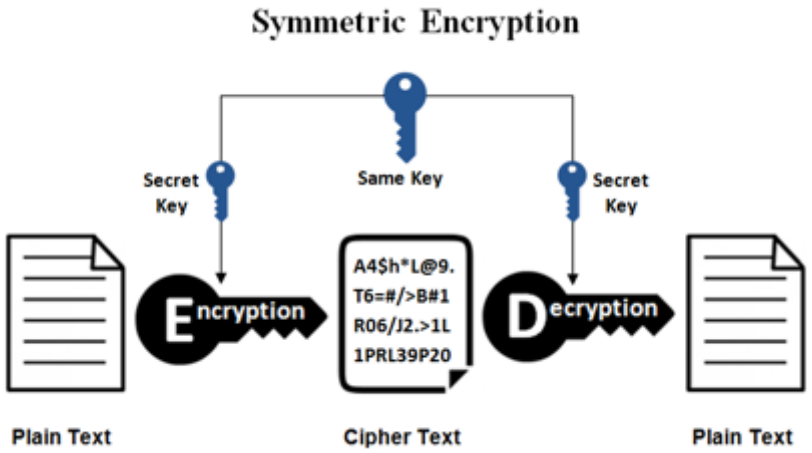
- Awareness
  - DPA Roadshow Events nationwide
- Simplification
  - One team with legal, process, and IT experts
  - Unified Knowledge Base
- Lowest Cost of Implementation
  - Packaged Legal and IT Services, e.g. PIA, DPO Advisory
  - Lowest Software Cost

DPA Technology Mapping

Implementing Privacy and Data Protection Measures	Highlights (npc-circular-16-01 & IRR)	Technology
(VI. DATA SECURITY)	**Encryption of Personal Data** (Rule II Sec. 8 of Circular-16-01) **Online Access to Personal Data** (Rule III Sec. 18 of Circular-16-01) **Local Copies of Personal Data Accessed Online** (Rule III Sec. 19 of Circular-16-01) **Emails** (Rule IV Sec. 24 of Circular-16-01) **Personal Productivity Software** (Rule IV Sec. 25 of Circular-16-01) **Portable Media** (Rule IV Sec. 26 of Circular-16-01)	Data Loss & Leakage Prevention (DLP) System Encryption
	Restricted Access (Rule II Sec. 9) **Online Access to Personal Data** (Rule III Sec. 18 of Circular-16-01)	Firewall Web Application Firewall Intrusion Prevention System Vulnerability Assessment & Patch Management Application White-listing
	Remote Disconnection or Deletion (Rule III Sec. 21 of Circular-16-01) **Emails** (Rule IV Sec. 24 of Circular-16-01)	Mobile Device Management
	Online Access to Personal Data (Rule III Sec. 18 of Circular-16-01)	Multi-Factor Authentication
	Encryption of Personal Data (Rule II Sec. 8 of Circular-16-01) **Authorized Devices** (Rule III Sec. 20)	Access Control Policy
	Physical Security Measures (Rule VI Sec. 27 of the IRR)	Door Access / CCTV
(VIII. BREACHES)	**Data Breach Notification** (Rule IX Sec 38-41 of the IRR)	Security Incident & Event Manager

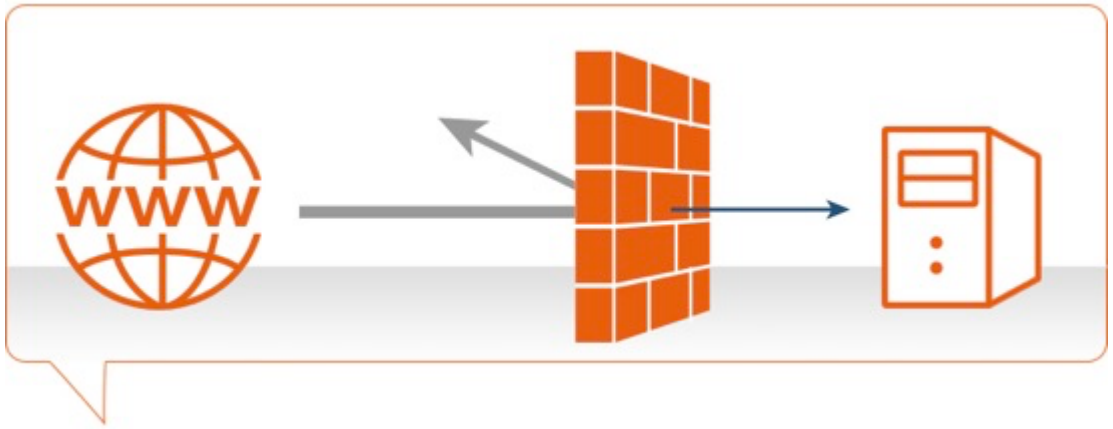
Data Leakage and Loss Prevention (DLP)

Data loss prevention software detects potential data breaches/data ex-filtration transmissions and prevents them by monitoring, detecting and blocking sensitive data while in-use (endpoint actions), in-motion (network traffic), and at-rest (data storage)



Encryption

Encryption is the process of encoding a message or information in such a way that only authorized parties can access it and those who are not authorized cannot



Firewall

In computing, a firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. A firewall typically establishes a barrier between a trusted internal network and untrusted external network, such as the Internet

Intrusion Prevention System

An Intrusion Prevention System (IPS) is a network security/threat prevention technology that examines network traffic flows to detect and prevent vulnerability exploits.

IT Services

Multi-Factor Authentication

Multi-Factor Authentication (MFA) is a security system that requires more than one method of authentication from independent categories of credentials to verify the user's identity for a login or other transaction

Application-Whitelisting

The technologies used to enforce application whitelists —to control which applications are permitted to be installed or executed on a host—are called whitelisting programs, application control programs, or application whitelisting technologies.

Mobile Device Management

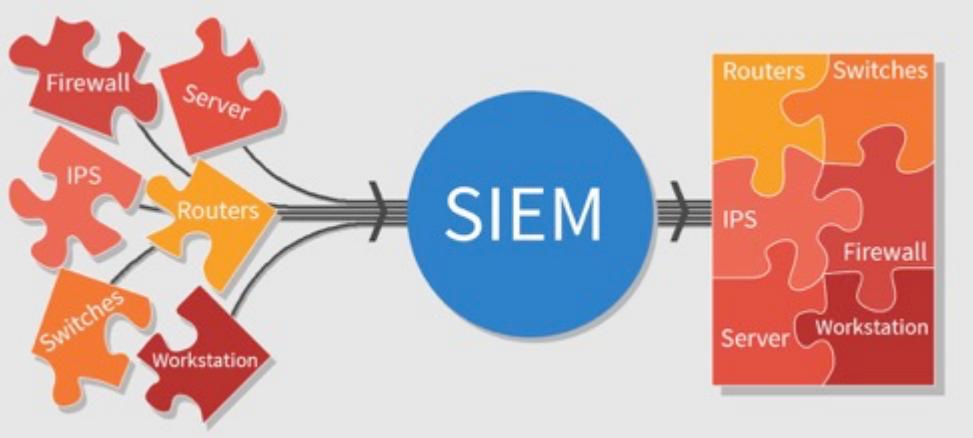
Mobile device management (MDM) is an industry term for the administration of mobile devices, such as smartphones, tablet computers, laptops and desktop computers. MDM is usually implemented with the use of a third party product that has management features for particular vendors of mobile devices

Access Control

In the fields of physical security and information security, access control (AC) is the selective restriction of access to a place or other resource. The act of accessing may mean consuming, entering, or using. Permission to access a resource is called authorization.

Vulnerability Management

Vulnerability management is a pro-active approach to managing network security. It includes processes for Identifying vulnerabilities and patching/fixing vulnerabilities



IT Services

Security Information & Event Manager (SIEM)

Security incident and event management (SIEM) is the process of identifying, monitoring, recording and analyzing security events or incidents within a real-time IT environment. It provides a comprehensive and centralized view of the security scenario of an IT infrastructure.

Security incident and event management is also known as security information event management.

IT Services

Data Center Security

Is a complete approach in securing the data center. Door Access, CCTV, Server hardening, firewalling, IPS etc.

DPA Technology Mapping

Implementing Privacy and Data Protection Measures	Highlights (npc-circular-16-01 & IRR)	Technology
(VI. DATA SECURITY)	**Encryption of Personal Data** (Rule II Sec. 8 of Circular-16-01) **Online Access to Personal Data** (Rule III Sec. 18 of Circular-16-01) **Local Copies of Personal Data Accessed Online** (Rule III Sec. 19 of Circular-16-01) **Emails** (Rule IV Sec. 24 of Circular-16-01) **Personal Productivity Software** (Rule IV Sec. 25 of Circular-16-01) **Portable Media** (Rule IV Sec. 26 of Circular-16-01)	Data Loss & Leakage Prevention (DLP) System Encryption
	Restricted Access (Rule II Sec. 9) **Online Access to Personal Data** (Rule III Sec. 18 of Circular-16-01)	Firewall Web Application Firewall Intrusion Prevention System Vulnerability Assessment & Patch Management Application White-listing
	Remote Disconnection or Deletion (Rule III Sec. 21 of Circular-16-01) **Emails** (Rule IV Sec. 24 of Circular-16-01)	Mobile Device Management
	Online Access to Personal Data (Rule III Sec. 18 of Circular-16-01)	Multi-Factor Authentication
	Encryption of Personal Data (Rule II Sec. 8 of Circular-16-01) **Authorized Devices** (Rule III Sec. 20)	Access Control Policy
	Physical Security Measures (Rule VI Sec. 27 of the IRR)	Door Access / CCTV
(VIII. BREACHES)	**Data Breach Notification** (Rule IX Sec 38-41 of the IRR)	Security Incident & Event Manager

IT Services

- Data Leakage and Loss Prevention (DLP)
- Encryption (Endpoint/Email/URL)
- Firewall / Web Filtering
- Intrusion Prevention System
- Multi-Factor Authentication
- Server Hardening / Application White-listing

IT Services

- Mobile Device Management
- Access Control
- Vulnerability Assessment
- Patch Management
- Security Information & Event Manager
- Data Center Security