Cloud Computing

ดร.ศักดิ์ เสกขุนทด

ผู้อำนวยการสำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน)

17 กันยายน 2556

Topic

- สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) (สรอ.)
- Government Cloud
- Security Guidance for Critical Areas of focus in Cloud Computing V3.0

EGA
e-Government Agency

สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) (สรอ.)

ที่มาและเหตุผลในการจัดตั้ง สรอ.

- หน่วยงานภาครัฐมีขีดความสามารถและความพร้อมในการพัฒนาด้าน e-Government ที่ไม่เท่ากัน
- มีหน่วยงานกลางเฉพาะที่มีรูปแบบการดำเนินงานที่คล่องตัวและมีกลไกซึ่งเอื้อต่อการมีบุคคลากรที่มีความเชี่ยวชาญมีศักยภาพสูงในการดำเนินงานด้าน e-Government เพื่อเป็นกลไกสำคัญในการขับเคลื่อนการพัฒนา e-Government ของประเทศ
- วันที่ 21 กุมภาพันธ์ 2554 ราชกิจจานุเบกษา ประกาศ พรฎ.จัดตั้งสำนักงานรัฐบาลอิเล็กทรอนิกส์ (สรอ.) ที่มีผลบังคับในวันที่ 22 กุมภาพันธ์ 2554
- วันที่ 22 มีนาคม 2554 มีมติ ครม. ให้ดำเนินการโอนย้ายทรัพย์สิน ภารกิจ คน ของสำนักงานพัฒนาวิทยาสตร์และเทคโนโลยีแห่งชาติ (สวทช) ในส่วนของสำนักบริการเทคโนโลยีสารสนเทศภาครัฐ (สบทร.) และภารกิจที่เกี่ยวกับด้านเทคโนโลยีสารสนเทศและการสื่อสารด้านรัฐบาลอิเล็กทรอนิกส์ของสำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร มาที่ สรอ.

วิสัยทัศน์ และ ภารกิจ

สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) (สรอ.)

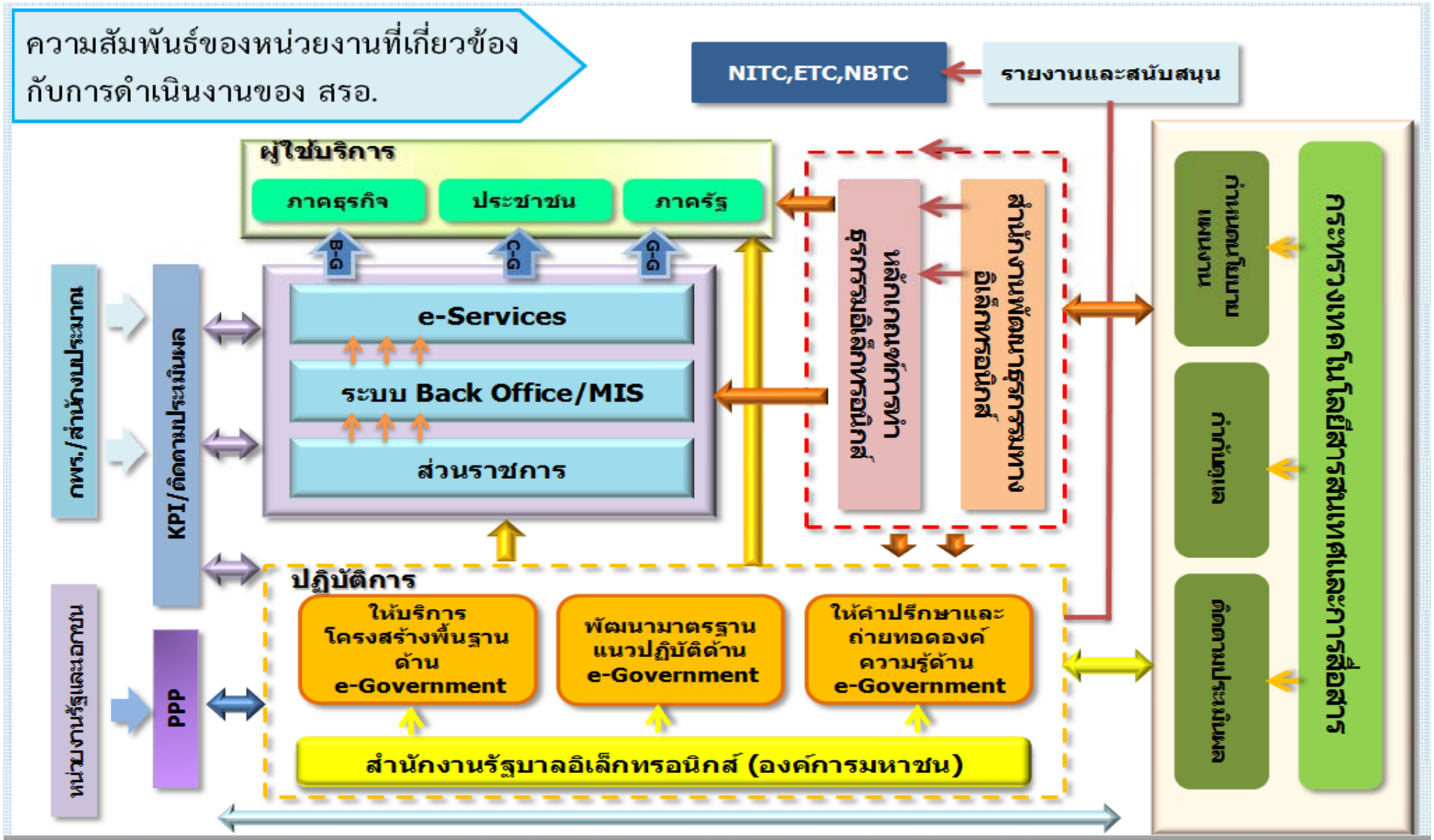
วิสัยทัศน์

"Enabling Complete & Secure e-Government"

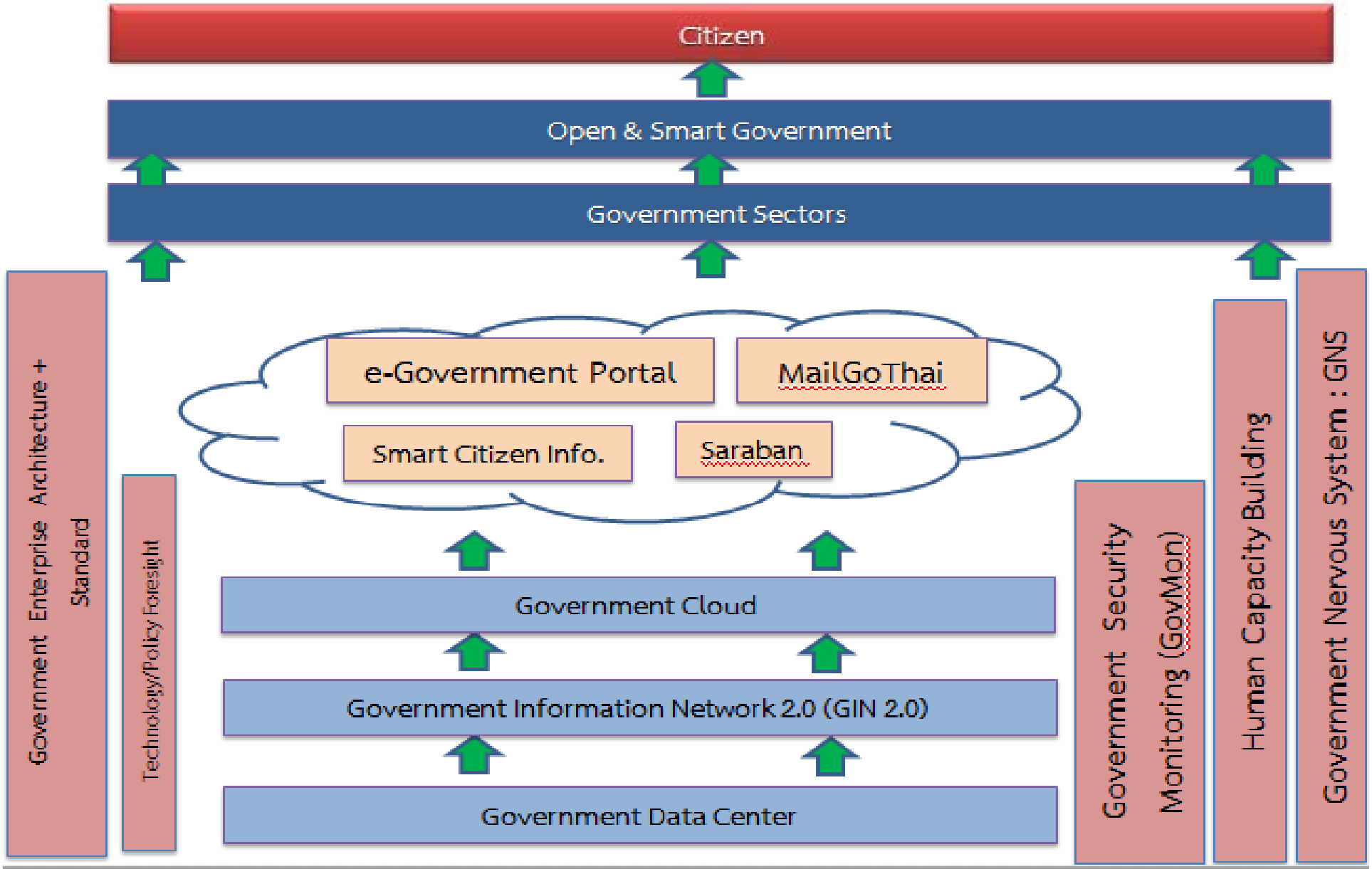
ภารกิจ

1. พัฒนา บริหารจัดการ และให้บริการ*โครงสร้างพื้นฐานสารสนเทศ*ในส่วนที่เกี่ยวกับรัฐบาลอิเล็กทรอนิกส์
2. ศึกษา วิจัย พัฒนา และเสนอแนะ*แนวทาง มาตรการ และมาตรฐาน*ด้านรัฐบาลอิเล็กทรอนิกส์
3. *ให้คำปรึกษา บริการด้านวิชาการ และบริหารจัดการโครงการ*ด้านเทคโนโลยีสารสนเทศและการสื่อสารในส่วนที่เกี่ยวข้องกับรัฐบาลอิเล็กทรอนิกส์
4. ส่งเสริม สนับสนุน และจัดอบรมเพื่อ*ยกระดับทักษะความรู้ความสามารถ*ด้านรัฐบาลอิเล็กทรอนิกส์ ตลอดจนเผยแพร่ข้อมูลข่าวสารที่เกี่ยวข้อง

ความสัมพันธ์ของหน่วยงานที่เกี่ยวข้องกับการดำเนินงานของ สรอ.



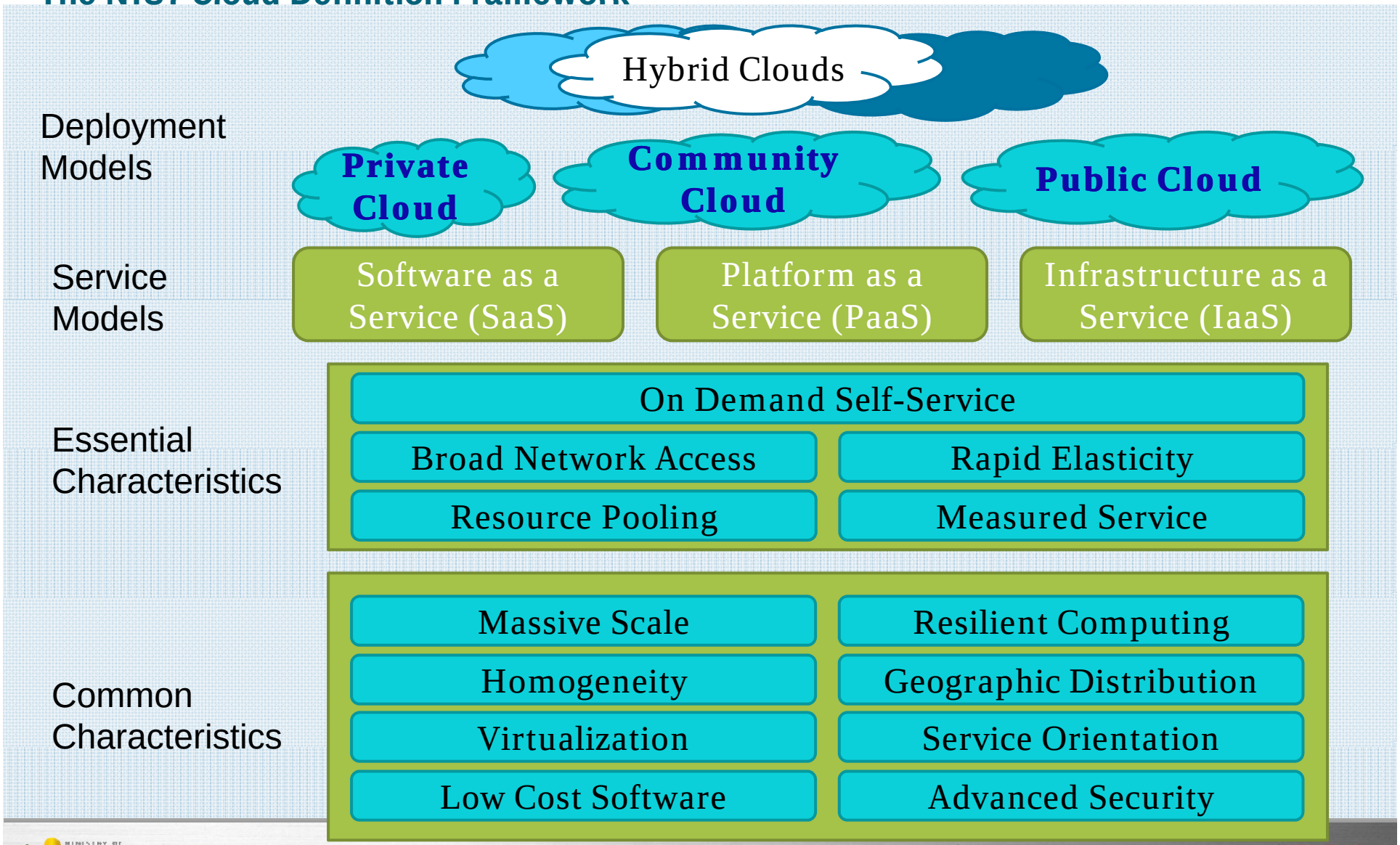
ความเชื่อมโยงระบบโครงสร้างพื้นฐานด้าน ICT



Government Cloud

Introduction to Cloud

The NIST Cloud Definition Framework



Based upon original chart created by Alex Dowbor - http://ornot.wordpress.com

G-Cloud

The G-Cloud Programme :

- Improving public service delivery
- Improving access to public services
- Increasing the efficiency of public service delivery

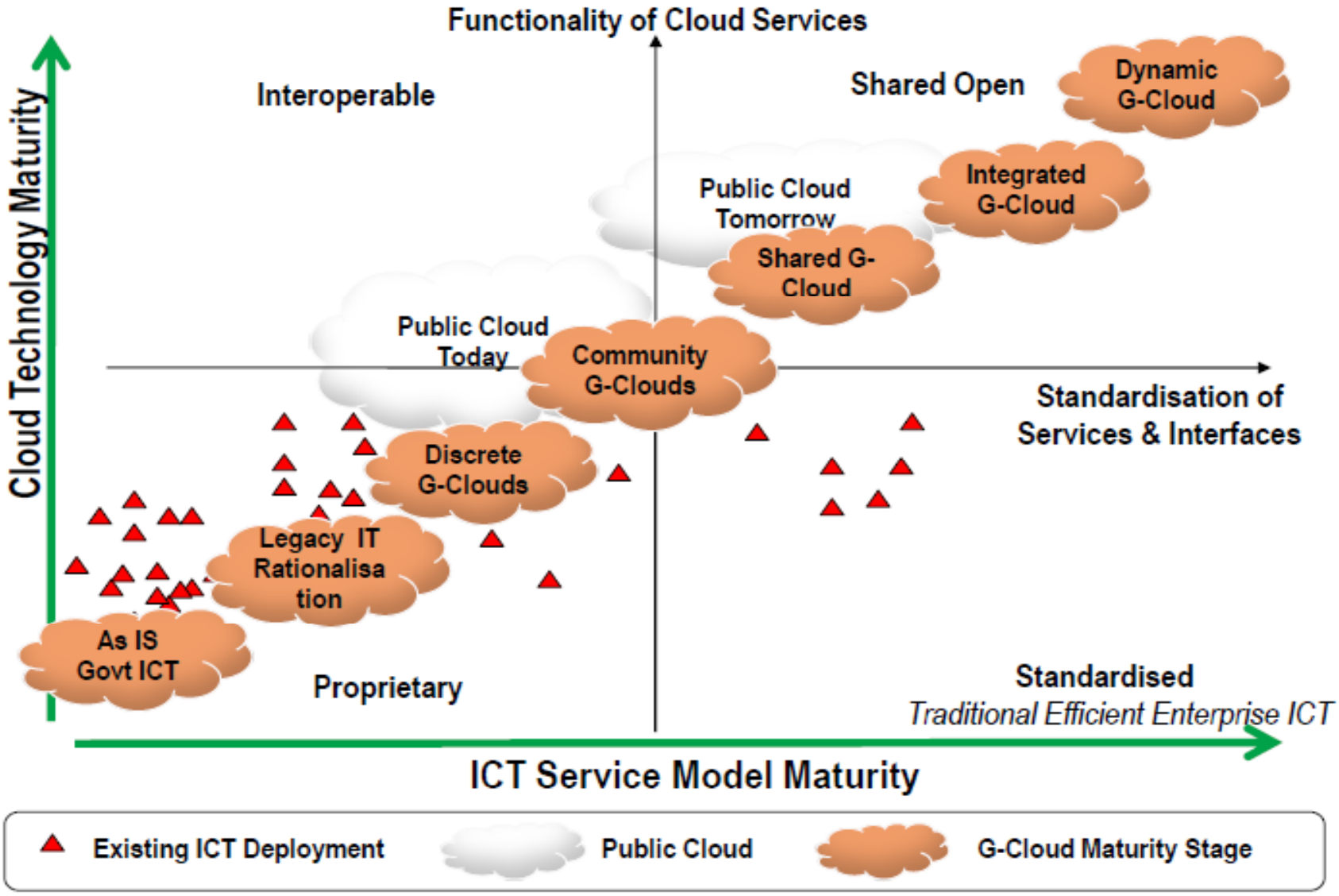
Data Centers Consolidation

Government Cloud

Application Store for Government

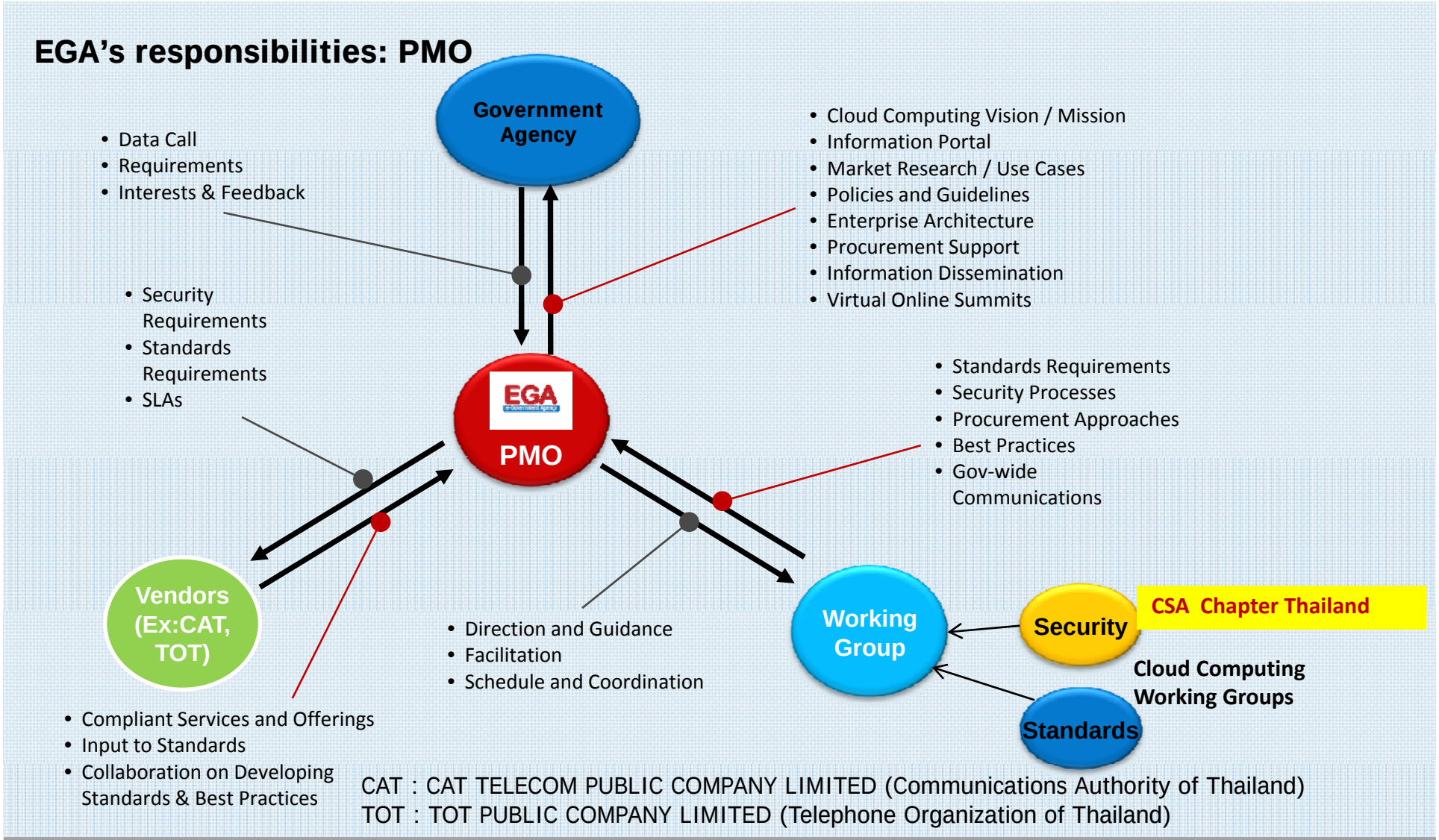
Source: Cisco Systems

Strategic Framework for Government



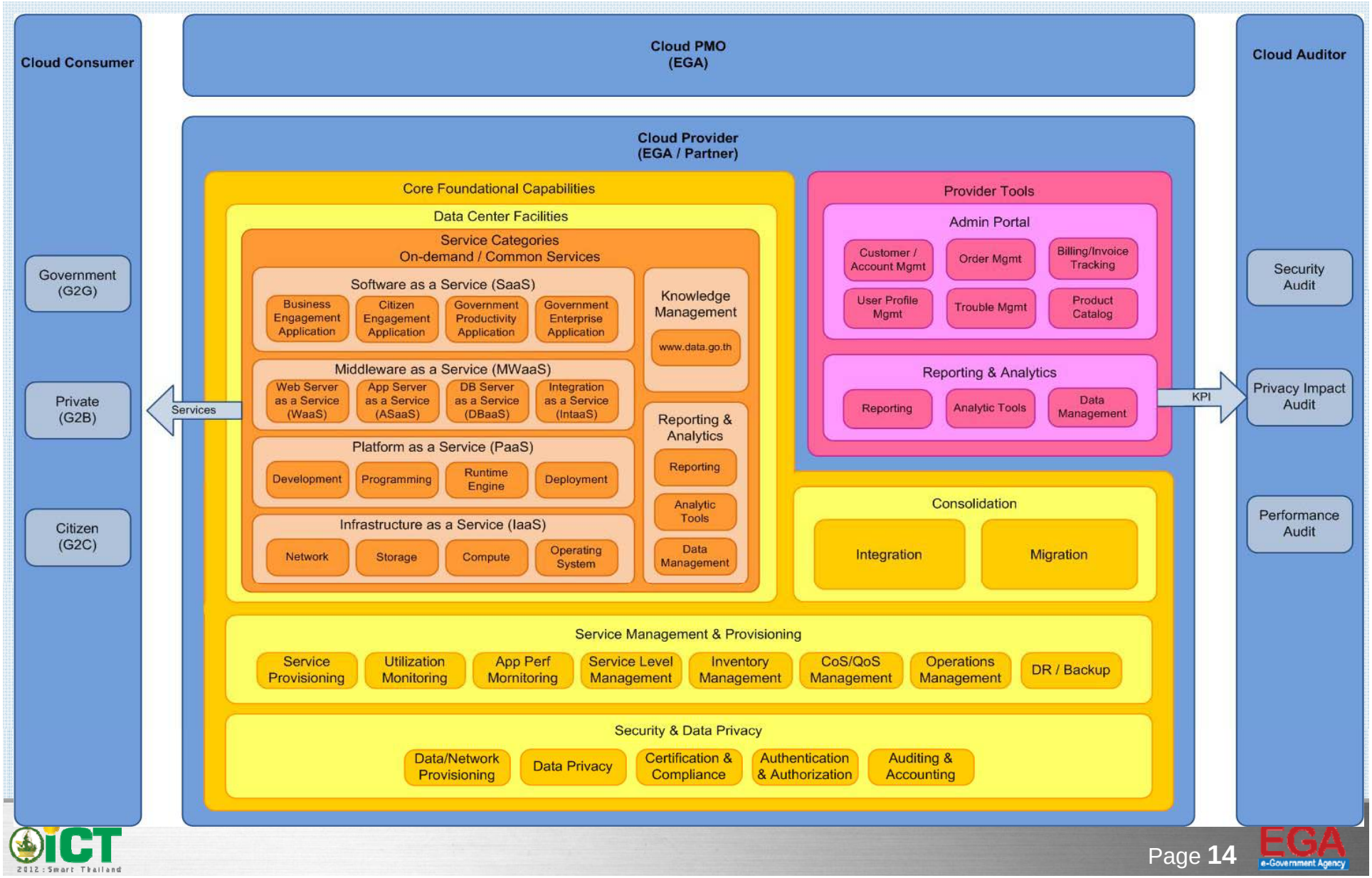
Source: Cisco Systems

Cloud Computing Initiative : Governance Model

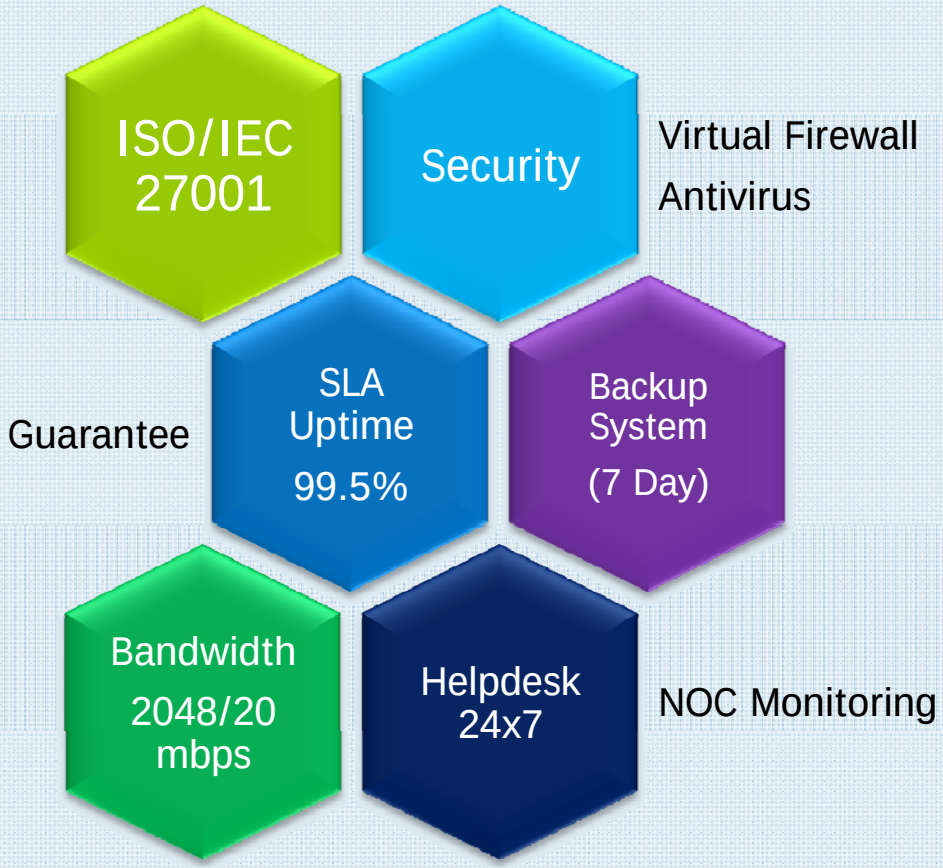


G-Cloud Scenario

Government Cloud Service Framework



G-Cloud Standard



G-Cloud Package

Standard Server

- 1 vCPU, 4GB vMem, HDD 50GB

Storage Server

- 1 vCPU, 4GB vMem, HDD 100GB

Performance Server

- 2 vCPU, 8GB vMem, HDD 50GB

Premium Server

- 2 vCPU, 8GB vMem, HDD 200GB

OS

Windows Server

LiNUX CentOS ubuntu

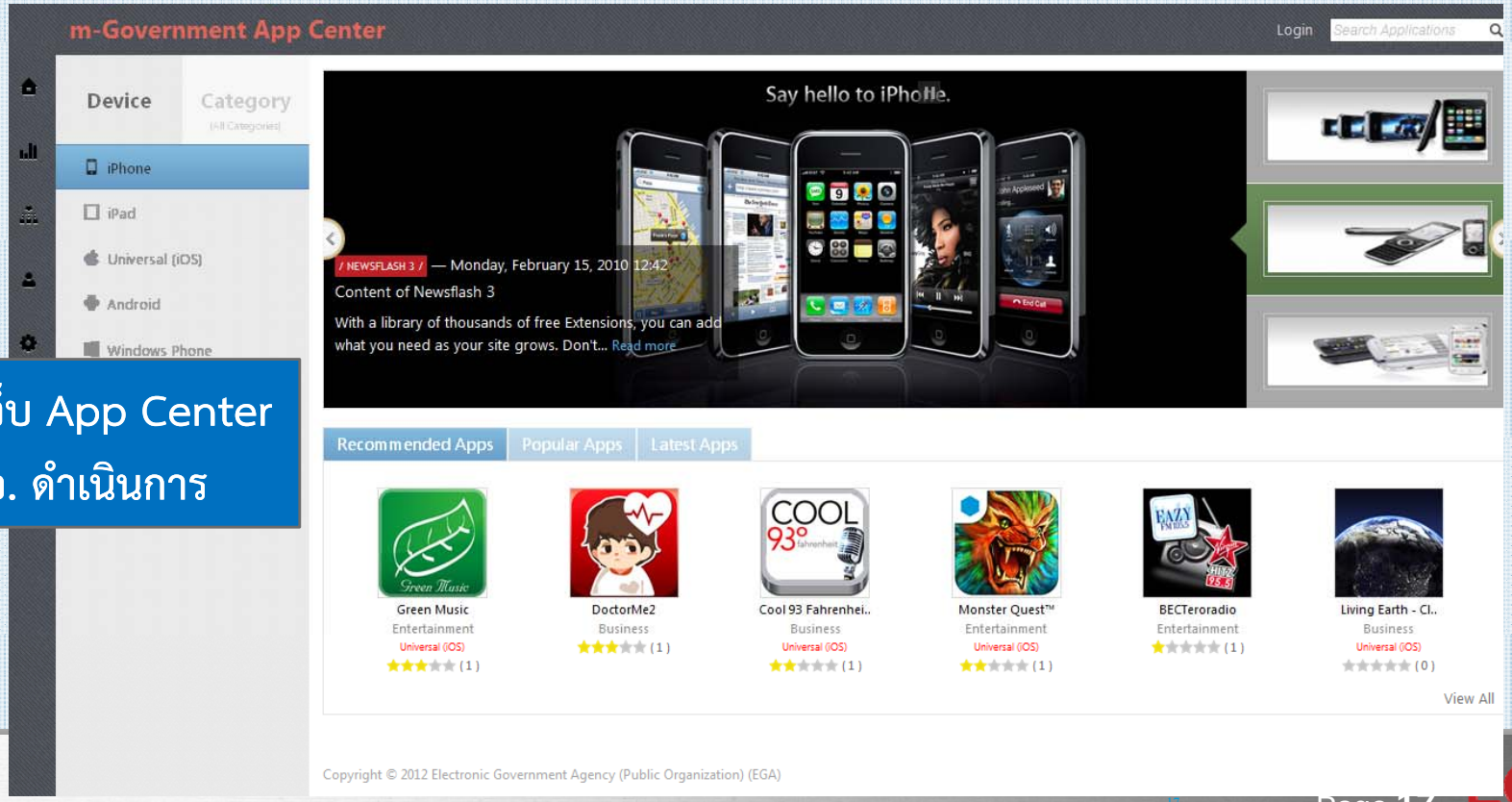
Database

Microsoft SQL Server

Government App Center

Government Application Center เป็นโครงการพัฒนาระบบที่รวมแอพพลิเคชั่นที่ภาครัฐต้องการใช้งาน เพื่อส่งเสริมการเป็นรัฐบาลอิเล็กทรอนิกส์ โดยศึกษารูปแบบการให้บริการที่เหมาะสม รวมทั้ง ส่งเสริมให้ภาคเอกชนนำ Application มาให้บริการ

กลยุทธ์ สร้างการมีส่วนร่วมของภาคเอกชนในการนำ app มาให้บริการ



ตัวอย่างเว็บ App Center ที่ สรอ. ดำเนินการ

Security Guidance for Critical Areas of focus in Cloud Computing V3.0

Cloud Information Architectures

Data Security Lifecycle

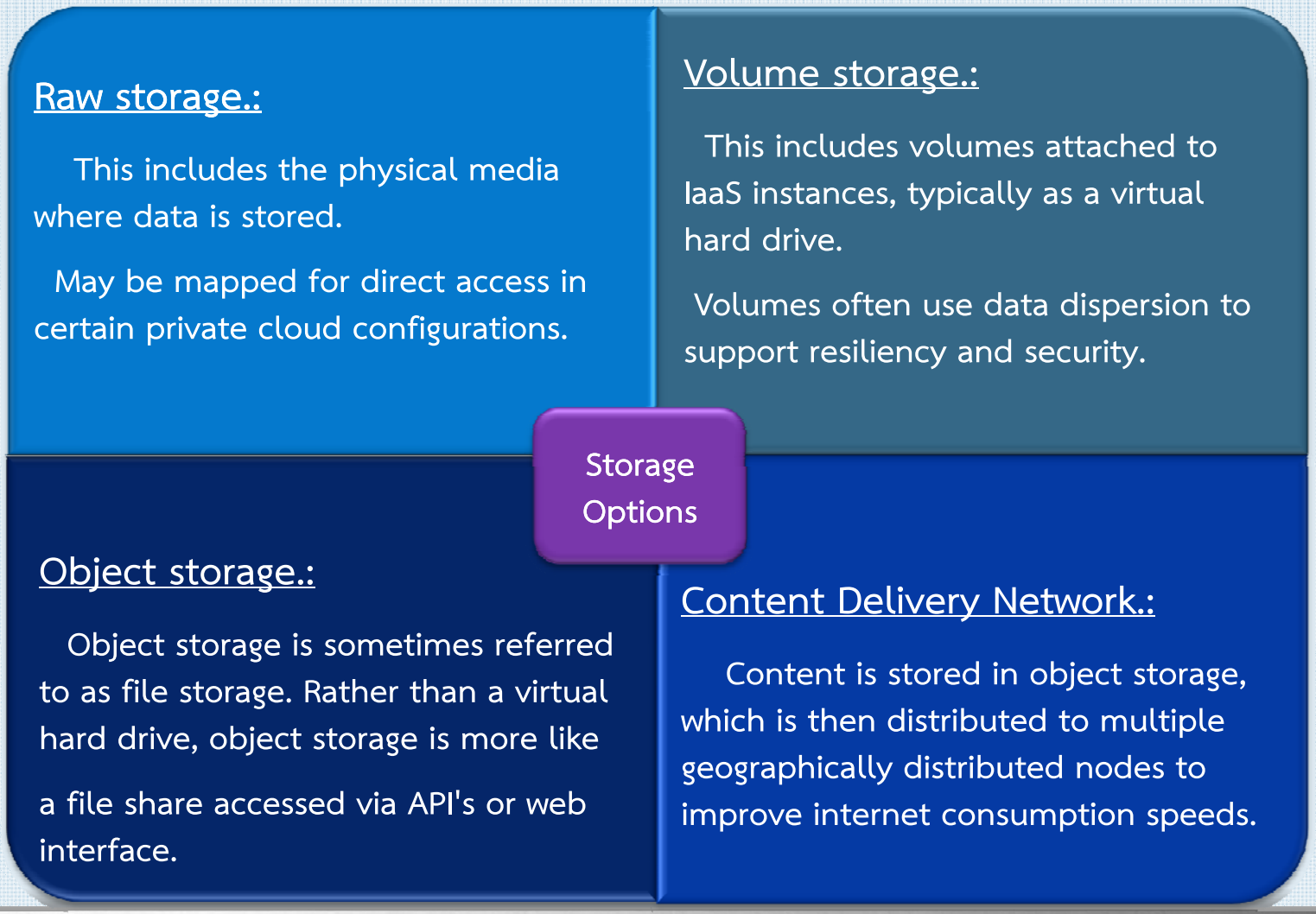
Information Governance

Cloud Information Architectures

Recommendation by Cloud Security Alliance

Infrastructure as a Service

IaaS, for public or private cloud, generally includes the following storage options:



Platform as a Service (1/2)

PaaS both provides and relies on very wide range of storage options.

PaaS may provide:

- Database as a Service.

  A multitenant database architecture that is directly consumable as a service. Users consume the database via APIs or direct SQL calls, depending on the offering.

  Each customers's data is segregated and isolated from other tenants. Database may be relational, flat, or any other common structure.

- Hadoop/Mapreduce/Big Data as a Service.

  Big data is data whose large scale, broad distribution, heterogeneity, and currency/timeliness require the use of new technical architectures and analytics. Hadoop and other Big Data applications may be offered as a cloud platform. Data is typically stored in Object Storage or another distributed file system. Data typically needs to be close to the processing environment, and may be moved temporally as needed for processing.

- Application storage.

  Application storage includes any storage options built into a PaaS application platform and consumable via API's that doesn't fall into other storage categories.

Platform as a Service (2/2)

PaaS may consume:

- Database.

  Information and content may be directly stored in the database (as text or binary objects) or as files referenced by the database. The database itself may be a collection of IaaS instances sharing common back-end storage.

- Object/File Storage.

  Files or other data are stored in object storage, but only asscessed via the PaaS API.

- Voludme Storage.

  Data may be stored in IaaS volumes attached to instances dedicated to providing the PaaS service.

- Other.

  These are the most common storage models, but this is a dynamic area and other options may be available.

Software as a Service (1/2)

SaaS use a very wide range of storage and consumption models. SaaS storage is always accessed via a web-based user interface or client/server application. If the storage is accessible via API then it's considered PaaS. Many SaaS providers also offer these PaaS APIs.

SaaS may provide:

- Information Storage and Management.

  Data is entered into the system via the web interface and stored within the SaaS application (usually a back-end database). Some SaaS services offer data set upload options ,or PaaS API's.

- Content/File Storage.

  File-based content is stored within the SaaS application (e.g., reports, image files, documents) and made accessible via the web-based user interface.

Software as a Service (2/2)

SaaS may consume:

- Databases.

  Like PaaS, a large number of SaaS services rely on database back-ends, even for file storage.

- Object/File Storage.

  Files or other data are stored in object storage, but only accessed via the SaaS application.

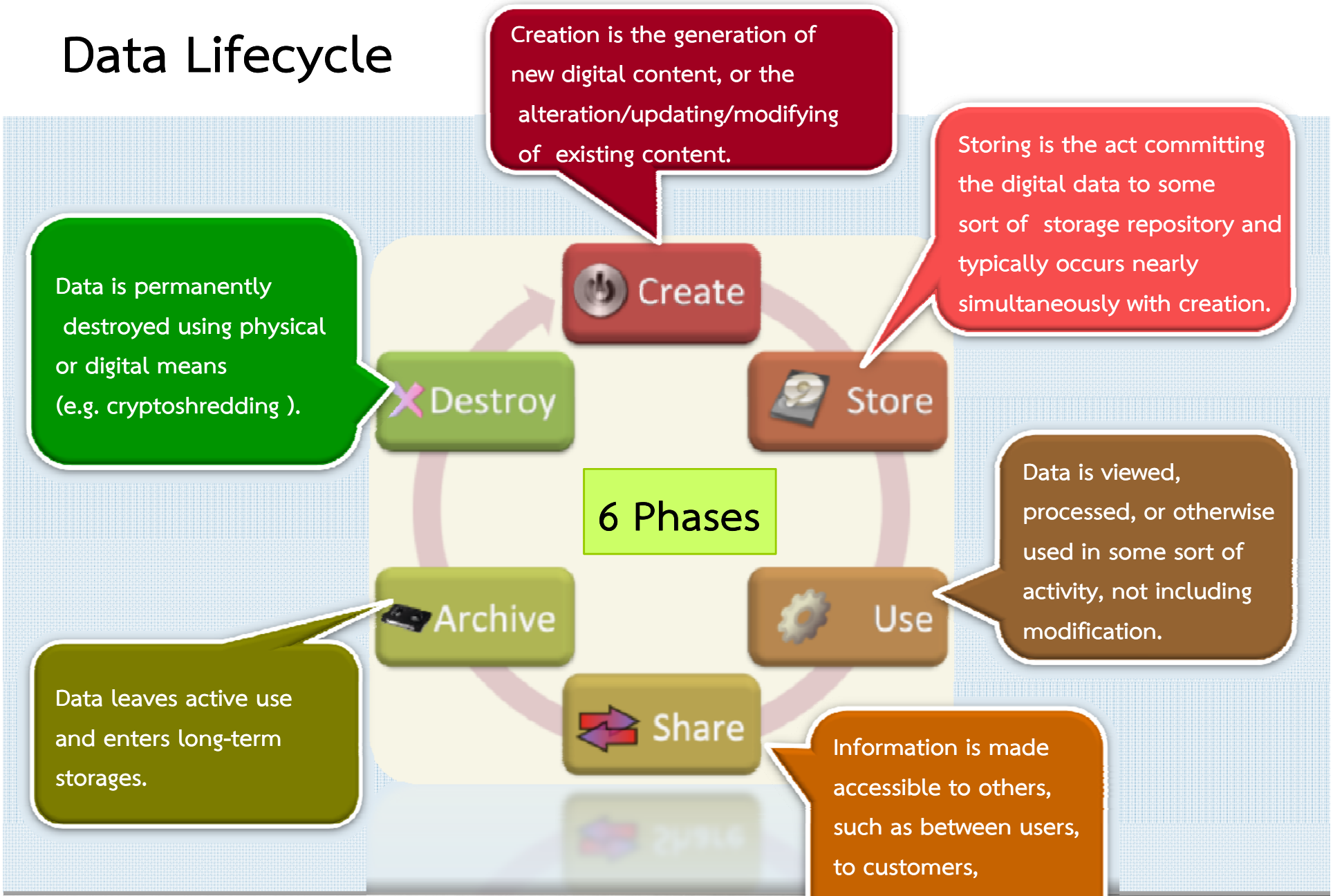
- Volume Storage.

  Data may be stored in IaaS volumes attached to instances dedicated to providing the SaaS service.

Data Security Lifecycle

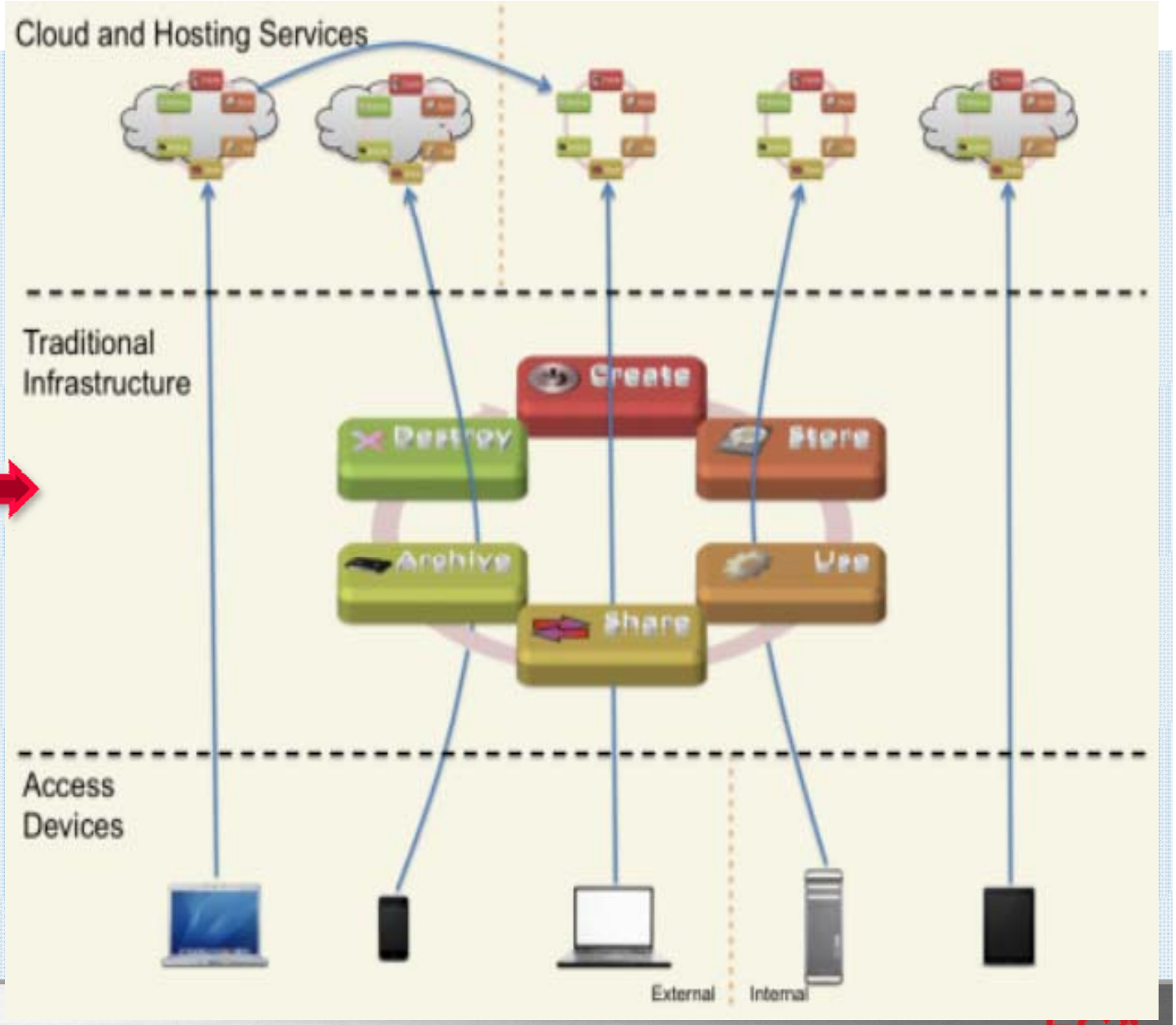
Recommendation by Cloud Security Alliance

Data Lifecycle



Cloud Access Devices

With a variety of data locations (and application environments), each with its own data lifecycle, all accessed by a variety of devices in different locations. Some data lives entirely within a single location, while other data moves in and out of various locations and sometimes directly between external providers.



Source: https://securosis.com/blog/data-security-lifecycle-2.0

Locations and Access

The lifecycle represents the phases information passes through but doesn't address its location or how it is accessed.

Locations:

- Thinking of the lifecycle as a series of smaller lifecycles running in different operating environments.
- At nearly any phase data can move into, out of, and between these environments.
- It is extremely important to understand both the logical and physical of data.

For data security, there are 4 things to understand:

1) Where are the potential locations for my data?
2) What are the lifecycles and controls in each of those locations?
3) Where in each lifecycle can data move between locations?
4) How does data move between locations (via what channel)?

Access:

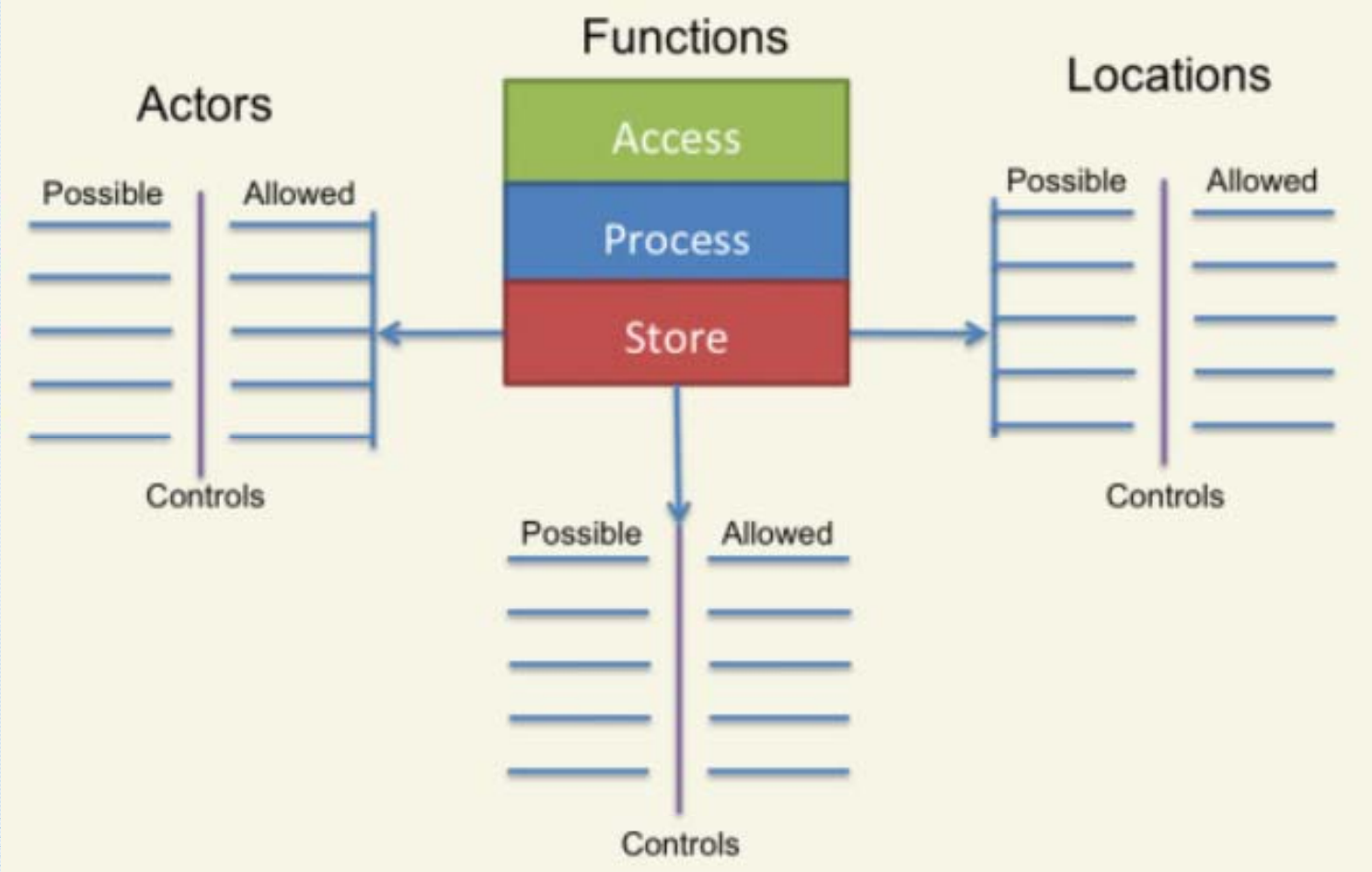
Users need to know who is accessing the data and how. There are 2 factors here:

1) Who access the data?
2) How can they access it (device & channel) ?

Data today is accessed using a variety of different devices. These devices have different security characteristics and may use different applications or clients

Functions, Actors, and Controls

Identifies the functions that can be performed with the data, by a given actor (person or system) and a particular location.



Source: https://securosis.com/blog/data-security-lifecycle-2.0

Functions

There are 3 things we can do with a given datum:

- **Access:** View/access the data, including, creating, copying, file transfers, dissemination,
  and other exchanges of information.
- **Process:** Perform a transaction on the data: update it; use it in a business processing transaction, etc.
- **Store:** Hold the data (in a file, database, etc.)

Information Lifecycle Phases: show which functions map to which phases of the lifecycle

	Create	Store	Use	Share	Archive	Destroy
Access	X	X	X	X	X	X
Process	X		X			
Store		X			X	

An actor (person, application, or system/process, as opposed to the access device) performs each function in a location.

Controls

A control restricts a list of *possible* actions down to *allowed* actions.

EX: encryption can be used to restrict access to data, application controls to restrict processing via authorization, and DRM storage to prevent unauthorized copies/accesses.

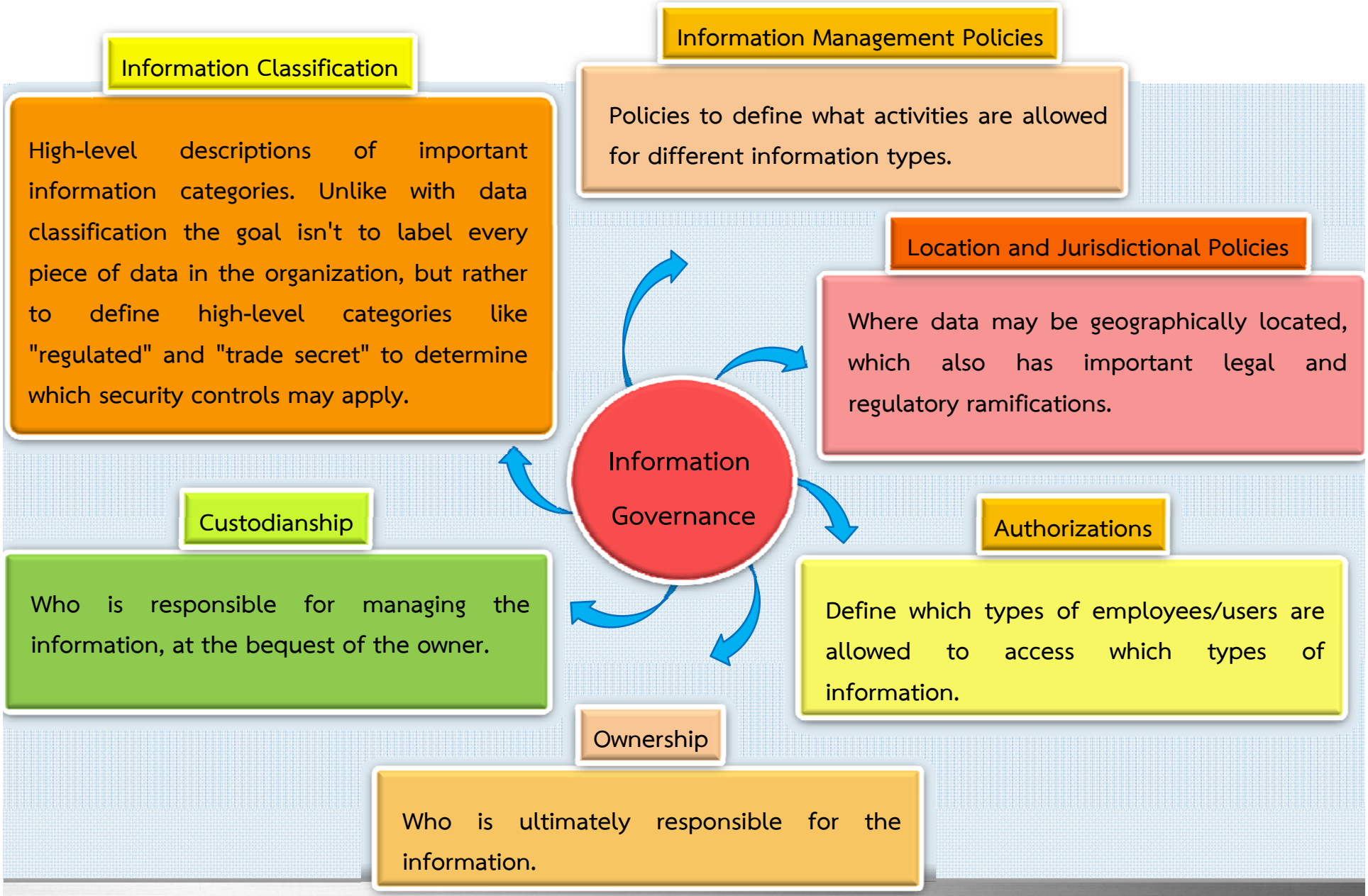
Possible and Allowed Controls:

- First list out all possible functions, locations, and actors; and then which ones to allow.
- Determine what controls we need to make that happen (technical or process)
- Then check whether it is allowed or not. Any time you have a 'no' in the allowed box, you would implement and document a control.

Function		Actor		Location	
Possible	Allowed	Possible	Allowed	Possible	Allowed

Information Governance

Recommendation by Cloud Security Alliance


Information Classification
High-level descriptions of important information categories. Unlike with data classification the goal isn't to label every piece of data in the organization, but rather to define high-level categories like "regulated" and "trade secret" to determine which security controls may apply.
Information Management Policies
Policies to define what activities are allowed for different information types.
Location and Jurisdictional Policies
Where data may be geographically located, which also has important legal and regulatory ramifications.
Information Governance
Custodianship
Who is responsible for managing the information, at the bequest of the owner.
Authorizations
Define which types of employees/users are allowed to access which types of information.
Ownership
Who is ultimately responsible for the information.

Thank you

EGA e-Government Agency www.ega.or.th

EGANews

itegov