

Week 2: Cloud Service Models (IaaS, PaaS, SaaS)

NT524 — Cloud Architecture and Security

PhD. Nguyen Ngoc Tu

September 16, 2025

Learning Objectives (Mục tiêu)

- Motivate service-model choices from **business needs (nhu cầu kinh doanh)** & **org readiness (mức sẵn sàng tổ chức)**.
- Distinguish **IaaS/PaaS/SaaS** & **public/private/hybrid** models; map workloads to each.
- Analyze **cost vs. control (chi phí vs. kiểm soát)** trade-offs; lock-in and compliance impacts.
- Compare provider strategies across models; extract migration/mitigation patterns.
- Practice with Ansible: IaaS (VMs), PaaS (Elastic Beanstalk demo), SaaS (Datadog agent integration).

Why Many Cloud Service Models?

- **Heterogeneous needs (Nhu cầu khác nhau):** No single model can satisfy finance, healthcare, startup, and government workloads.
- **Trade-off balance (Đánh đổi):** Control vs. speed vs. cost vs. compliance.
- **Innovation cycles (Chu kỳ đổi mới):** IaaS = automation/AI; PaaS = container/serverless; SaaS = AI-driven features.
- **Forensic & compliance diversity (Khác biệt về pháp y và tuân thủ):** Evidence collection differs between IaaS vs. SaaS.

Provider Perspective (1/))

1. Market segmentation (Phân khúc thị trường)

- IaaS: **raw control** for enterprises (banking, telecom).
- PaaS: **rapid deployment** for developers/startups.
- SaaS: **ready-to-use apps** for business units (CRM, HR).
- Multi-model portfolio maximizes coverage and reduces churn (giảm thiểu sự xáo trộn).

Provider Perspective (2/)

2. Economies of scale (Kinh tế theo quy mô)

- **Reusing infrastructure:** SaaS runs on top of provider's existing *IaaS/PaaS* (VMs, databases, functions).
Example: AWS QuickSight chạy trên EC2, S3, RDS.
- **Shared infra = lower cost:** Multi-tenant architecture (nhiều khách dùng chung hạ tầng) giúp giảm chi phí trung bình, tăng **profit margin**.
Example: Một cluster Kubernetes phục vụ hàng trăm tenants SaaS CRM.
- **Barriers to entry:** Hyperscalers (AWS, Azure, GCP) có lợi thế nhờ quy mô toàn cầu, startup nhỏ khó cạnh tranh về giá và độ tin cậy.
- **Cross-selling effect (bán chéo):** Provider dễ upsell dịch vụ SaaS cho khách hàng đang dùng IaaS/PaaS.
Example: khách hàng dùng EC2 + RDS \Rightarrow thêm QuickSight BI chỉ vài click.

Takeaway: SaaS không tồn tại độc lập; nó tận dụng IaaS/PaaS. Quy mô lớn = chi phí thấp, lợi nhuận cao, khó bị đối thủ thay thế.

Provider Perspective (3/))

3. Compliance-as-a-service (Cung cấp các gói Tuân thủ luật pháp, chính sách)

- Built-in certifications: GDPR, HIPAA, PCI-DSS.
- Tools: AWS Artifact, vendor Data Processing Addenda (DPA).
- Reduces tenant burden, especially SMEs (doanh nghiệp nhỏ).
- Compliance becomes a competitive differentiator.

Provider Perspective (4/))

4. Innovation platform (Nền tảng đổi mới)

- IaaS: GPUs, AI/ML accelerators, edge computing.
- PaaS: containers, serverless runtimes.
- SaaS: AI copilots, predictive analytics, vertical solutions.
- Multi-model = continuous innovation cycle across layers.

Tenant Perspective (1/)

1. Control vs. Delegation (Kiểm soát vs. ủy thác)

- **IaaS**: tenant manages OS, patching, hardening, monitoring.
- **PaaS**: tenant controls application/data, provider handles runtime/OS.
- **SaaS**: provider manages most; tenant only controls data + config.
- Forensics: IaaS = full access to artefacts; SaaS = limited, need API/log export.
- Action: define shared-responsibility boundaries in runbooks (tài liệu vận hành).

Tenant Perspective (2/)

2. Cost and Skills (Chi phí và kỹ năng)

- **Cost components (Thành phần chi phí):**

- **Service fees (Phí dịch vụ):** compute, storage, managed DB, SaaS licenses, network/egress.
- **Operational manpower (Nhân sự vận hành):** hiring, on-call, SRE/DevOps, SecOps, support contracts.
- **Hidden / ancillary costs (Chi phí ẩn):** data egress, migration & exit fees, training, compliance audits, incident response, backup/restore.

- **Organization fit (Phù hợp theo loại tổ chức):**

- **Startups / SMEs:** tend to prefer *SaaS/PaaS* — lower operational burden, faster time-to-market (tốc độ đưa sản phẩm ra thị trường).
- **Banks / Healthcare / Regulated:** often prefer *IaaS / private* — greater control, data residency, stronger evidentiary posture for audits.

Tenant Perspective (3/)

2. Cost and Skills (Tiếp tục)

- **Decision & management actions (Hành động / Quản trị):**

- Compute **TCO (Total Cost of Ownership / Tổng chi phí sở hữu)** over a 3–5 year horizon, explicitly including people cost and projected egress/migration fees.
- Apply **FinOps practices**: resource tagging, budget alerts, rightsizing, reserved/commitment planning (RI/Savings Plans).
- Consider **managed services** or hybrid deployments when internal skills are limited (thuê ngoài hoặc hybrid khi thiếu kỹ năng).
- Maintain training plans and runbooks to avoid single-person dependencies and reduce MTTR for incidents.

Tenant Perspective (4/)

4. Legal Exposure (Ràng buộc pháp lý)

- Laws regulate data residency, logging/retention, cross-border flows.
- Example: Vietnam Cybercrime Law (Luật an ninh mạng) requires compliance readiness.
- Forensics: SaaS often limits tenant evidence; chain-of-custody crosses provider.
- Mitigations: DPA (Thỏa thuận xử lý dữ liệu), local hosting options, export clauses.
- Action: maintain Legal + Forensics runbook for provider law-enforcement requests.

Tenant Perspective (5/)

Summary Checklist (Danh mục kiểm tra)

- ① Control vs. delegation: which layers are tenant vs. provider?
- ② Cost drivers: service fees + manpower (chi phí nhân sự).
- ③ Skills gap: do we have DevOps/SecOps skills? if not → PaaS/SaaS.
- ④ Lock-in risk: is exit possible in 30–90 days? test exports.
- ⑤ Legal exposure: local laws (e.g., Việt Nam) + provider compliance posture.

Motivation Summary

Provider Drivers (Nhà cung cấp)

- **Market segmentation (Phân khúc thị trường):** IaaS, PaaS, SaaS \Rightarrow nhiều nhóm khách hàng.
- **Economies of scale (Kinh tế theo quy mô):** SaaS tận dụng hạ tầng IaaS để tối ưu chi phí, lợi nhuận.
- **Compliance-as-a-service (Tuân thủ như dịch vụ):** gắn sẵn chứng nhận (GDPR, HIPAA, PCI).
- **Innovation platform (Nền tảng đổi mới):** đa mô hình giúp duy trì cạnh tranh và sáng tạo.

Tenant Drivers (Người thuê)

- **Control vs. delegation (Kiểm soát vs. ủy thác):** IaaS = kiểm soát nhiều; SaaS = NCC quản lý nhiều.
- **Cost & skills (Chi phí và kỹ năng):** Startup \Rightarrow SaaS/PaaS; Ngân hàng \Rightarrow IaaS/private.
- **Lock-in risk (Rủi ro khóa chặt):** APIs độc quyền vs. open standards; cần chiến lược thoát (exit).
- **Legal exposure (Ràng buộc pháp lý):** Ví dụ Việt Nam \Rightarrow sẵn sàng tuân thủ luật an ninh mạng.

Service Model Pyramid (Kim tự tháp dịch vụ)

SaaS (Phần mềm như dịch vụ)

Bạn quản lý: dữ liệu, cấu hình, người dùng/quyền truy cập;

Nhà cung cấp quản lý: ứng dụng, nền tảng, hạ tầng

Ví dụ: *Microsoft 365, Salesforce, Google Workspace*

PaaS (Nền tảng như dịch vụ)

Bạn quản lý: ứng dụng, dữ liệu;

Nhà cung cấp: runtime, middleware, OS, scaling, hạ tầng

Ví dụ: *AWS Elastic Beanstalk, Google App Engine, Azure App Service*

IaaS (Hạ tầng như dịch vụ)

Bạn quản lý: OS, middleware, ứng dụng, dữ liệu;

Nhà cung cấp: ảo hoá (hypervisor), phần cứng, mạng, DC

Ví dụ: *AWS EC2, Azure VMs, Google Compute Engine, OpenStack*

- **Responsibility shift (dịch chuyển trách nhiệm):** Khách hàng quản lý nhiều hơn ở IaaS, ít dần khi lên PaaS, và tối thiểu ở SaaS.

Decision Framework - IaaS, PaaS, SaaS (Khung quyết định)

- **Tiêu chí chính:** kiểm soát, tốc độ triển khai, chi phí, tuân thủ, kỹ năng đội ngũ, **lock-in**.

Tiêu chí	IaaS	PaaS	SaaS	Trọng số
Kiểm soát (control)	5	3	1	0.25
Tốc độ (speed)	2	4	5	0.20
Tuân thủ (compliance)	4	3	3	0.20
Chi phí vận hành	2	4	5	0.20
Kỹ năng đội ngũ	3	3	5	0.15

Gợi ý: Tô điểm số theo trọng số để chọn mô hình cho từng *workload*, không phải toàn doanh nghiệp.

Cloud Lock-in Risk Analysis (Phân tích Rủi ro khóa chặt)

- **Identity lock-in (Khoá chặt định danh)** Phụ thuộc IAM/IdP riêng của provider (AWS IAM, Azure AD). *Mitigation*: dùng chuẩn mở (SAML, OIDC), external IdP (Okta, Keycloak).
- **Data lock-in (Khoá chặt dữ liệu)** Dữ liệu ở format độc quyền, khó xuất/import (ví dụ: BigQuery export, SaaS CRM schema). *Mitigation*: dùng format chuẩn (CSV, Parquet, JSON), kiểm tra export API.
- **API/Service lock-in (Khoá chặt API/dịch vụ)** Sử dụng API độc quyền (AWS DynamoDB, Google Spanner) không port sang provider khác. *Mitigation*: ưu tiên open API, abstract qua middleware (Terraform, Kubernetes).
- **Tooling/Skill lock-in (Khoá chặt công cụ/kỹ năng)** Đội ngũ chỉ quen tool/cloud duy nhất (CloudFormation, Azure Resource Manager). *Mitigation*: đa kỹ năng, dùng tool đa-cloud (Terraform, Ansible, Crossplane).

Note: Always maintain an *exit strategy* (kế hoạch thoát) để giảm rủi ro.

Decision Example: Online Banking App (Ngân hàng trực tuyến)

Workload yêu cầu: dữ liệu nhạy cảm, tuân thủ (compliance) nghiêm ngặt, kiểm soát cao.

Tiêu chí	IaaS	PaaS	SaaS	Trọng số
Kiểm soát	5	3	1	0.35
Tốc độ triển khai	2	4	5	0.20
Tuân thủ	4	3	3	0.20
Chi phí vận hành	2	4	5	0.15
Kỹ năng đội ngũ	3	3	5	0.10
Tổng điểm	3.55	3.35	3.2	1.00

Kết luận: Trong kịch bản ngân hàng, **IaaS** được ưu tiên hơn vì đáp ứng tốt tiêu chí kiểm soát và tuân thủ, mặc dù chi phí vận hành cao hơn.

Lưu ý: Với workload khác (ví dụ: ứng dụng SaaS CRM cho marketing), điểm số sẽ nghiêng về **SaaS**.

Decision Example: Startup E-commerce App (Ứng dụng thương mại điện tử)

Workload yêu cầu: tốc độ triển khai nhanh, chi phí thấp, dễ vận hành; ít yêu cầu tuân thủ.

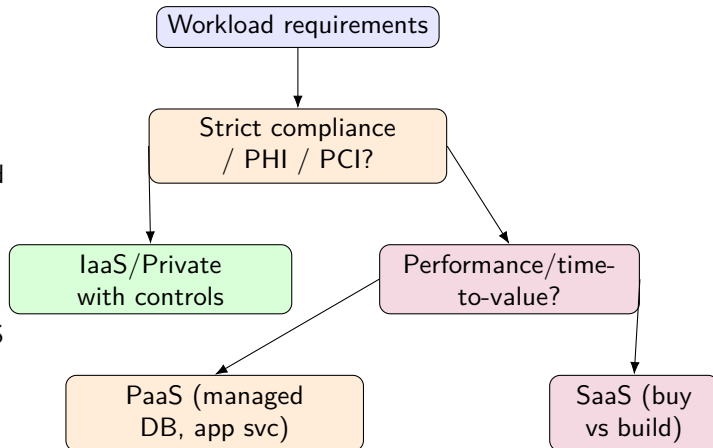
Criterion	IaaS	PaaS	SaaS	Weight
Control	5	3	1	0.10
Speed of deployment	2	4	5	0.30
Compliance	4	3	3	0.10
Operational cost	2	4	5	0.30
Team skills	3	3	5	0.20
Total score	2.85	3.45	4.20	1.00

Conclusion: Trong kịch bản startup, **SaaS** là lựa chọn phù hợp nhất vì tốc độ triển khai nhanh, chi phí thấp, và yêu cầu kỹ năng thấp.

Note: Trade-off: kiểm soát thấp, rủi ro lock-in cao hơn.

Service-Model Decision Tree (Cây quyết định)

- **Compliance & data sensitivity?**
⇒ Private/IaaS or vetted PaaS/SaaS with BAA/DPA.
- **Time-to-market critical?** ⇒ SaaS/PaaS first; revisit IaaS if need deep control.
- **Runtime specialization?** (GPU, kernel mods) ⇒ IaaS.
- **Elastic traffic & events?** ⇒ PaaS serverless/managed runtimes.
- **Operational maturity?** (DevOps skill) ⇒ lower ops = PaaS/SaaS.
- **Exit strategy?** prefer open standards, data export, IaC abstractions.



Fit Matrix (Ma trận phù hợp)

Workload	IaaS	PaaS	SaaS	Note
Regulated core banking	✓	—	—	Data residency
Web & mobile API	—	✓	—	Autoscale
Analytics/BI	—	✓	✓	Data gravity
Collaboration/CRM	—	—	✓	SSO/SCIM
ML training (GPU)	✓	✓	—	Cost bursty
Legacy ERP	✓	—	—	Lift/shift

Activity: Teams pick 3 workloads, justify placement with constraints (compliance, skills, cost).

Responsibility Analysis by Model (Trách nhiệm theo mô hình)

Layer	IaaS	PaaS	SaaS
Applications & Data	Customer	Customer	Customer (config/-data)
Runtime / Middleware	Customer	Provider	Provider
Operating System (OS)	Customer	Provider	Provider
Virtualization / HW / DC	Provider	Provider	Provider
Security & IAM	Shared (mostly Customer)	Balanced shared	Shared (mostly Provider)
Compliance	Customer-led	Shared responsibility	Shared responsibility

Note: Responsibility shifts upward — the higher the model (IaaS → PaaS → SaaS), the more the provider manages, and the less the customer controls.

Big Cloud Provider Positioning (Các nhà cung cấp lớn hiện tại)

Nhà cung cấp	IaaS/PaaS nổi bật	SaaS tiêu biểu
AWS	EC2/EBS/VPC; RDS/EKS/Lambda	QuickSight; (Kết nối SaaS: Salesforce, Datadog)
Azure	VMs/VNet; App Service/AKS/Functions	Microsoft 365, Power BI
Google Cloud	GCE/VPC; Cloud Run/GKE/BigQuery	Workspace, Looker Studio
Salesforce	(PaaS: Heroku)	CRM/Sales/Service Cloud
Others	OpenStack (private IaaS), Red Hat OpenShift (PaaS)	Atlassian, GitHub, Zoom, Slack

Public Cloud (Công cộng)

● Pros (Ưu điểm)

- Nhanh chóng scale (tăng/giảm tài nguyên tức thì).
- Dịch vụ phong phú (AI/ML, CDN, DBaaS, serverless).
- Chi phí ban đầu thấp, phù hợp OPEX model.
- Triển khai nhanh cho startup / SME.

● Cons (Nhược điểm)

- Ít kiểm soát hạ tầng vật lý.
- Vấn đề về dữ liệu (data residency, cross-border).
- Tuân thủ khó khăn cho ngành nghiêm ngặt (PCI-DSS, HIPAA).

● Use cases (Tình huống): SME/startup, web/mobile apps, bursty workloads.

Private Cloud (Riêng tư)

- **Pros (Ưu điểm)**

- Kiểm soát tối đa toàn bộ hạ tầng và dữ liệu.
- Bảo mật và tùy biến cao (hardening, isolation).
- Dễ chứng minh tuân thủ (PCI-DSS, HIPAA, GDPR).

- **Cons (Nhược điểm)**

- Chi phí CAPEX và OPEX cao (mua + vận hành).
- Thiếu khả năng scale nhanh như public.
- Cần đội ngũ IT chuyên sâu (Ops, SecOps).

- **Use cases (Tình huống):** Ngân hàng, y tế, chính phủ, dữ liệu nhạy cảm.

Hybrid Cloud (Hỗn hợp Công cộng và Riêng tư)

- **Pros (Ưu điểm)**

- Kết hợp linh hoạt Public + Private.
- Đặt workload theo yêu cầu (placement flexibility).
- Hỗ trợ di trú dần (phased migration).
- Tăng khả năng DR (disaster recovery) đa nơi.

- **Cons (Nhược điểm)**

- Phức tạp trong quản lý (identity, policy, networking).
- Chi phí kết nối (VPN, interconnect).
- Đòi hỏi kiến trúc hybrid & governance rõ ràng.

- **Use cases (Tình huống):** Data residency, partial migration, multi-region DR.

Industry Trend: Shift from Public to Hybrid Cloud

- **Global shift:** Many enterprises are moving from *Public-only* to *Hybrid* or *Multi-cloud* strategies.
- **Drivers:**
 - Cost control (ẩn phí egress, vận hành dài hạn).
 - Data residency & compliance (GDPR, HIPAA, luật an ninh mạng Việt Nam).
 - Latency-sensitive workloads (real-time, edge processing).
 - Business continuity & DR (disaster recovery).
- **Challenges:**
 - Quản lý phức tạp (networking, identity, policy đồng bộ).
 - Đòi hỏi kỹ năng hybrid/multi-cloud chuyên sâu.

References:

- Mordor Intelligence – Hybrid Cloud Market Report
- IMARC Group – Hybrid Cloud Market Statistics 2024–2033
- Allied Market Research – Hybrid Cloud Market Outlook 2023–2033
- Capgemini UK – Migration from Public Cloud back to Hybrid

Case Study: Finance vs. Healthcare (Tình huống)

• Finance (Ngân hàng/Fintech):

- *Drivers*: PCI-DSS, chống gian lận, độ trễ thấp, DR (khôi phục sau thảm họa).
- *Mix*: Core trên IaaS/private; kênh số & phân tích dùng PaaS; SaaS cho CRM/ITSM.
- *Patterns*: Private link, KMS/HSM, tokenization, network isolation chặt.

• Healthcare (Y tế):

- *Drivers*: HIPAA/PHI, chia sẻ hồ sơ, thiết bị IoT y tế.
- *Mix*: SaaS EHR + PaaS analytics (ẩn danh dữ liệu); IaaS cho hệ thống di sản.
- *Patterns*: Audit mạnh, DLP, encryption mọi nơi, BAA (phụ lục kinh doanh liên kết).

Cost Analysis & Mitigation (Chi phí & giảm thiểu)

- **Cost drivers:** compute giờ/GB, lưu trữ/tầng (tier), egress, request, license PaaS/SaaS, nhân sự vận hành.
- **Mitigation (IaaS):** rightsizing, **RI/Savings Plans**, autoscaling, spot, lifecycle S3/Swift.
- **Mitigation (PaaS):** scale-to-zero, scheduled scaling, connection pooling, tối ưu query (RDS/BigQuery).
- **Mitigation (SaaS):** license governance, SSO/SCIM deprovision, audit sử dụng.
- **FinOps:** tagging bắt buộc; budget/alerts; showback/chargeback.

Anti-patterns (Phản mẫu)

- **Lift-and-shift lên PaaS/SaaS:** kỳ vọng “tự chạy” nhưng ứng dụng không phù hợp.
- **IaaS over-provision:** VM quá cỡ, nhiều EIP/volume nhàn rỗi.
- **Shadow IT SaaS:** không SSO/DLP; rò rỉ dữ liệu.
- **Lock-in mù quáng:** phụ thuộc API độc quyền mà không đánh giá rủi ro thoát (exit).

Security & Compliance by Model (Bảo mật/tuân thủ)

- **IaaS:** cứng hoá OS, patching, SG/NACL, key management (KMS/Barbican), logging/audit (CloudTrail/Keystone).
- **PaaS:** secret management, network policy, DB encryption, rotate credentials, minimal privileges.
- **SaaS:** SSO/SAML/OIDC, SCIM, DLP, backup/export, data residency, vendor risk review.

Practice Overview (Thực hành)

- **IaaS:** Tạo VM trên OpenStack & AWS bằng Ansible; hardening cơ bản; SG đúng.
- **PaaS:** Tạo ứng dụng & môi trường Elastic Beanstalk; deploy gói mẫu.
- **SaaS:** Tích hợp Datadog (giám sát SaaS) vào VM bằng agent & API key.

Ansible: OpenStack VM (IaaS)

```
- hosts: controller
  tasks:
    - name: Create keypair
      openstack.cloud.keypair:
        state: present
        name: wk2-key
        public_key_file: ~/.ssh/id_rsa.pub

    - name: Create server
      openstack.cloud.server:
        state: present
        name: wk2-web-01
        image: ubuntu-golden-v1
        flavor: m1.small
        network: wk2-net
        key_name: wk2-key
        security_groups: ["default"]
```


Ansible: AWS EC2 (IaaS)

```
- hosts: localhost
  connection: local
  collections:
    - amazon.aws
  tasks:
    - name: Launch EC2
      amazon.aws.ec2_instance:
        name: wk2-ec2-01
        key_name: wk2-key
        instance_type: t3.micro
        image_id: ami-1234567890abcdef0 # replace per region
        vpc_subnet_id: subnet-abc123
        security_groups: ["sg-web"]
        tags: { Project: Week2, Owner: TeamX }
        wait: true
```

Ansible: Elastic Beanstalk (PaaS) — App & Env

```
- hosts: localhost
connection: local
collections:
  - community.aws
tasks:
  - name: Create EB application
    community.aws.elasticbeanstalk_app:
      name: wk2-eb-app
      state: present
  - name: Create EB application version
    community.aws.elasticbeanstalk_app_version:
      app_name: wk2-eb-app
      version_label: v1
      s3_bucket: my-bucket
      s3_key: wk2/sample-app.zip
  - name: Create EB environment
    community.aws.elasticbeanstalk_environment:
      app_name: wk2-eb-app
      env_name: wk2-eb-env
      solution_stack_name: "64bit Amazon Linux 2 v3.5.3 running Python 3.8"
      version_label: v1
```

Ansible: Datadog Agent (SaaS Integration)

```
- hosts: iaas_vms
  become: true
  vars:
    datadog_api_key: "DD_API_KEY_PLACEHOLDER"
  tasks:
    - name: Install Datadog agent
      apt:
        name: datadog-agent
        state: present
        register: dd
    - name: Configure Datadog
      copy:
        dest: /etc/datadog-agent/datadog.yaml
        content: |
          api_key: {{ datadog_api_key }}
          tags:
            - project:week2
            - env:lab
    - name: Enable service
      service: { name: datadog-agent, state: started, enabled: yes }
```

Mini Lab (Tóm tắt)

- ❶ IaaS: boot 1 VM ở OpenStack và 1 EC2; kiểm thử SSH/HTTP; SG đúng chuẩn.
- ❷ PaaS: deploy sample lên Elastic Beanstalk; truy cập URL & chụp màn hình.
- ❸ SaaS: cài Datadog agent; xác thực metrics xuất hiện trong dashboard.

Further Reading and Assessment & Deliverables (Bài nộp)

- Find reading material and guides in the "Further Reading_Cloud Service Models (IaaS, PaaS, SaaS)"
- **Báo cáo (3–5 trang):** See Study Tasks and Checklist.
- **Minh chứng:** May demo your some claim in AWS, AZURE or Openstack

Threat Model Lite (STRIDE) theo mô hình

- **Spoofing:** identity/API keys \Rightarrow SSO/MFA, rotate keys, scoped tokens.
- **Tampering:** pipeline deploy PaaS/SaaS \Rightarrow signed artifacts, RBAC, approvals.
- **Repudiation:** thiếu audit \Rightarrow CloudTrail/App logs/SaaS audit, immutable storage.
- **Information Disclosure:** dữ liệu SaaS \Rightarrow DLP, encryption, tenant isolation, data residency.
- **DoS:** quota/Autoscale; WAF/CDN; retry/backoff PaaS.
- **EoP:** quyền admin SaaS/IaaS quá rộng \Rightarrow least privilege, SoD, JIT access.

Wrap-up (Tổng kết)

- Không có “một mô hình cho tất cả” — chọn theo **workload**, ràng buộc, kỹ năng, & chi phí.
- IaaS/PaaS/SaaS tạo **phổ trách nhiệm** khác nhau; hiểu rõ để thiết kế bảo mật & vận hành.
- Lab trải nghiệm: VM (IaaS), Beanstalk (PaaS), Datadog (SaaS).
- Tuần 3: **Virtual Machine Technology**.

Week 2 Deepening Map (Bản đồ chi tiết Tuần 2)

Module	Objectives (Mục tiêu)	Assessment & CLOs
Motivation & Concepts	Clarify boundaries, shared responsibility, provider models	Quick quiz; G1.1
Industry Perspective	Compare finance vs healthcare patterns, lock-in tradeoffs	Case discussion; G1.1, G2.1
Decision Framework	Build fit-matrix & decision tree per workload	Worksheet artifact; G2.1
Hands-on (Ansible)	Launch IaaS VM; deploy a PaaS app; SaaS agent integration	Lab screenshots; G1.1, G2.1
Cost & Risk	Estimate cost, spot lock-in risks & mitigations	Mini-report; G2.1

Alignment: G1.1 (concepts), G2.1 (classify & choose model), Labs feed A2; case/quiz feed A1/A3.

Security-by-Model Checklists (Danh mục kiểm)

IaaS: Harden OS, SG/NACL, key mgmt (KMS/Barbican), patch cadence, baseline AMIs/images.

PaaS: Secrets store, restricted egress, DB encryption, authZ to platform APIs, runtime policy.

SaaS: SSO (SAML/OIDC), SCIM, data export/backup, DLP, tenant isolation, vendor due diligence.

Activity: Map 6 controls for the team's chosen workloads; mark shared-responsibility boundaries.

Provider Adaptation Patterns (AWS/Azure/OpenStack)

- AWS:** EC2/EBS/VPC (IaaS);
 EB/Lambda/RDS (PaaS);
 QuickSight (SaaS).
- Azure:** VM/VNet (IaaS);
- OpenStack:**
- App Service/Functions/AKS (PaaS);
 M365/Power BI (SaaS).
- Nova/Neutron/Cinder (IaaS);
PaaS via add-ons (K8s on IaaS);
 SaaS integrates via agents/APIs.

Exercise: Port the workload across two providers; list changes in networking, identity, and data services.

Study Checklist (Danh mục kiểm tra học tập)

- ❶ Who controls each layer (IaaS, PaaS, SaaS)?
- ❷ What are the main cost drivers (compute, license, human effort)?
- ❸ Where are security compliance responsibilities placed?
- ❹ How easy is exit (exit strategy / mitigation of lock-in)?
- ❺ What challenges exist for forensic readiness (sẵn sàng pháp y)?