ITIL Advanced Practices – Detailed Notes + Use Cases (Day – 2)

Capacity & Performance Management

Objective

Ensure **IT infrastructure and services** meet **current and future** performance requirements **cost-effectively**, without over/under-provisioning.

Key Activities

Activity	**What it means**	**Example**
Monitoring	Track usage of resources	CPU, memory, bandwidth, DB queries
Analysis & Forecasting	Predict future needs	Growth based on business seasonality
Demand Management	Map business demand to resources	E-commerce festival sale forecasting
Performance Tuning	Reduce latency & improve throughput	DB indexing, caching, CDN
Capacity Planning	Budgeting for expansion	Infra roadmap for next 3 years

Capacity Plan Deliverables

- Utilization dashboard (Peak vs Avg)
- Performance bottleneck report
- Scaling strategy → Horizontal / Vertical

Real-World Use Case

FinTech Payment App sees daily peaks at 7–10 PM.
Forecasts show **15% increase** due to new cashback scheme.
Capacity management actions:
✓ Auto-scaling on cloud
✓ DB read-replicas
✓ API rate-limit thresholds
→ No downtime during peak launch event ✅

Availability Management

Objective

Deliver **agreed availability** (SLA uptime) efficiently, managing components, monitoring, resilience, and incident trends.

Availability Concepts

Term	Meaning	Example
Availability	% uptime during agreed hours	99.95% SLA
Reliability	How often failures occur	MTBF (Mean Time Between Failure)
Maintainability	How quickly it is restored	MTTR (Mean Time To Recover)
Serviceability	Vendor support capabilities	Managed WAN provider

Techniques

- **Redundancy** → N+1, clusters
- **Fault Tolerance** → Multi-AZ deployment
- **Predictive Monitoring** → AI ops, health checks
- **Backup & DR Strategies** → RPO/RTO alignment

Real-World Use Case

Online Trading Platform requires ultra-low downtime (< 2 mins/month).
Actions:
✓ Active-active datacenter
✓ Automated failover
✓ Synthetic checks every 30 sec
→ Achieves 99.999% uptime ✅

IT Asset Management (ITAM)

Objective

Control lifecycle of **hardware + software assets** to ensure **compliance, cost optimization & security**.

Two Key Areas

Area	Focus	Tools	Example
HAM – Hardware Asset Management	Physical assets lifecycle	RFID, Asset DB	Laptops, servers, routers
SAM – Software Asset Management	Licensing compliance	License mgmt tools	Windows CALs, Oracle DB licenses

Full Asset Lifecycle

Procure → Deploy → Maintain → Optimize Cost → Retire/Disposal

ITAM Controls

- Warranty tracking
- Renewal alerts
- Unauthorized software detection
- Cloud resource governance (orphaned instances)

Real-World Use Case

During cloud security audit:
✓ Found 120 unused but billed VMs
✓ 20 unauthorized cracked apps
✓ Vendor penalty risk

SAM cleanup saved **₹ 45 Lakhs annually**

Service Configuration Management (CMDB)

Objective

Maintain **accurate knowledge of all Configuration Items (CIs)** and their **relationships** to support decision-making.

What is a CI?

Anything that **impacts a service**:
Servers | DBs | Microservices | APIs | Licenses | Network | Docs

Relationship Mapping (Examples)

- App → Web Server → DB → Storage → Network
- Incident impacts traced via CI dependencies

CMDB Key Concepts

Term	Meaning
CI Attributes	Manufacturer, IP, license key, owner
CI Relationship	Depends-on, Hosted-on, Uses-DB
Configuration Baseline	Approved/verified CI version
Reconciliation	Fixing duplicates/inaccuracies

Supporting Practices

- Change Enablement → update CMDB in every change
- ITAM → sync HW/SW lifecycle
- Incident & Problem → impact mapping

Real-World Flow

Incident: "Checkout API failing ❌"
Service Desk: Use CMDB impact map →
Found failing dependency: **DB node down**
→ Faster RCA and change approval ✅

Combined Use Case – "Major Release in Banking App"

Practice	Role
Capacity & Performance	Ensures infra scaling for new feature
Availability Management	Failover + health checks during rollout
ITAM	License procurement for additional nodes
CMDB	Updated dependency map → faster rollback if needed

Result → **Zero downtime deployment** ✅ and **SLA adherence** ✅

Value Co-Creation & Governance (ITIL 4)

Value Co-Creation

Concept

Value is **not delivered only by service providers** — it's **jointly created** with customers, users & partners through collaboration, transparency & shared goals.

Formula

Value = Outcomes achieved + Optimized Costs + Minimized Risks
achieved *through mutual contribution*

Who are the stakeholders?

Stakeholder	**Primary Role in Value Co-Creation**	**Example**
Customer	Defines value, goals & budget	Bank defining uptime targets
User	Provides feedback & operational insights	App users report transaction delays
Service Provider	Enables technology, support & innovation	Cloud provider scaling infra
Supplier / Vendor	Deliver components required for service	CDN provider improving media delivery
Regulator	Ensures legal & compliance alignment	RBI enforcing KYC compliance

---

Example — UPI Transaction Service

Co-delivery → RBI + Banks + NPCI + App vendors + Telecom operators

Customer wants:
✓ Zero-failed transactions
✓ Fraud-free transactions
✓ Instant settlement

Co-creation actions:

- Banks → API availability & SLA
- NPCI → Routing & fraud checks
- Users → Report failed transactions
- Regulators → Secure transaction protocol

Value is created only when **everyone performs their role**.

Governance in ITIL

Objective

Ensure **policies, controls & decision-making** uphold strategy, compliance & value outcomes.

Governance consists of 3 components:

Component	Purpose	Example
Direct	Set strategic direction	Approve cloud-first strategy
Control	Monitor compliance & risks	Audit cyber incidents / SLA breaches
Evaluate	Review performance vs goals	Balanced scorecards, OKRs

---

Organizational Governance Structures

Structure	Responsibility	Example in IT
Board / Steering Committee	Investment & strategy decisions	Approve Datacenter exit plan
CIO Council	Technology direction	Adopt Zero-Trust architecture
CAB (Change Advisory Board)	Change risk assessment	Production release approvals
PMO	Program governance	Budget vs schedule controls
Information Security Council	GRC oversight	SOC 2 / ISO controls

Governance ensures everyone works **within guardrails** for outcome delivery.

Risk Management & Compliance Alignment

Objective

Identify, analyze & manage risks affecting **service continuity, security & value outcomes**.

Risk categories:

Category	Example Risk
Financial	Cloud cost overrun
Operational	Outage during migration
Security	Data breach via 3rd party
Reputational	Social media backlash

Category	Example Risk
Regulatory	GDPR, RBI non-compliance

4-Step Risk Lifecycle

Identify → Assess → Mitigate → Monitor

Mitigation Strategies:

- **Avoid** → Stop offering high-risk service
- **Reduce** → Multi-AZ deployment & monitoring
- **Transfer** → Outsource or insurance
- **Accept** → Low-likelihood, low-impact

Compliance Alignment

IT services must adhere to regulatory frameworks:

Domain	Example Standard/Regulation
Security	ISO 27001, SOC2
Finance	RBI, PCI-DSS
Privacy	GDPR, DPDP Act (India)
Service Mgmt	ISO 20000-1

ITIL practices embed compliance into **change**, **incident**, **vendor mgmt**, **CMDB**, **capacity/availability mgmt**

Integrated Example – FinTech Card Processing Platform

Goal	Reduce payment failures to < 1%
Governance Role	Approve auto-scaling + NOC 24/7
Value Co-Creation	Banks + card networks + app provider improve reliability
Risk Management	SPOF removal + DDoS protection
Compliance Alignment	PCI-DSS controls for card data

Everyone contributes → customer conversion + trust ↑ → business revenue ↑

Governance – Compliance Domains & Key Regulations

Domain	Purpose / Focus	Example Standards & Regulations	Who Enforces / Applies
Security	Protect information confidentiality, integrity & availability	**ISO 27001**, **SOC 2**, NIST CSF, CERT-IN guidelines	Internal Security Teams, SOC, Cyber Auditors
Finance / Payments	Secure financial transactions, prevent fraud & ensure audit compliance	**RBI** Cybersecurity Master Directions, **PCI-DSS**, SOX (for listed companies)	Banks, FinTech firms, Payment Gateways, Card Service Providers
Privacy & Data Protection	Protect personal & sensitive data of users	**GDPR (EU)**, **DPDP Act (India)**, HIPAA (Health), CCPA (USA)	DPO, Legal & Compliance, Data Governance Teams
Service Management	Establish service quality, lifecycle control & continual improvement	**ISO 20000-1**, ITIL Maturity Assessments	Service Delivery Mgmt, ITSM Leaders, Internal Audits

---

Quick One-Liners for Classroom Recall

- **ISO 27001** → Information Security Management System
- **SOC 2** → Trust Principles (Security, Availability, Confidentiality, Processing Integrity, Privacy)
- **PCI-DSS** → Mandatory if handling card payments
- **GDPR / DPDP Act** → User consent, data minimization, breach reporting
- **ISO 20000-1** → Service delivery excellence aligned to business value

---

Detailed Notes: Key Compliance Standards in IT Governance

ISO 27001 — Information Security Management System (ISMS)

Core Purpose

A systematic framework to **protect information Confidentiality, Integrity & Availability (CIA)**.

Focus Areas

- Risk-based security controls
- Access control & identity governance
- Incident response planning

- Asset classification & secure operations
- Business continuity (BCP/DR)

Why organizations adopt it

✓ Reduced cyber risks
✓ Trusted by partners & regulators
✓ Mandatory in IT outsourcing deals

Used by: All IT/ITES, Banks, Cloud providers

SOC 2 — Trust Services Criteria

Core Purpose

Assures that **service organizations** handle customer data securely.

5 Trust Principles

1. **Security** — Protection from unauthorized access
2. **Availability** — Service uptime & monitoring
3. **Processing Integrity** — Transactions are correct and timely
4. **Confidentiality** — Data restrictions enforced
5. **Privacy** — Personal data handling compliant with law

Why it matters

✓ Required for SaaS & cloud vendors
✓ Market trust for global clients
✓ Third-party risk reduction

Used by: SaaS apps, data centers, BPO/KPO

PCI-DSS — Payment Card Industry Data Security Standard

Core Purpose

Secure **cardholder data** & prevent payment fraud.

Key Controls

- Encryption of card data
- Separate card network from corporate LAN
- Regular vulnerability scans & penetration tests
- Tokenization of payment details
- Strict roles & access restrictions

Who must comply

✓ Banks
✓ UPI/Card payment apps
✓ POS vendors & merchants

Non-compliance → **hefty fines + payment license suspension**

GDPR / IN DPDP Act — Data Privacy Regulations

Core Purpose

Protect **personal data rights** of individuals.

Key Principles

- **Consent is mandatory**
- **Purpose limitation** (collect only what you need)
- **Data minimization & retention control**
- **Right to access / forget**
- **Breach notification requirements**

Enforcement Scope

GDPR → EU residents' data anywhere in the world
DPDP Act (India) → Data fiduciaries inside India

Major penalties for data misuse (e.g., WhatsApp privacy case in EU)

ISO 20000-1 — Service Management System Standard (SMS)

Core Purpose

Standardized approach to **plan, deliver & improve IT services**.

Core Areas

- Service lifecycle governance
- Incident, Change, Problem management alignment
- SLA & availability planning
- Continual improvement
- Supplier control & service assurance

Why adopt

✓ IT services tied closely to business value
✓ Improved user experience (XLA mindset)
✓ Ensures readiness for audits and outsourcing

Often combined with ITIL in large enterprises

Standard	Focus	Applies To
ISO 27001	Information Security	Any IT organization
SOC 2	Cloud service trustworthiness	SaaS & service providers
PCI-DSS	Payment data protection	Banks, merchants
GDPR/DPDP	Personal data rights	Any entity processing personal data
ISO 20000-1	Service management excellence	IT service providers

---

ITIL & Modern Practices

ITIL in Agile, DevOps, and SRE • ITIL vs IT4IT vs COBIT vs ISO 20000 • Cloud & Digital Transformation Integration

---

1) ITIL in Agile, DevOps, and SRE Environments

A. What stays the same vs what changes

Area	Classic ITIL Focus	Modern Adaptation (Agile/DevOps/SRE)
Change Enablement	CAB approvals, lead time	**Risk-based, automated approvals** (policy-as-code), standard changes auto-approved, feature flags, canary
Incident Management	Triage → Assignment	**Swarming**, chatOps, auto-remediation, SRE **incident command** model
Problem Management	RCA docs, known errors	**Blameless postmortems**, error budgets, defect SLOs; track toil reduction
Release Management	Windows, handoffs	**Continuous Delivery**, blue/green, progressive delivery
Service Level Mgmt	SLA % uptime	**SLOs/SLIs + XLAs**; user-centric, latency & quality metrics
Capacity/Performance	Trend + forecast	**Autoscaling**, load testing in pipelines, cost/perf guardrails

Area	Classic ITIL Focus	Modern Adaptation (Agile/DevOps/SRE)
Availability	Redundancy, DR	**SRE reliability engineering** (golden signals, chaos testing)

B. How to blend practices

- **Change** = Pull Request + Pipeline Gates + Observability Sign-off (SLO not violated)
- **Incident** = ChatOps + Runbooks + On-call SRE + Rapid rollback via feature flag
- **Problem** = Postmortem actions added to backlog with owners & deadlines
- **Release** = Trunk-based dev + automated testing + progressive rollout + kill switch
- **Knowledge** = Everything-as-code + runbooks in repo + searchable KB via docs-as-code

C. RACI pattern (pragmatic)

Practice	Product Owner	Dev Team	SRE/Platform	ITSM Lead
Change Enablement	A	R	R	C
Incident	C	R (sev ≤2)	A (sev 1 P1)	C
Problem/Postmortem	C	R	A	C
Release	A	R	C	C
SLM (SLO/XLA)	A	C	R	C

A = Accountable, R = Responsible, C = Consulted

D. Metrics to track (mix SLAs+SLOs+Flow)

- **Reliability**: SLO attainment, error budget burn, MTTR, time to detect
- **Flow/DevOps**: Lead time for change, deployment frequency, change failure rate
- **Customer**: XLA (CSAT/NPS), task success rate, page speed (p95)
- **Operations**: % auto-remediated incidents, toil hours/month, on-call load

E. Anti-patterns to avoid

- CAB as bottleneck for **low-risk** changes → use **policy-as-code** & standard changes
- Postmortems with blame → **no learning, repeat failures**
- SLAs only on uptime → **ignores latency/quality**; adopt SLOs/SLIs
- Separate Dev/Ops tools & data → **slow RCA**; unify telemetry + CI/CD + ITSM

---

2) ITIL vs IT4IT vs COBIT vs ISO 20000 (When to use what)

A. Quick comparison

Framework/Std	What it is	Primary Audience	Scope	Where it shines
ITIL 4	Best-practice guidance (non-cert standard)	Service mgmt teams, operations	Practices across **SVS** (Service Value System)	Day-to-day service design, delivery, improvement
IT4IT (Open Group)	**Operating model/reference architecture** for digital delivery	Enterprise architects, platform/SRE	Value streams: Strategy→Portfolio, Requirement→Deploy, Detect→Correct, etc.	Tool/data integration, end-to-end flow, "backbone" model
COBIT 2019	**Governance & management** of enterprise IT	Execs, risk & audit, compliance	Principles, objectives, governance system design	Board-level governance, control objectives, audit alignment
ISO 20000-1	Certifiable **Service Mgmt System (SMS)** standard	Organizations seeking certification	Management system requirements	External assurance, client RFPs, consistency & audits

B. Integration recipe (simple & powerful)

- **COBIT** sets **governance** & policy guardrails
- **ITIL** describes **how** teams operate service practices
- **IT4IT** provides the **data model & value streams** to integrate tools
- **ISO 20000-1** certifies the **management system** you built

Use **COBIT** for board/steering controls, **ITIL** for team playbooks, **IT4IT** to connect toolchains (backlogs→pipelines→monitoring→ITSM), and **ISO 20000** for external credibility.

---

3) Practical Integration with Cloud & Digital Transformation

A. Map cloud-native building blocks to ITIL practices

ITIL Practice	**Cloud/Platform Enablers**
Change Enablement	GitOps/PRs, CI/CD gates, policy-as-code (OPA), feature flags
Release Mgmt	Blue/green, canary, service mesh traffic shifting
Incident Mgmt	AIOps alerts, runbooks, ChatOps (Slack/Teams), paging (on-call)
Problem Mgmt	Postmortem automation, failure pattern mining, defect SLOs
Service Catalog	Self-service portal + Terraform modules + golden AMIs
Capacity/Perf	Autoscaling, HPA, AWS ASG/Azure VMSS, rightsizing, load tests in CI
Availability	Multi-AZ/region, DR-as-code, chaos experiments
Service Config (CMDB)	**Dynamic CMDB** fed by discovery + IaC state + tags/labels
Supplier/Vendor	FinOps, SaaS risk assessment, contract SLOs, exit plans

B. Cloud tagging & CMDB fusion (field-proven approach)

1. **Standardize tags/labels**: Service=Checkout, Owner=TeamA, Tier=Prod, CostCenter=FIN
2. **Ingest into CMDB** from cloud APIs + IaC (Terraform state) + K8s (labels/annotations)
3. Build **service maps** from telemetry (APM traces) to keep relationships fresh
4. **Gate changes**: deploy only if CMDB/labels complete (policy-as-code)

C. SLOs that matter in digital programs

- Web/API latency p95, error rate, availability
- Business SLIs: checkout success %, search relevance, streaming rebuffering rate
- Experience: Core Web Vitals, app crash rate
- Platform: deployment lead time, % automated rollbacks, cost per request

D. FinOps meets ITIL

- **Capacity Mgmt** ↔ **Rightsizing + Auto-off** non-prod
- **Service Catalog** ↔ **Cost guardrails** baked into templates
- **Change/Release** ↔ **Cost checks** in pipeline (block if 30-day run-rate spike)
- KPIs: unit economics (₹/transaction), wastage %, RI/Savings Plan coverage

E. Reference implementation blueprint (cloud-native)

1. **Plan**: Portfolio mgmt → product roadmaps, value hypotheses, OKRs
2. **Build**: Trunk-based dev, CI with contract & perf tests, SBOM security scans
3. **Release**: Canary via mesh, error-budget guard, auto-rollback
4. **Run**: SRE on-call, golden signals, runbooks, chaos drills, DR tests
5. **Improve**: Postmortems feed backlog, weekly ops review, SLO recalibration

---

4) Templates & Checklists

A. "Risk-based Change" template

- **Change type**: Standard / Normal / Emergency
- **Risk score** (auto): blast radius, rollback ease, prod data touch (Y/N), SLO risk
- **Gates**: tests pass, vulnerability scan, perf budget, CMDB/labels present
- **Decision**: auto-approve if score ≤ threshold; else asynchronous review

B. Blameless Postmortem (Problem Mgmt)

- **What happened** (timeline)
- **Primary impact metrics** (SLOs breached, users affected)
- **Contributing factors** (systems + org)
- **Fix now** (containment) / **Fix forever** (backlog items, owners, dates)
- **Learning & prevention** (playbook update, alert tuning)

C. SLO Starter Kit (per service)

- **Availability**: 99.9% monthly; **Latency p95**: API < 300 ms; **Error rate** < 0.5%
- **User SLI**: Task success > 98% (checkout/search/ride-booking)
- **Alert policy**: Page only on error-budget burn or user-impacting symptoms

---

5) Maturity Roadmap (90-day accelerator)

Days 0–30 (Foundation)

- Define **service boundaries** + owners + tags
- Pick **5 core practices**: Change, Incident, Problem, SLM, Config
- Establish **SLOs** for top 3 user journeys; set on-call; adopt postmortems

Days 31–60 (Automation)

- CI/CD gates (security, perf), standard changes, feature flags

- CMDB auto-discovery + IaC integration; first **service map**
- Start **FinOps** rightsizing; set unit-cost targets

Days 61–90 (Reliability & Scale)

- Error-budget driven release policy
- Chaos drills, DR test, multi-AZ/region for critical services
- Combine ITIL reviews with **product ops**: OKR + SLO scorecards

---

6) Case Snippets

E-commerce IPL Surge: Risk-based change with canary, autoscale, DLQ for orders; result: 0.2% error rate at 4× load.

- **FinTech Reg Audit**: COBIT governance → policy-as-code; ISO 20000 audit passed; cut change failure rate 40%.
- **Media Streaming**: SLOs on rebuffering; cache pre-warm; progressive rollouts; NPS +9 points in 2 quarters.

ITIL Intermediate Certification Prep & Mock Exam

ITIL 4 Intermediate Certification Paths

A. ITIL Managing Professional (ITIL MP)

For **IT operations, technical teams, service managers**.

Module	**Focus**
CDS – Create, Deliver & Support	Service delivery, DevOps, workflows
DSV – Drive Stakeholder Value	Engagement, co-creation, SLAs + XLAs
HVIT – High Velocity IT	Agile, DevOps, SRE, digital transformation
DITS – Direct, Plan & Improve	Lean, governance, continual improvement

Achieves **ITIL Managing Professional** designation when all 4 passed.

B. ITIL Strategic Leader (ITIL SL)

For **leaders, architects & executives**.

Module	Focus
DITS – Direct, Plan & Improve	Shared with MP path
DPIA – Digital & IT Strategy	Digital operating models, governance

Achieves **ITIL Strategic Leader** designation when both passed.

Certification Roadmap

- ITIL Foundation → MP (CDS + DSV + HVIT + DITS)
- ITIL Foundation → SL (DITS + DPIA)
- Completing both → **ITIL Master Pathway**

Exam Structure & Scoring

Aspect	Details
Format	Online, closed-book
Type	Multiple Choice & Scenario-Based
Questions	40 per module
Duration	90 mins
Scoring	Pass = **70% (28/40)**
Language	English + other major languages

Weighted answers in “lead answer” scenarios:

- **Best answer → 4 pts**
- **Second best → 3 pts**
- **Acceptable → 2 pts**
- **Least correct → 1 or 0 pts**

Read scenario **first → then question → then check answers** against SVS principles.

Typical Cost Ranges

- Foundation Level: ~ **US$ 475** for the exam voucher.

- Intermediate / Advanced Modules: Each module typically ~ **US$ 400-$900** depending on region.
- Complete Paths (e.g., MP or SL designation): Total cost often ~ **US$ 750-1,050+** just for exam vouchers before training.
- Training + exam bundle in India: e.g., Foundation + modules range INR ~ 50,000 to 1,50,000 (≈ US$ 600-1,800) depending on cohort.

Example Specifics

- The “Leader: Digital & IT Strategy” module shows a bundled price of **US$ 839 – US$ 1,599** (incl. exam + eLearning) on the official site.
- Exam vouchers in some sources are cited at ~$150-$500 depending on country.