objectives → Δ Law → E-storage → e Sign → e-books → EDI, Ecomm → Efiling (gov) → ETT

- CA Sukriti Jain sukriti9225@gmail.com

SECTION LIST – INFORMATION TECHNOLOGY (AMENDMENT) ACT, 2008

3	Authentication → DSC → Asym Crypto + Hash fx (Technique)
3A	Electronic Sign - reliable → Pvt key linked, Control of Signatory & Any Alt to data/sign is detectable
4	E-records – Creation
5	E- Sign – Authentication.
6	E-Governance – E-Filing, E-Reply, E-payment
6A	E-service + Authorised + Scale of service charge fixed by gov.
7	Retention of E-records → 3 cond - ① Assessible for subsequ ② form format same ③ id origin, dest, date/time.
7A	E-audit (N.A. → Law पालन, Autoform, E gazette)
8	E-Gazette
9	No right to insist 'e'
10	Power of CG to make Rules for E-sign
10A	E-Contracts
14	secured E-records – Encryption ↔ Decryption तक
15	secured E-signature – secured if → ① Exclusive control of signatory ② stored & Affix as prescribed
16	security procedures & practices
43	offences – Virus access SD & steal ₹ + sec 66 punish
43A	Failure to protect data + Sec 85
44	Penalty – not submit info - Failure 150000 Belated 5000/day Books 10000/day
45	Residuary penalty ≤ 25000
65	Tampering computer Source code
66	Punishment for Offences (sec 43) (3 yr / + 5 lacs)
66A	Offensive message → grossly offensive, known to be false, (email to mislead/annoy - हत्या की murder)
66B	Buyer of stolen computer – knowingly buy – पता था चोरी का माल है
66C	identity theft → ESC & Pwd, kisi aur ka use
66D	cheating by personating → via computer/online – Faked, UTV audition, Phishing, Nigerian scam, spoof (my FB)
66E	images of private area – without consent
66F	cyber terrorism → commit/conspire → DOS, Unauth Access, virus → Threat unity/int./sov of India, CII, foreign relation (ie against देश की सत्ता) (Lifetime)
67	obscene Material – वाहियात Pics (1st गलती) (फिल्मों जैसे)
67A	Adult - sexually explicit act
67B	Baccha - sexually explicit, Non veg msg, image, browse, download, send (abuse online)
67C	Intermediary to Retain Preserve info – call logs (3 yr)
69	Power of CG to intercept, Decrypt, monitor any info – if against देश की सत्ता [sec 68 - controller give direction to CA]
69A	blocking from Public Access – Any info – if it is against देश की सत्ता or for investigation – eg - News channel
69B	CG-authority to access computer – collect Traffic Data/info – to enhance cyber security, prevent intrusion, spread of virus
70	Protected system – Critical Info Infrastructure – unauth Access/Attempt (10 years)
70A	National Nodal Agency – measures (R&D) to protect CII
70B	Indian computer emergency response team (ICERT) – incident Response, collect info, forecast, measures, coordinate, guidelines
71	Misrepresentation – obtain license / ESC
72	Misuse of power – Breach of Confidentiality & Privacy – by gov officials – having power, to access info, under this Act
72A	breach of Lawful contract – Disclosure of Info – while providing services – eg - CA, employee. Sj
73	Publishing False ESC/DSC – invalid DSC – Not issued/accepted or suspended - ias
74	Valid DSC used to do Fraud
75	scope → India + J|K + Offence of/s India, computer I|I
76	confiscation → computer used in offence – if owner innocent है – तो Actual Criminal को पकड़ो।
79	intermediary – not liable → Provided only access to Network; Due diligence; पता चलने पे Remove/disable access → Not Aid, induce, conspire the sender → Not start txn, select receiver, Δ info
79A	Examiner of Electronic Evidence – expert opinion in Court
79	power of police → search & arrest w/o warrant – from public place – Suspected to commit/ comited/ting offence
80	Overriding effect → except copyright, Patent
81A	Electronic & Truncated Cheque – cyber law subject to negotiable instrument act
84B	Abet offence – उकसाना षड्यंत्र → same punishment as offence
84C	Attempt to commit – असफल प्रयास → same punishment as offence – jail 50% / fine 100% / both.
85	offences by company → also liable if consent, connivance, Neglect. Not Liable - if prove - due diligence & w/o knowledge

Steps to Comply IT Act → Std → Procedure → safeguard → Training → Officer → Report

Requirements of Various authorities for System Controls & Audit:

(1) RBI - Sample areas of review covered by IS audit / KEY AREAS of IS audit :- (More imp)

System Controls

1. *Programmer & operator should be different*
2. *Contingency plans introduce & tested* (BCP)
3. *Appropriate controls to protect system from attacks*
4. *Uniformity of software used by various branches*
5. *BOD & Top M ensure effectiveness of internal controls* — BoD Responsible
6. *Annual review of IS audit policy to ensure its relevance & effectiveness*
7. *Quality Assurance of internal audit & IS audit – at least once every 3 years* — QA 1/3 — 1-3

System Audit - checklist given by RBI → 32 pt acc. Audit

1. *Separate IS Audit function* within Internal Audit department.
2. **Reporting** to Internal Audit Head or Chief Audit Executive (CAE)
3. IS auditor- **independent**, exercise due professional care.
4. competent - have **skills, knowledge, Training,** experience & qualified & have **professional certificates**
5. IT Gov, Info Security gov, IT General Controls, critical biz applications/system, having financial/compliance implications, regulatory Requirement & risk management must be **IS Audit @least once a year** — 1-1
6. cover branches, with focus on **large & medium branches**
7. **Pre-implementation review** & **Testing of controls** on new developed systems – to ensure that Existing Controls not diluted while migrating to new applications, Controls to meet regulatory requirement & bank policies (CORE)
8. **Post implementation review** of application controls, to confirm controls are operating effectively.
9. Detailed audit of **SDLC process** to ensure security features are incorporated in new systems
10. ensure **data integrity** in new system & review **data migration** from legacy to new system.
11. **Validate IT risk** before launch of service
12. Review **residual risk** & if it is inappropriate, then discuss with senior management
13. LFAR has specific questions relating to IT security, BCP, which needs to be reviewed by Statutory auditors

RBI inspection wing which conducts inspection of banks & NBFC. It review scope, coverage, frequency & report of systems audit. If discrepancy – report to M .

(2) IRDA (less imp)

IRDA - PRELIMINARIES -Information to be obtained by the auditor before starting audit:

1. Locations
2. IT applications used
3. Layout of IT & network infrastructure
4. Centralized or decentralized applications
5. unresolved issues in Previous internal & statutory audit & IRDA inspection reports,
6. Internal circulars & guidelines
7. Standard Operating procedures (SOP)
8. List of new products introduced & IRDA approval for them
9. List of all investments, classified as per IRDA guidelines
10. IRDA correspondence, notifications, circulars, guidelines, etc
11. IT security policy — Sj
12. Network security report of IT assets
13. BCP

IS Audit - 1-3

- Audit at least **once in 3 years** by a CA firm
- Current internal/concurrent/statutory auditor is **not eligible** for appointment
- CA firm must have minimum **3 to 4 years experience** of IT audit of banks, MF, Ins co.

IRDA - SYSTEMS CONTROLS

- **electronic transfer of data** without manual intervention.
- All Systems **integrated**.
- Procedures to review & maintain **Audit Trail** for Data entry, authorization, cancellation, modifications.
- Auditor **Comment** on audit trail maintained.
- Ascertain that - System has separate login for each user & maintains trail of every transaction wrt user ID, date, time.

SEBI (Most imp)

System Audit - As per SEBI stock exchanges shall conduct annual systems audit as follows:

1. Audit conducted as per norms & **Terms of references (TOR)** & Guidelines issued by SEBI
2. appoint Auditor as per the prescribed **selection norms**
3. Same Auditor can perform max **3 successive audits**
4. **Proposal** from auditor submit to SEBI for records.
5. **Audit schedule** submitted to SEBI at least **2 months** in advance
6. **Scope** of audit may be **extended by SEBI** considering the changes since last year
7. Audit report be **submitted** to **auditee**.
8. Audit report to specify compliances & **non-compliances, observations** for minor deviations & qualitative comments for scope of improvement & also cover any open issues in previous year audit report.
9. **Auditee Mgmt to comment** on Non conformities (NC) & Observations. **Corrective actions** must be taken within **3 months** & reported to SEBI
10. Auditor to indicate if- **Follow on audit** required, to review status of NC
11. **Report & Comments** of auditee - **submitted to SEBI** within **1 month**

SEBI - Auditor Selection Norms:

1. **Min 3 years experience** of IT audit of stock exch
2. Auditor **Certification- CISA**, CISM, CISSP
3. Auditor should have **IT audit framework** like **COBIT**
4. Auditor should have **no conflict of interest**. Not have been engaged over last 3 years for any consulting engagement by the entity under audit.
5. Auditor should **no cases pending** against Previous auditees under SEBI.

SEBI - Audit Report Norms:

1. **Systems audit report** with comments of auditee, be **communicated to SEBI**
2. Audit report should have **explicit coverage** of each major **area** mentioned in **TOR**, indicating any **NC** or **observations**
3. Auditor should also provide **qualitative inputs** about **ways to improve the process,** based on best practices.

System Control –

- Along with audit report, stock exchange required to submit a declaration from MD/ CEO certifying security & integrity of IT system.
- Proper audit trail for upload/ maintenance/ download of KYC data to be maintained.
- GOI maintains panel of System auditors, which are used by govt enterprises for system audit

Cyber Forensic and Cyber Fraud Investigation

- **latest scientific technique** - emerged due to effect of increasing computer frauds.
- **Cyber** means 'net'. **Forensic** means scientific method of investigation & analysis techniques, to gather, procee; interpret evidence & use it in court of law.
- **Cyber Investigation** is an investigation method gathering digital evidences to be produced in court of law
- **cyber laws** now permit courts to rely upon **digital evidence**.
- Cyber forensic use **special methods** to gather electronic evidence, which stand the rigorous scrutiny, when presented in court.
- To ensure that above objectives are achieved, experts use **standard process & globally accepted methods** so that **same results** will be achieved if the **same evidence** is **checked by another expert**.
- Cyber frauds are increasing globally so there is increase in demand of cyber forensic experts also.
- ICAI – "Certificate course on Forensic accounting & Fraud detection" - to CA

Security Standards

CA Sukriti Jain

Information Security is essential in day-to-day operations of enterprises. Security breaches can lead to substantial impact on the enterprises. **COBIT 5** (published by ISACA, USA) highlights the **NEED** for enterprises to implement information security.

NEED FOR INFROMATION SECURITY – Risk ↓ CIA

- Maintain **information risk at acceptable level** & **protect information** from unauthorized disclosure/access.
- Ensure **continuous availability** of services & systems, leading to user satisfaction. ☺
- Comply with relevant **laws & regulations** & contractual requirements on information security. 43A
- **Achieve** above needs at same time, **controlling costs of IT services** & Technology Protection

NATIONAL CYBER SECURITY POLICY 2013

Considering the importance of security, GOI recently published NCSP 2013. The policy highlights the vulnerabilities & the need for security of cyberspace. Cyber attacks can cause extensive damage to the information infrastructure or key assets. Also disrupting the functioning of critical information systems. This may threaten lives, economy & national security. To mitigate the damage caused by malicious cyberspace activity, rapid identification, information exchange, investigation & coordinated response is needed. The protection of information infrastructure & **preservation of CIA of information** is the essence to secure cyberspace.

Vision: *To build a secure & resilient cyberspace for citizens, business & government*
↳ able to recover quickly from difficultys.

Mission: CIA

- *To protect information & information infrastructure in cyberspace,*
- *build capabilities to prevent & respond to cyber threats,* 43+66
- *reduce vulnerabilities & minimize damage from cyber incidents through a combination of institutional structures, people, processes, technology & cooperation.*

Major objectives of NCSP are-

1. **create a secure cyber ecosystem** & generate adequate **trust & confidence** in IT systems & txn
2. Assurance framework to **design security policies & compliance** of global security standards & best practices
3. **Regulatory framework** to ensure secure cyberspace ecosystem.
4. create **24*7** Mechanism for obtaining strategic information regarding threats to IT infrastructure.
5. operate **24*7** National Critical Information Infrastructure Protection Center (NCIIPC), for protection of nation's Critical Info Infrastructure.
6. develop suitable indigenous **security technologies** to achieve national security requirements.
7. To improve **integrity of IT products & services** & testing them for security.
8. To create a **workforce** of 500000 professional skilled in cyber security in next 5 years
9. To provide **fiscal benefits to businesses**, for adoption of standard security practices
10. To protect information to safeguard **privacy of data** & **reduce economic losses** due to data theft
11. To **prevent cyber crimes** by enhancing cyber law capabilities.
12. To create a **culture** of cyber security & privacy जागरूकता
13. To develop **public private partnerships** & collaborative engagements for enhancing security of cyberspace
14. To enhance **global cooperation** for security of cyberspace

Few Standards & Frameworks used in cyber security are-

- ✓ ISO 27001
- ✓ SA 402
- ✓ ITIL

1. ISO 27001:

ISO/IEC 27001 (International Organization for Standardization – ISO) (International Electro-Technical Commission – IEC) tells **how to implement information security in any kind of organization**. Organization which implements ISO 27001, gets **certified** by independent certification body, **which confirms that info security has been implemented in the best possible way in the organization.**

ISO 27001 is international best practice standard to implement ISMS. It formally specifies the Information Security Management System (ISMS), a series of activities to identify, analyze & address the information security risks. It is a systematic approach to manage confidential & sensitive information so that it remains secure ie – CIA. ISMS ensures effective security arrangements coordinated consistently & cost effectively.

❖ How The Standard Works?

ISO 27001 requires that management –

- *Systematically examines organization's information security **risks**, **threats**, **vulnerabilities** & **impacts**;*
- *Designs & implements a coherent & comprehensive suite of information security **controls** & other forms of **risk treatment** (such as risk avoidance or risk transfer) to address those risks that are deemed unacceptable; &*
- *Ensure that the information security controls continue to **meet** the organization's information security **needs** on an ongoing basis.*

❖ *History*

ISO/IEC 27001 is derived from The British Standard BS 7799 Part 2, published in 1999. BS 7799 Part 2 was revised by BSI in 2002, explicitly incorporating Deming's PDCA process concept, & was adopted by ISO/IEC as ISO/IEC 27001 in 2005. It was extensively revised in 2013, bringing it into line with the other ISO certified management systems standards & dropping the PDCA concept.

(a) **ISO/IEC 27001: 2005**, part of the growing ISO/IEC 27000 family of standards, was an ISMS standard published in October 2005 by ISO/IEC. Its full name is "ISO/IEC 27001:2005 –IT – Security techniques – ISMS – Requirements". It was superseded, in 2013, by ISO/IEC 27001:2013. It consisted of the PDCA cycle.

Plan-Do-Check-Act (PDCA) Cycle or *4 phases of ISMS*

ISMS consists of 4 phases that should be continuously implemented in order to minimize risks to confidentiality, Integrity, Availability (CIA) of information. PDCA cycle never ends & all the activities must be implemented cyclically in order to keep the ISMS effective. ISO/IEC 27001:2005 applies this to all the processes in ISMS.

PDCA Cyclic Process –

1. ***The Plan Phase (Establishing the ISMS)***: This phase serves to plan the basic organization of information security, set objectives for information security & choose the appropriate security controls (the standard contains a catalogue of 133 possible controls).
2. ***The Do Phase (Implementing & Working of ISMS)***: This phase includes carrying out everything that was planned during the previous phase
3. ***The Check Phase (Monitoring & Review of the ISMS)***: The purpose of this phase is to monitor the functioning of the ISMS through various "channels", & check whether the results meet the set objectives.
4. ***The Act Phase (Update & improvement of ISMS)***: The purpose of this phase is to improve everything that was identified as non-compliant in the previous phase.

(b) **ISO/IEC 27001: 2013** is the 1st revision of ISO/IEC 27001 that specifies the requirements for establishing, implementing, maintaining & continually improving an ISMS within an organization. It is an information security standard that was published on 25th September 2013. It also includes requirements for the assessment & treatment of information security risks tailored to the needs of the organization. The requirements set out in ISO/IEC 27001:2013 are generic & are intended to be applicable to all organizations, regardless of type, size or nature. ISO 27001:2013 does not put so much emphasis on the PDCA cycle.

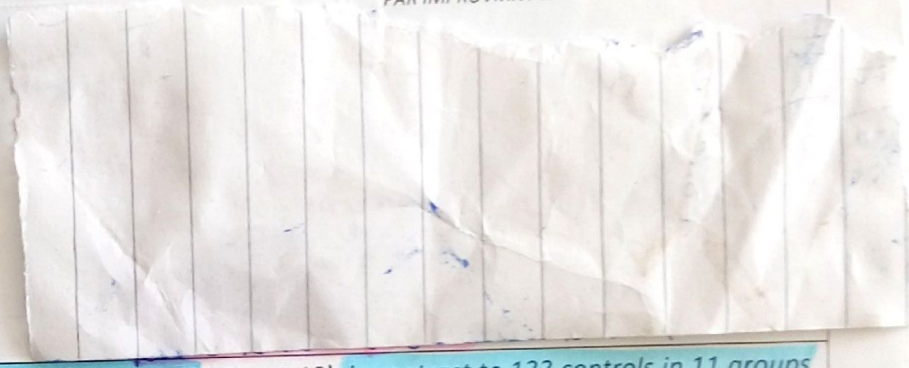
- **Structure**

In the new structure, the Processing Approach, used in ISO27001:2005 (ie the PDCA model), was eliminated. The reason for this is that the requirement is for **continual improvement** & **PDCA is just one approach** to meet that requirement. There are other approaches & organizations are now free to use them if they wish. The introduction also draws attention to the order in which requirements are presented, stating that the order does not reflect their importance or imply the order in which they are to be implemented.

- **ISO 27001:2013 has 10 short clauses, plus 1 long Annex,** which covers the following:

TELESCOP LAE ROUND ROUND DIKHA CHAND LAND PAIR SUPPORT
OPERATION PERFORM KARNA HAI KARO&CHAND
PAR IMPROVMNT KAR K AJAOO

Clause 1: Scope
Clause 2: Normative references
Clause 3: Terms & Definitions
Clause 4: Context of the organization
Clause 5: Leadership
Clause 6: Planning
Clause 7: Support
Clause 8: Operation
Clause 9: Performance evaluation
Clause 10: Improvement
Annex A: List of controls & their objectives



- ISO/IEC 27001:2013 specifies **114 controls in 14 groups (A.5 to A.18)**, in contrast to 133 controls in 11 groups in the old standard. **A brief mention about the groups & their controls** is as follows-

- **A.5**: Information **security policy** (2 controls)
- **A.6**: **Organization** of information security (7 controls)
- **A.7**: **Human** resource security (6 controls that are applied before, during, or after employment)
- **A.8**: **Asset** management (10 controls)
- **A.9**: **Access** control (14 controls)
- **A.10**: **Cryptography** (2 controls)
- **A.11**: **Physical & environmental** security (15 controls)
- **A.12**: **Operations** security (14 controls)
- **A.13**: **Communications** security (7controls)
- **A.14**: **Information systems** acquisition, development & maintenance (13 controls)
- **A.15**: Relationship with **external parties** (5 controls)
- **A.16**: Information security **incident management** (7 controls)
- **A.17**: Information security in **business continuity** management (4 controls)
- **A.18**: **Compliance** with legal & contractual requirements (8 controls)

- **Changes from the 2005 standard-**

The new standard puts more emphasis on **measuring & evaluating** how well an organization's ISMS is **performing**, & there is a new section on **outsourcing**, which reflects the fact that many organizations rely on third parties to provide some aspects of IT. It does not emphasize the PDCA cycle that 27001:2005 did. Other continuous improvement processes like Six Sigma's DMAIC method can be implemented. More attention is paid to the **organizational context of information security**, & risk assessment has changed. Overall, **27001:2013 is designed to fit better alongside other management st&ards such as ISO 9000 & ISO 20000, & it has more in common with them.**

Major changes to the standard are:

- ***Annex A** has been **revised & restructured;** there are **now 114 controls under 14 categories** rather than the previous 133 controls under 11 categories.*
- ***The Plan-Do-Check-Act Cycle (PDCA) is no longer mandated.***

Key Benefits of ISO 27001

i. **extension of the current quality system**
ii. **Identifies & manages risks** to key information and systems assets.
iii. **confidence & assurance** to trading partners & clients; acts as a marketing tool.
iv. Allows an **independent review** & assurance on **information security** practices.

A company may adopt ISO 27001 for the following **Reasons (Why):** -

- For **protecting critical & sensitive information**.
- It provides a holistic **risk-based approach to secure information** & compliance.
- Demonstrates **credibility, trust, satisfaction & confidence** with stakeholders, partners, citizens & customers.
- Demonstrates **security status** according to **internationally accepted criteria**.
- Creates a **market differentiation** due to prestige, image & external goodwill.
- If a company is certified once, it is **accepted globally**.

2. *Standard on Auditing 402 – Audit Considerations relating to an entity using Service Organisation* -

SA 402 deals with the user auditor's responsibility to obtain SAAE- when a user entity uses the services of one or more service organizations. SA 402 also deals with the aspects like obtaining an understanding of the services provided by S.O., including internal control, responding to the assessed risks of material misstatement, Type 1 & Type 2 reports, fraud, non-compliance with laws & regulation & uncorrected misstatements in relation to activities at S.O. & reporting by the user auditor, *to ensure CIA of Information at S.O.*

3. ITIL (Information Technology Infrastructure library):

CA Sukriti Jain

- ITIL is a set of practices for IT services Management (ITSM)
- It is a standard for best practice in providing IT services
- Focus on aligning IT services with needs of Biz.
- It integrates ITSM into a single lifecycle
- It describes procedures for establishing minimum level of competency.
- It gives baseline, used to demonstrate compliance & measure improvement

ITIL FRAMEWORK - ITIL Version 3 - set of 5 Volumes (books)

Service Strategy

What

origin point of the ITIL Service Lifecycle. provides guidance on the design, development & implementation of service management policies, guidelines, across ITIL Life Cycle.

IT Service Generation

ITSM is implementation & management of quality IT services & performed by IT service providers through People, Process & IT.

Business Relationship (M)

A formal approach to understand inter-biz activities related to providing & consuming services via networks. Franchise

Service Portfolio (M)

application of systematic management to investments & activities of enterprise IT departments.

Financial Management

Accurate & cost effective administration of IT assets & resources used in providing IT Services.

Demand Management

a planning methodology used to manage & forecast demand of products & services.

Service Design

How

translates strategic plans & objectives into designs & specifications & development of services & service management processes.

Service Catalogue (M)

produce Catalogue & it contains accurate details, dependencies & interfaces of all services made available to customers.

Information Security (M)

Ensure information security (CIA) & protect information assets against risks

Service Level (M)

ensure that agreed IT services are delivered when & where they are supposed to be. review levels of IT services specified in SLAs.

Availability Management:

Ensure IT service-availability to support biz at justifiable cost.

IT Service Continuity (M)

ensure that IT services can recover & continue even after a serious incident occurs.

Supplier Management

to obtain value for money from suppliers. It ensures tht contracts align with business needs, SLA & Service Level Requirements.

Capacity Management

supports optimum & cost-effective provision of IT services by matching IT resources to business demands.

Service Transition

old → New

Guidance to develop & improve capabilities for transitioning new & changed services into operations. how requirements of Service Strategy encoded in Service Design are effectively realized in Service Operation, whilst controlling risks of failure & disruption.

Sukriti Jain

Knowledge (M)

To capture, develop, share & effectively use org^{n} knowledge, achieve org^{n} objectives by making best use of knowledge

Service Asset & Configuration (M)

Sj

maintain information (i.e., configuration) abt assets (ie Configuration Items) required to deliver IT service.

Change management & Evaluation:

To ensure standardized methods & procedures are used for efficient handling of all changes, with minimum risk to IT infrastructure.

Release & Deployment

Ready to use, चालू कर दो service

used for platform-independent & automated distribution of s/w & h/w, across the entire IT infrastructure. Proper control ensures availability of licensed, tested & version-certified S/w & H/w, which functions as intended.

Service Validation & Testing:

ensure that Released & deployed services meet customer expectations & IT operations are able to support the new service.

Service Transition Planning & Support

Phase wise

Ensures orderly transition of new/modified service into production, with necessary adaptations to the service management processes.

Service Operation

system चालू होने के बाद जो problem आए उन्हें कैसे ठीक करें

रोज की prob.

4 Functions

Service Desk

handling incidents & requests & providing an interface for other ITSM processes. SPOE, SPOC

IT Operations

Documented procedures & sub process. Like – output (M), Job scheduling, backup restore

Application management

best practices to improve overall quality of IT software development & meet business objectives.

IT Technical Support

It provides a number of specialist functions, research & evaluation, technical expertise & document creation

Incident Management:

restore normal service operation quickly & minimize adverse effect on business operations, thus ensuring best levels of service quality Loss↓ Tir

Request fulfillment:

fulfil Service Requests, like - requests to change pwd. or requests for info.

Event Management:

It generates & detects notifications, indicating that something is not functioning correctly, leading to an incident being logged.

Continual Service Improvement: measure service performance, suggesting improvements, to ensure- service delivers max benefit. It combines principles, practices & methods from change management, quality management & capability improvement to achieve significant improvements in service quality, operational efficiency & biz continuity. Link improvement efforts with service strategy, design & transition

ITIL V3 → SaturDay Times of India

Sj

Strategy - अपनी generation में Relationship में रहना बहुत difficult हो गया है
भाई अपना portfolio बना कर Facebook पर डाल दे।
फिर देख Demand

Design - Court marriage - मैं Catalogue तो तब ही sign करूंगी,
जब वो मुझे Security देगा & मेरी height Level का होगा
Phone Call पर continuity मेरे ~~लिए~~ लिए Available रहेगा
& उसमें मुझे (Shopping) supplier करने की capacity होगी

Transition - पर जैसे ही मुझे पता ~~चला~~ knowledge
पुरानी वाली को छोड़ कर नई वाली पर जाओ
कि उसके पास ज्यादा Assets नहीं है
तो इसने अपना mood change किया
और उसे Divorce Release दे दिया

Old → New
Δ

Divorce paper को पढ़ा test & validate & sign कर दिया
जब हम इस stage से गुजर रहे थे Transition
तब हमारे DOAST ने हमें support किया

Opuration -

- Desk
- opurations
- Application
- Technical Support

Continual Service Improvement - बस ऐसे ही हमारी अधूरी कहानी चलती रही ....

Doast के साथ ~~के~~ Event भेजने के लिए Request किया
पर रास्ते में 1 हादसा incident हो गया।

Sukriti jain.