CH -1

Corporate Compliance Framework

- **Compliance with laws** is integral to **corporate strategy**.
- **Board of Directors**: Responsible for recognizing scope and implications of applicable laws.
- **Compliance framework**: Supports risk management, reduces non-compliance risk.

Steps for Effective Compliance:

1. **Senior management participation** in developing and maintaining a compliance program.
2. **Review compliance management system** at periodic intervals.
3. **Ensure system is updated** with changes in laws, regulations, and business environment.

- **Compliance framework** enables organizations to achieve objectives while staying compliant and mitigating risks.
- **Secretarial audit**: Periodic audit by an independent professional to ensure compliance.
- **Company Secretaries**: Act as compliance officers and Key Managerial Personnel (KMP).

Corporate Compliance Management:

- Involves **research, analysis**, **investigation**, and **evaluation** of compliance performance.
- Corporates with **effective compliance** gain **positive public image** and **customer trust**.

Compliance Management Case Studies

1. **Maruti Suzuki**:
    - Systems and controls ensure **zero non-compliance**.
    - **Compliance certificate** submitted quarterly.
    - Over **3,500 compliances** tracked, **78 health checks** conducted.
    - Annual **Compliance Month**: Focused on business integrity, new regulatory issues, and risk management.
2. **Hindustan Unilever**:
    - Committed to **complying** with all laws and regulations.
    - **Legal and regulatory teams** ensure adherence to standards.
    - **Award**: **ICSI National Award** for Corporate Governance.

Emerging Concept: Governance, Risk Management, and Compliance (GRC)

- **GRC**: Integrates **Governance, Risk**, and **Compliance** across departments.
- **Purpose**: Reduces **risks**, **costs**, and **duplication of effort**.

3 Key Elements of GRC:

1. **Governance**: System of **rules, practices**, and **standards** guiding business.
    - Executed by **Board of Directors**.
    - Ensures **accurate, timely** management information for decision-making.
2. **Risk Management**:
    - Identifies and mitigates **business risks** (e.g., financial, technological).
    - Involves **controlling, avoiding**, or **transferring risks**.
3. **Compliance**:
    - Adheres to **laws**, **regulations**, and **company policies**.
    - Ensures **ethical** and **legal** conduct.
    - Prioritizes and funds necessary corrective actions.

Case Studies on GRC Implementation:

1. **Tata Motors**:
    - Comprehensive **GRC program** covering **legal compliance**, **risk management**, and **ethics**.

    - **Risk management framework** to identify and mitigate risks.
2. **Mahindra & Mahindra**:
    - **GRC framework** covering **operations, compliance**, and **ethical practices**.
    - **Risk management committee** ensures adherence to laws and regulations.

Components of Corporate Compliance Framework

- **Growing Compliance Obligations**:
    - Anti-money laundering
    - ESG (Environmental, Social, Governance) requirements
    - Economic and trade sanctions
    - Varying regulations across jurisdictions
- **Mechanism**:
    - **Policies and procedures**
    - **Training**
    - **Whistleblowing channels**
    - **Internal audit**
    - **Escalation, response, disclosure**

---

3 Key Components of the Compliance Framework:

1. **Compliance Chart**:
    - **Overview** of local, state, central, and international laws.
    - **Risk mitigation activities** embedded in business processes.
    - **Compliance calendar** and activities for compliance risk management.
2. **Compliance Advisory**:
    - Advises on **compliance obligations** and **non-compliance consequences**.
    - **Helps evaluate**, prevent breaches, and respond quickly to violations.
3. **Compliance Scorecard**:
    - Analyzes the **compliance position** of the organization.
    - Tracks **compliance breaches**, prioritizes remediation based on **risk level**.
    - Predefined roles for **remediation** and **escalation**.

Compliance Chart Preparation:

- Based on company operations, structure, industry, and sector.
- Includes:
    1. **Identification of compliances** (laws, rules, regulations).
    2. **Risk assessment**.
    3. **Risk mitigation** (includes **training**).
    4. **Compliance monitoring** (includes **action tracking**).
    5. **Compliance reporting** (includes **incident management**).

Contents of Compliance Chart:

- **Key compliance laws, regulations**, industry standards, company policies.
- **Risk levels** (critical, high, medium, low).
- **Business processes/people** impacted by compliance obligations.
- **Risk mitigation activities**, tracking, and monitoring.
- **Ownership** of processes and activities.
- **Company Secretary** as **compliance manager**.

Key Functions of a Well-Designed Compliance Framework:

1. **Compliance Dashboard**: Tracks compliance events.
2. **Compliance Policies and Procedures**: Managing policy lifecycle.
3. **Access to Rules and Regulations**: Keeps organization updated on changes.
4. **Compliance Audit**: Facilitates internal and external audits.

5. **Quality Management**: Supports quality initiatives (e.g., ISO, Six Sigma).
6. **Compliance Training**: Employee training on compliance obligations.
7. **Compliance Task Management**: Centralized data reporting for compliance status.

Compliance Framework Stages:

1. **Identification of Compliance Obligations**:
   - Relevant **laws, rules, regulations**, and policies.
2. **Preparation of Compliance Chart**:
   - Define roles and responsibilities of **management**, **legal**, and **compliance teams**.
3. **Assessment of Historical Compliance Status**:
   - Review **reports**, **statements**, and audits.
4. **Assessment of Compliance Risk**:
   - Identify **non-compliance** risks and develop **mitigation strategies**.
5. **Compliance Reporting**:
   - Reports from **internal auditor**, **independent agencies**, **regulators** on potential **consequences** (e.g., suspension, license cancellation).

Process of Corporate Compliance Framework

1. **Compliance Identification**:
   - Identify applicable **acts** and **legislations** in consultation with **functional heads**.
   - Legal team determines **required compliances** under each legislation.
2. **Compliance Ownership**:
   - **Compliance owner**: Person responsible for compliance.
   - Ownership is **function** and **individual** specific.
   - **Primary owner**: Responsible for compliance.
   - **Secondary owner**: Supervises primary owner's compliance.

   Example: In **ABC Pvt. Ltd.**, **Mr. S (Company Secretary)** is primarily responsible for compliance.
3. **Compliance Awareness**:
   - Establish **legal compliance management**.
   - Create awareness about **legal compliances** among responsible parties.
   - Methods: **Training**, **meetings**, and **manuals** to explain compliance requirements.
4. **Compliance Reporting**:
   - **Non-compliance reporting** ensures corrective actions.
   - Reports provided **annually** by the **compliance officer**.
   - Compliance status communicated through **MIS** (Management Information System).

Compliance Management Process:

- **Maintenance**: Identifying and evaluating compliance obligations.
- **Development**: Managing non-compliance and continuous improvements.
- **Mitigation**: Reducing compliance risks.
- **Evaluation**: Performance evaluation and reporting needs.

Compliance Management in Legal Department:

- **Monitors compliance** across all entities, locations, and departments.
- Tracks **expiry dates** of contracts for renewal.
- Manages **litigation dates**, **documents**, and **orders**.
- Ensures compliance with **document policies** and processes.

Identification of Applicable Laws and Regulations

- **Compliance Requirements**: Identifying laws and regulations applicable to the organization.
  - Includes identifying and implementing **changes** in compliance with amended laws.
  - **Periodic reviews** necessary for effective compliance management.
- **Familiarity with Business Model**:
  - Understand **business model**, **environmental**, **health**, **safety**, and **data security** aspects.
  - **Compliance chart** must reflect obligations and risks from **company policies** and **laws**.
- **Key Sources for Compliance Obligations**:
  - Engagement with **management** and key staff.
  - **Laws and regulations**, **permits**, **licenses**, **regulatory orders**.
  - **Court judgments**, **treaties**, **internal policies**.
  - **Voluntary codes**, **professional group memberships**.
  - **Regulatory monitoring**: websites, meetings, media, etc.
- **Business Types**: Compliance with laws such as:
  - **Labour Laws**
  - **Fiscal/Tax Laws**
  - **Environmental Laws**
  - **Securities Laws**
  - **Commercial Laws** (IPR included)
  - **Cyber Laws** (IT Laws)
  - Industry-specific and **corporate laws**.

Case Law:

- **Siddarth Gupta v. Delhi Golf Club Ltd**:
  - Court held membership can only be cancelled after following **MOA** and **AOA** and **Natural Justice** principles.
  - **No notice** or **opportunity** was provided to the appellant.
  - Resolution reversed by the court.

Conflict Resolution:

- If **company policies** conflict with **local laws** or **international regulations**, follow the **more stringent** obligation.

Case Studies:

1. **Non-Compliance with Mandatory Standards (Pressure Cookers)**:
   - **CCPA fined Cloudtail** ₹1 Lakh for violating **Domestic Pressure Cooker (Quality Control) Order, 2020**.
   - Cloudtail also directed to **reimburse** ₹1,033 cookers and submit a **compliance report** within 45 days.
2. **Amalgamation of Companies (ATPPL & RMSPL)**:
   - NCLT **dismissed petition** for **non-compliance** with **advertisement requirements** under **Companies Act, 2013** (Sections 230 & 232).
   - **Amalgamation scheme** not sanctioned due to failure in meeting statutory requirements.

Compliance Risk Assessment: Basis for Compliance Management

- **Compliance Chart**: Oversees execution, management, control, and reporting of risk.
  - **Management's accountability**: Ultimate responsibility for risk control.
  - **Risk assessment**: Should be updated with changes in business profile (new laws, activities, social standards).
- **Risk Assessment Process**:
  1. **Identify non-compliance areas**.
  2. **Rate the risks**.

3. Assess outcomes to determine need for **training**, **monitoring**, **internal controls**, and **corrective actions**.

- **Risk Drivers**:
    0. **Legal Effect**: Penalties, fines, imprisonment, debarment, product seizure.
    1. **Financial Effect**: Low share prices, financial losses, lower investor trust.
    2. **Business Effect**: Shutdowns affecting operations.
    3. **Reputational Effect**: Loss of customer confidence, negative media impact.
- **Risk Levels**: Classify risks as **critical**, **high**, **medium**, or **low**.
    - The risk outcome determines the **mitigation strategy**.
    - **Systems** needed for tracking and monitoring risk.

Types of Risk Assessments:

1. **High-Level Risk Assessment**:
    - **Top-down process**: Facilitated by **Risk Management team**.
    - Includes **critical** and **high** compliance risks.
    - Results in a **high-level risk assessment report**.
2. **Detailed Risk Assessment**:
    - In-depth assessment with input from **support functions** or **external experts**.
    - Used for managing **critical/high risk** areas.

Case Studies: Best Practices in Risk Assessment (2022):

1. **Future Generali India Insurance**:
    - **Top-down approach** with **Risk Surveys**, **Risk Registers**, and **Scenario Analysis**.
    - **Vendor risk assessment** at onboarding and renewal.
2. **Bharti Airtel**:
    - Identified risks **mapped to senior executives' KRAs**.
3. **Hindustan Unilever**:
    - **Cross-functional risk identification** through **quantitative/qualitative assessments**.
    - **KPIs** for risk ownership and mitigation.
4. **Wipro**:
    - **ERM Framework**: Supported by **Risk & Governance Committee**.
    - Uses **'DigiQ'** to track audits and findings closure.
5. **Reliance**:
    - **Risk management process** includes identification, assessment, and mitigation of risks.

Compliance Monitoring and Responsibility Centre Mapping

- **Compliance Monitoring**: Key mechanism to ensure **framework implementation**.
    - **Dynamic business environment** requires regular updates on compliance.
    - **Continuous monitoring** is necessary for mergers, acquisitions, and changing partnerships.
- **Compliance Ownership**:
    - Described **function-wise** and **individual-wise**.
    - **Primary owner** responsible for compliance; **secondary owner** supervises.

  Example:
    - **Secretarial Officer** is the **primary** owner, while **Group Company Secretary** is **secondary**.

Management and Roles in Compliance Ownership:

1. **Top Management**:
    - Understand compliance obligations and recent changes.
    - Approve policies and motivate timely compliance.
    - Review and communicate compliance policies.
2. **Legal Cell**:
    - Resolve doubts, provide clarity, and review regulations.
3. **Senior Management & Functional Heads**:
    - Create policies, guide compliance officers, track compliance chart, and manage risks.
4. **Compliance Officer/Subordinate Staff**:
    - Perform compliance obligations, update chart, identify risks, and communicate conflicts.

- **Management's Role**:
    - Develop and update the compliance chart.
    - Identify relevant processes and individuals responsible for compliance activities.
    - **Formal approval** of the chart and communication of any changes to policies or strategy.

Escalation and Compliance Reporting

- **Purpose**:
    - Assesses if **Compliance Risks** exceed the **risk appetite** of the company.
    - Enables **timely, informed decisions** on potential compliance risks.
    - Reports discussed at **risk management committee** at least quarterly.
- **Types of Reporting**:
    1. **Cyclical Reporting**:
        - Quarterly **non-financial risk reports** by Compliance Officer.
    2. **Incident Reporting**:
        - Reports **material compliance incidents** affecting reputation, legal sanctions, or financial loss.

Case Study: ABC Limited Compliance Reporting:

- **Audit & Risk Management Committee**:
    - **Quarterly reports** on compliance performance.
    - Reports on **major non-compliance incidents**.
- **Annual Certifications**:
    - Responsible Officers certify compliance at year-end.
- **Regulatory Reporting**:
    - Compliance issues reported according to **legal requirements**.

Creation of Compliance Reporting System

- **Reporting Process**:
    1. **Functional Heads** report compliance under their areas (e.g., CFO for finance laws, HR for labor laws).
    2. Functional heads **collect, classify**, and consolidate compliance data.
    3. **Affirmation** from heads that the report is accurate.
    4. Reports forwarded to **Company Secretary** and **Managing Director** for consolidation.
    5. **Comprehensive report** presented to the **Board**.
- **Compliance MIS**:
    - Periodical reporting on **compliance status**, gaps, and incidents to the **Board** and **Senior Management**.

Effective Compliance Reporting Requirements

- **Clear and concise language**.

- Include **executive summary**.
- List **actions to be taken** and **timelines** for improving non-compliance.
- Specify **necessary actions** for management.

Compliance Risk - Review and Updation

- **Purpose**:
  - Test if **risk mitigation activities** are working and identify **new risks**.
  - Annual review and update of monitoring plan.
- **Contents of Compliance Risk Monitoring Plan**:
  1. **Critical and high risks**.
  2. **Key mitigation activities**.
  3. **Tracking & monitoring** of compliance obligations.
  4. **Compliance with laws**, **policies**, and **company values**.
  5. **Delegated obligations** (e.g., complaints, privacy).
- **Plan Methodology**:
  0. **Concise statements** of compliance obligations.
  1. Link obligations to **business processes**.
  2. **Risk mitigation** activities.
  3. **Tracking and monitoring** (1st, 2nd, and 3rd line of defense).
  4. **Tracking frequency** and **recipients** of reports.

Compliance Mechanism Methodology:

1. **Risk/Cultural Assessment**: Identify gaps in practices through **employee surveys** and **document reviews**.
2. **Program Design/Update**: Review compliance guidelines and board committees.
3. **Policies and Procedures**: Review and enhance policies (e.g., financial reporting, conflicts of interest, sexual harassment).
4. **Communication, Training, and Implementation**: **Train employees** on compliance standards, responsibilities, and consequences.
- **Ongoing Monitoring**:
  - **Self-assessments**, **internal controls**, and **audits** ensure **adherence** to regulations.
  - **Cultural assessment** ensures continuous adaptation to new regulations and business changes.

Training and Implementation

- **Importance**: Create awareness of **compliance requirements**.
  - **Training formats**: **Meetings**, **communications**, and **manuals**.
- **Key Areas in Compliance Training**:
  1. **Company framework** and integrity risk areas.
  2. Roles and responsibilities.
  3. **Critical compliance obligations**.
  4. **Process for addressing compliance issues**.
- **Five Essentials for Compliance Training Program**:
  0. **Personal**: Make training relevant to the individual.
  1. **Interesting**: Engage the audience.
  2. **Understandable**: Ensure clarity.
  3. **Accessible**: Available to all.
  4. **Ongoing**: Continuous reinforcement.
- **Training Plan**:
  - Annual **compliance training** plan, including **target audience**, **delivery method**, and **frequency**.

Compliance Audit

- **Purpose**: Independent assessment of compliance with **laws** and **regulations**.
  - **Regulatory**: Adherence to laws and agreements.
  - **Propriety**: Ethical conduct and financial management.

- **Objectives**:
    1. Verify **procurement** compliance with rules.
    2. Ensure **financial propriety** in tendering and contracts.
    3. **Plant efficiency**: Verify operational norms.
    4. Ensure **CSR activities** comply with **corporate policy** and regulations.

Benefits of Corporate Compliance Management

- **Better Compliance**: Ensures adherence to laws and regulations.
- **Real-Time Status**: Provides current overview of **legal/statutory compliances**.
- **Improved Operations**: Enhances **productivity** and operational efficiency.
- **Control Environment**: Establishes a foundation for stronger **internal controls**.
- **Litigation Tracking**: Monitors **pending litigation** status.
- **Avoid Penalties**: Prevents **personal penalties** (monetary and imprisonment).
- **Enhanced Loyalty**: Strong **ethics** and compliance lead to **employee/customer loyalty**.
- **Stronger Market Capitalization**: Positive compliance culture translates into **public respect** and **shareholder returns**.
- **Risk Mitigation**: Acts as a **safety valve** against **non-compliance** and **prosecutions**.
- **Cost Savings**: **Avoid penalties/fines** and minimize litigation costs.
- **Employee Engagement**: Improves **talent retention** and engagement.
- **Brand Image**: Enhances **company reputation** and market positioning.
- **Credibility**: Improves **credibility** and **creditworthiness** with stakeholders.
- **Goodwill**: Builds **trust** among **shareholders**, **investors**, and **regulators**.
- **Corporate Citizenship**: Recognized as a **responsible corporate citizen**.

Secretarial Audit and Compliance Management System

- **Key Factors**:
    1. **Nature of business**.
    2. **Geographical operations**.
    3. **Company size** (operations, investments, technology, manpower).
    4. **Jurisdictions**.
    5. **Listed status**.
    6. **Regulatory authority**.
    7. **Company type** (private, public, government).
- **ERP Systems**: Large companies use **ERP** to manage complex operations, integrating compliance systems.
    - **Auditing** in ERP systems requires access to evaluate compliance processes.
- **Purpose of Secretarial Audit**:
    - **Non-fault-finding**: Helps scale up compliance mechanisms.
    - **Advisory Role**: Suggests **stronger compliance systems** when identified during audits.

Role of Company Secretaries in Compliance Management

- **Compliance Manager**: Company Secretaries ensure compliance with all **regulatory provisions**.
    - Specialize in **corporate disclosures**: statutory, non-statutory, specified, and continuous.
    - **Compliance risk advisory**: Supports **management**, **Boards**, and **committees**.
    - Proactively **advises** on compliance responsibilities, obligations, and risks.

- **Key Responsibilities**:
    1. **Corporate governance**: Ensures **best practices** and **global standards**.
    2. **Disclosures**: Handles **financial disclosures**, **director remuneration**, **related party transactions**.

Directors' Responsibility Statement (Section 134(5) of the Companies Act, 2013)

- Directors must:
    1. Follow **accounting standards** and **policies**.
    2. Ensure proper **accounting records** and safeguarding of assets.
    3. Prepare accounts on a **going concern basis**.
    4. **Internal financial controls** for listed companies.
    5. **Compliance with laws** through an effective system.

Case Law: Director Breaching Fiduciary Duty (Rajeev Saumitra v. Neetu Singh)

- **Issue**: Director involved in **competing business**, breaching fiduciary duty under **Section 166 of Companies Act, 2013**.
- **Court Decision**: Director's actions conflicted with the company's interests, causing **legal action** in favor of the company.

Important Compliance Requirements under Companies Act, 2013

1. **Disclosures by Directors (Form MBP-1)**: Directors must disclose interests at the **first Board meeting** and whenever there's a change.
2. **Disqualification of Directors (Form DIR-8)**: Directors disqualified if company has not filed financial statements for 3 years or failed to repay deposits, etc.
3. **Annual Return (Form MGT-7)**: To be filed within **60 days** of AGM. Signed by a **director** and **company secretary**.
4. **Financial Statements (Form AOC-4 & AOC-4 CFS)**: Filed within **30 days** post AGM.
5. **Certification of Return (Form MGT-8)**: Required for companies with a **paid-up capital of ₹10 crores** or turnover above ₹50 crores.

Penalties and Consequences for Non-Compliance

- **Failure to Maintain Register of Members**: Penalty of ₹3 lakh for the company and ₹50,000 for officers.
- **Failure to Appoint Company Secretary**: Penalty of **₹5 lakh** for the company and **₹50,000** for directors.

Case Law: Economy Hotels India Services (Appellant) v. Registrar of Companies

- **Issue**: Typographical error in the **minutes** regarding the **special resolution** for capital reduction.
- **Court Decision**: NCLAT allowed the **capital reduction** as the company had complied with **Companies Act, 2013** despite the error.

Case Law: Registrar of Companies v. Karan Kishore Samtani

- **Issue**: Director violating **Section 165(6)** by serving as a director in more than 20 companies.
- **Court Decision**: NCLAT upheld the **minimum fine** under **Section 165** of **₹13.6 lakh** for the contravention period.

Registers to be Maintained Under Companies Act 2013

1. **PAS-5**: Record of **Private Placement Offers**.
2. **SH-2**: **Register of Renewed and Duplicate Share Certificates**.

3. **SH-3**: **Register of Sweat Equity Shares**.
4. **SH-6**: **Register of Employees Stock Options**.
5. **SH-10**: **Register of Shares/Other Securities Bought Back**.
6. **CHG-7**: **Register of Charges**.
7. **MGT-1, MGT-2**: **Register of Members** and **Debenture Holders**.
8. **MGT-1**: **Foreign Register of Members**.
9. **MGT-2**: **Foreign Register of Debenture Holders** with index.
10. **BEN-3**: **Register of Significant Beneficial Owners**.
11. **No Format**: **Attendance Register** for **Board/Committee Meetings**.
12. **No Format**: **Minutes** (General Meetings, Shareholders, Creditors, Postal Ballots).
13. **Schedule III**: **Books of Account** (including vouchers).
14. **MBP-1**: **Notice of Interest** by Directors.
15. **MBP-2**: **Register of Loans, Guarantees, Securities** and acquisitions.
16. **MBP-3**: **Register of Investments not held in its own name**.
17. **MBP-4**: **Register of Contracts/Arrangements** with related parties and bodies corporate.

Compliance Management Tool

- **Purpose**: Required in organizations handling **multiple risks** to ensure **legal, regulatory, security** compliance.
- **Software**: Automates **business processes**, minimizing risk and error in tracking compliance.
    - **Example**: **NSE's NEAPS** for online **SEBI disclosures**, **corporate governance reports**, and other filings.
- **Objectives**:
    - **Digitization**:
        1. Replaces **manual processes** with digital workflows.
        2. Increases **visibility** and **accountability**.
    - **Automation**:
        1. Provides **automated legal updates**.
        2. **Compliance tracker** with **reminders** and **escalations**.
    - **Compliances**:
        1. Ensures **adherence** to laws and regulations.
        2. Helps **avoid penalties**, **prosecutions**, and **litigation**.
        3. **Audit management** and **documentation** support.
- **Cloud Computing**: SEBI's **cloud framework** helps regulated entities adopt **secure and compliant cloud practices**.

Case Studies

1. **Bharti Airtel Limited**:
    - **Automated Compliance Framework**: Based on **global inventory** of laws.
    - **Proactive Alerts**: Sent to compliance owners to ensure timely action.
    - **Quarterly Reports**: Presented to **Audit Committee** and **Board**.
2. **BCL India**:
    - **Legal Compliance**: Tracks **changing government regulations**.
    - **End-to-End Service**: From **registration** to **filing** and **auditing**.
3. **Oracle**:
    - **Corporate Governance**: Board adopted **guidelines** and **committee charters** for

independent evaluation of business operations.

Key Benefits of Compliance Management

- **Digitization**: Replaces manual processes, reduces errors.
- **Automation**: Updates on **legal changes**, tracks compliance, sends reminders.
- **Compliances**: Ensures adherence to laws, reduces **litigation**, improves **audit management**.

Kinds of Compliance Management Tools

1. **All-Purpose Compliance Management Platforms**:
   - Suitable for any organization.
   - Focus on:
     - **Risk remedies**
     - **Solving technical issues**
     - **Corporate governance**.
2. **Industry-Specific Compliance Management Tools**:
   - Tailored to specific industries (e.g., **healthcare**, **manufacturing**, **financial**).
   - Structured to comply with industry-specific regulations and laws.
3. **GRC Software**:
   - General compliance tool focusing on:
     - **Managing risks**.
     - **Monitoring compliance risks**.
     - **Handling corporate governance**.
     - **Streamlining workflows and initiatives**.

Case Studies of Compliance Management Tools:

1. **Bharti Airtel Limited**:
   - Uses **in-house rule-based data analytics tool** and **Oracle GRC** for risk management.
2. **Reliance BP Mobility Limited**:
   - Developed **GRCA 2.0 Platform**: Real-time dashboards and risk monitoring.
   - Integrated **iRCMS**: Tracks state-wise, legislation-wise compliance, ensuring **Zero non-compliance**.

Benefits of Compliance Management Tools:

- **Reduction in Manual Work**:
  - Automates compliance tracking and reporting, eliminating tedious spreadsheet work.
- **Streamlined Implementation**:
  - Simplifies the implementation of frameworks and **compliance audits**.
- **Simplified Monitoring & Reporting**:
  - **Auto-populates compliance dates** and sends **alerts** for issues.
- **Reduced Risk of Human Errors**:
  - Automates report generation and compliance failure detection.
- **Improved Organization Reputation**:
  - Maintaining compliance boosts **reputation** with customers and employees.
- **Creates a Roadmap for Business**:
  - **Compliance calendar** helps prioritize **improvements** and **fixes** in compliance activities.

Case Study: Infosys - Project Eagle

- **Purpose**: Track, detect, prevent, and remediate violations of laws.
- **Regulatory Areas**: Includes **Global Immigration**, **Health**, **Safety**, **HR**, **Tax**, **Anti-Bribery**, **IP**, **Info Security**, etc.
- **Tools Used**: **Compliance Manager Tool** for global **regulatory compliance management**.
- **Process**:

- Collaborates with **external consultants** to keep regulations updated.
- **Functional heads** oversee and certify adherence to regulations.
- Regular reviews by the **Audit Committee** and **external auditors**.

Ch -2

Introduction to Documents and Records

- **Document**: Written, printed, or electronic matter providing information. Can be structured or unstructured.
  - Example: Emails, reports, shopping lists.
- **Record**: Evidence of the past, used as proof in legal/business matters.
  - Examples: Reports, emails confirming actions, contracts, photographs.
- **Role of Company Secretary**:
  - **Prepare and maintain records**: Ensures proper documentation and confidentiality.
  - **Ensure consistency**: Documents must align with prior records, policies, and avoid conflicts with agreements, laws, or tax implications.

Case Law: Non-Maintenance of Updated Register of Members (M/s. SDU Holdings Pvt. Ltd.)

- **Violation**: Incomplete **MGT-1** register of members.
- **Consequences**: Penalty imposed by **Registrar of Companies** for non-compliance with **Section 88** of the Companies Act, 2013.

Company Secretary's Responsibilities in Document Management

- **Storing, maintaining, and retrieving documents**: Ensures documents are stored securely and are easily accessible.
- **Overseeing subsidiary records**: May involve **local partners** in managing corporate records.
- **Execution of documents**: Guides on document creation, confidentiality, and legal compliance.

Case Law: Welspun Project Ltd. v. NCLT (2016)

- **Violation**: Incomplete **Register of Directors' Shareholding** (Section 170).
- **Consequence**: Violation compounded by **NCLT** after admission of mistake by the company.

Purpose of Documentation

1. **Client Service**: Helps professionals serve clients effectively.
2. **Communication**: Facilitates clear, accurate communication.
3. **Accountability**: Records actions for **performance management** and legal matters.
4. **Professional Responsibility**: Demonstrates professional conduct.
5. **Legal Requirement**: Mandated to maintain records per laws and standards.
6. **Quality**: Evaluates **peer reviews**, **audits**, and **regulatory inspections**.
7. **Research**: Provides valuable data for **research** and **evidence-based practice**.
8. **Resource Management**: Offers data for managing business resources.

Guiding Principles of Good Documentation

1. **Clear**: Easily understandable.
2. **Concise**: No excess information.
3. **Complete**: All necessary details included.
4. **Contemporary**: Updated and relevant.
5. **Correct**: Free from errors.

6. **Client-Centric**: Focused on client's needs.
7. **Confidential**: Protects sensitive information.
8. **Consecutive**: Logically ordered.
9. **Comprehensive**: Covers all aspects.
10. **Collaborative**: Shared between relevant parties.

Good vs. Poor Documentation Practices

- **Good Practices**:
  - **Completed at time of activity**.
  - **Legible, accurate**, and **traceable**.
  - **Retain superseded documents**.
  - **Clear examples**.
- **Poor Practices**:
  - Errors, **corrections**, not **signed** or **dated**.
  - **Write-overs** and excessive use of **white-out**.
  - Events not recorded in **sequence**.
  - **Unrecorded delegation of work**.

Scenario-Based Example

- **With Good Documentation**:
  - Regulatory authority's questions answered **quickly**, demonstrating **compliance**.
- **Without Documentation**:
  - **Inability to locate records** leads to **non-compliance** and **penalties**.

Case Law: Indiabulls Real Estate Ltd. – Non-Compliance with Secretarial Standards

- **Violation**: Failure to comply with **Section 118(10)** regarding **attendance register**.
- **Consequence**: Penalty imposed for non-compliance of **Secretarial Standards**.

Good Documentation Do's and Don'ts

- **Do's**:
  1. Record data **immediately** after generation.
  2. **Add reference notes** for context.
  3. Keep **data backup** securely.
  4. Limit access to **authorized personnel**.
- **Don'ts**:
  1. **Delay** recording data.
  2. **Falsify** records.
  3. **Pre-date** or **back-date** documents.
  4. **Archive** documents without authorization.

Electronic Repository of Documents

- **Document Management Systems (DMS)**: Software used to store, manage, and track electronic documents.
  - **Cloud document management** allows access from any location and ensures **secure** storage and **audit trails**.

Case Study: Health Care Provider Moves to Electronic Records

- **Challenge**: Standardize records management across multiple locations.
- **Solution**: **Electronic Record Keeping Service** standardized and implemented electronic records, converting **500,000 records**.
- **Advantages**: Improved **data integrity** and **efficiency**.

Advantages of DMS (Document Management System)

1. **Cost-effective**: Reduces physical storage costs.
2. **Ease of Use**: **Searchable**, easily shareable documents.
3. **Labor Savings**: Reduces manual processes.
4. **Searchability**: **OCR** technology makes documents keyword-searchable.

5. **Portability**: Easy to transport documents digitally.
6. **Version Tracking**: Tracks changes to documents, making edits traceable.

Disadvantages of Electronic Records

1. **Software Risk**: Risks of **unsupported systems** or **vendor issues**.
2. **Format Risk**: Changing or obsolete **file formats** may lead to inaccessibility.
3. **Reliability**: Unlike paper, digital systems are vulnerable to **data loss** or **cyber theft**.
4. **Portability**: Easy to **misplace** or **corrupt** electronic data without proper safeguards.

Case Law: Admissibility of Electronic Evidence (Arjun Panditrao Khotkar vs. Kailash Kushanrao Gorantayal)

- **Issue**: Interpretation of **Section 65B of the Indian Evidence Act** regarding the admissibility of **electronic evidence**.
- **Court Decision**: **Electronic evidence** is admissible if authentic, with appropriate certification.

Maintenance and Inspection of Documents in Electronic Form under Companies Act, 2013

Section 120 & Rules 27 & 28 of the **Companies Act, 2013**:

- Documents, records, registers, minutes, etc., can be maintained in **electronic form**.
- **Rule 27**: Companies with **1,000+ shareholders, debenture holders, or security holders** may maintain records electronically.
- **Section 2(36)**: "Document" includes summons, notices, forms, registers, etc., whether paper or electronic.

Key Requirements for Electronic Document Maintenance:

1. **Consistency**: Maintain in accordance with Act and rules.
2. **Readability**: Must be retrievable, reproducible, and readable.
3. **Digital Signature**: Must be digitally signed where required.
4. **Security**: Records must be non-editable after signing and should be **updateable** with timestamp.

Security of Records Maintained in Electronic Form - Rule 28

1. **Responsibility**: Managing Director or Company Secretary is accountable for **security of electronic records**.
2. **Protection**:
    - Against unauthorized access, alteration, or tampering.
    - Ensure **backup** and **availability**.
    - Ensure records are **non-rewriteable** and **non-erasable** (e.g., **PDF** format).
3. **Backup**:
    - Periodic **daily backup**.
    - Secure storage with proper **authentication**.
4. **Access Control**: Restricted to authorized personnel.

Case Laws

1. **Michelin India Pvt. Ltd. (2022)**:
    - **Violation**: Failure to maintain proper internal financial controls and **backups** of books of accounts in electronic form.
    - **Penalty**: Imposed for non-compliance with **Section 134(3)(f)**.
2. **Anil Kumar Poddar v. Bonanza Industries Ltd.**:
    - **Issue**: Shareholder's right to inspect statutory records.
    - **Court Decision**: **Dismissed** the application, emphasizing the availability of records on the **MCA portal**.

Physical vs. Virtual Data Room

Particulars	Physical Data Room	Virtual Data Room
Documents	Paper-based	Digital (PDF, audio, video)
Security	Integrity relies on the in-charge person	More secure (login, password, firewalls)
Creation Time	Long	Created within 48 hours
Cost	High (travel, personnel)	Low (online access)
Convenience	Time-consuming document search	Easier with search facility
Access Timing	Restricted	Accessible anytime
Document Restriction	Difficult	Easy to implement
Document Tracking	Not available	Available (log and stats)
Document Copying	Possible	Not always allowed
Communication	One-to-one	Not available

Good Documentation Practices

1. **Do's**:
   - **Record immediately** after activity.
   - **Reference notes** for context.
   - **Keep data backup** securely.
   - **Limit access** to authorized personnel.
2. **Don'ts**:
   - **Delay** recording data.
   - **Falsify** records.
   - **Pre-date** or **back-date** documents.
   - **Archive** without authorization.

Coding and Nomenclature for Documents

1. **File Naming Guidelines**:
   - **Be unique** and **consistent**.
   - **Limit character length** to **25**.
   - **Avoid spaces**, use underscores (_) or hyphens (-).
   - Use **leading zeros** for **numerical sorting** (e.g., `001`, `002`).
   - **Use file extensions** (e.g., `.pdf`, `.docx`).
2. **File Naming Do's and Don'ts**:
   - **Do**: Keep file names **concise** and **descriptive**.
   - **Don't**: Use **complex structures** or **spaces**.

Best Practices for Document Management

- **Do's**:
  - **Include sufficient elements** for **easy retrieval**.
  - Use **underscore** for delimiting elements.
  - Ensure **files** are **completed at time of activity**.
- **Don'ts**:
  - **Avoid long folder names**.
  - **Don't use spaces**; use hyphens or underscores.
  - **Avoid overly complex naming schemes**.

File Naming Rules Summary:

Rule	Do's	Don'ts
1. Naming Structure	Keep concise, avoid long paths	Complex hierarchical folder structures
2. Element Quantity	Sufficient for precise identification	Overloading file name
3. Delimiters	Use **underscore** or **hyphen**	Use spaces or special characters
4. Date/Time Format	Follow **YYYYMMDD** and **HHMMSS**	Use incorrect date formatting
5. Names in	Start with	Reverse order

Rule	Do's	Don'ts
Proper Order	**general** to **specific**	
6. Version Control	Use **V01** for versions	Use words like **Final**, **Draft**
7. Personal Names	Family name first	First name first

Case Law on Electronic Evidence

1. **Arjun Panditrao Khotkar vs. Kailash Kushanrao Gorantayal** (2017):
   - **Issue**: Admissibility of **electronic evidence** under **Section 65B** of the **Indian Evidence Act**.
   - **Ruling**: **Electronic evidence** admissible if authentic, **certification** required under **Section 65B(4)**.

Circulation of Documents

- **Document Control**: Ensure documents (instructions, procedures, drawings, etc.) are **reviewed**, **approved**, and **distributed** appropriately.
- **Document Changes**: Changes should be reviewed and approved by the same authority unless otherwise designated.
- **Key Measures**: Documents should be:
  - Reviewed for **adequacy** before release.
  - Distributed and used at the location where the activity occurs.

Safety and Retrieval of Records

- **Record Maintenance**: Essential to maintain sufficient records for evidence of activities affecting quality.
- **Key Elements**:
  - **Operating Logs**: Track individuals working on documents.
  - **Review Results**: Record changes suggested by reviewers.
  - **Inspections**: List individuals with access to records.
  - **Work Performance Monitoring**: Helps in monitoring activities.
  - **Information Analysis**: For effective tracking of files.
- **Regulatory Compliance**: Ensure records are identifiable and retrievable in line with applicable regulations.

Record Life Cycle Management

1. **Keeping Together**:
   - Records should be maintained in their **original order**, by the department responsible for creation.
   - This helps in **retrieval** and ensures **evidential nature**.
2. **Ensure Life Cycle**:
   - **Current Phase**: Regularly used in business.
   - **Semi-Current Phase**: Infrequent use, stored in a records center.
   - **Non-Current Phase**: Destroyed unless they have **archival value**.
3. **Record Preservation**:
   - **Ongoing Care**: From creation to preservation in archives.
   - **Key Actions**: Identification, intellectual control, access provision, and physical control.

Case Study: FDA Warning Letters

- **Ranbaxy Laboratories**:
  - **Violation**: Failed to maintain batch production and control records at Dewas and Poanta Sahib facilities.
- **Canton Laboratories**:
  - **Violation**: Reported test results that were never performed.
- **Wockhardt Limited**:
  - **Violation**: Failed to control changes in production records at

Aurangabad plant, leading to data integrity issues.

Preservation of Records - SEBI (LODR) Regulations, 2015

- **Regulation 9**:
  - Listed entities must have a **policy for preservation of documents**:
    - Permanent preservation for some documents.
    - Minimum **eight years** for other documents post-transaction completion.
- **Regulation 30(8)**:
  - Disclosures made to stock exchanges must be hosted on the company's website for at least **five years**.
- **Archival Policy**:
  - Companies must develop a policy for document preservation, covering:
    - Classification, retention, and destruction of documents.
    - Periodical reviews and employee responsibility.

Preservation of Litigation Documents

- **Retention**: Documents related to litigation must be preserved for **eight years** after conclusion unless specified by the court or authority.
- **Deviation**: Court orders may override company policies on document destruction or preservation.

Model Policy for Preservation of Documents

1. **Classification**:
   - **Permanent**: Property records, corporate records, etc.
   - **Eight Years**: Books of account, filings, payroll records, etc.
   - **Three Years**: Tender documents, legal files, insurance records, etc.
2. **Employee Responsibility**:
   - Employees are responsible for the preservation of documents in their work areas.
3. **Periodical Review**:
   - The **CEO/Managing Director** is responsible for reviewing and updating the policy.
4. **Suspension of Disposal**:
   - If involved in litigation or audit, **disposal of documents** is suspended until resolved.

Advantages of Preserving Records

- **Effective Organization**: Helps in organized and efficient **retrieval** of records.
- **Compliance**: Ensures adherence to legal and regulatory **requirements**.
- **Security**: Protects records against **tampering** and **unauthorized access**.

Best Practices for Record Preservation

- **Backup**: Periodic backups of **digital records** with authentication and proper storage.
- **Access Control**: Limit access to authorized personnel only.
- **Reproducibility**: Ensure records can be retrieved in **readable** and **printable form**.

Physical vs Virtual Data Rooms

Particulars	Physical Data Room	Virtual Data Room
Form of Documents	Paper, files, boxes	Digital files (PDF, audio, video)
Security	Relies on in-charge person	Secured with login, passwords, firewalls
Time to Create	Longer time	Created in 48 hours

Particulars	Physical Data Room	Virtual Data Room
Cost	High (travel, personnel)	Low (online access)
Convenience	Time-consuming document search	Easier with search facility
Accessibility	Restricted timing	Accessible anytime

File Naming and Document Management

- **Best Practices**:
  - **Keep filenames unique** and concise.
  - **Avoid spaces**; use underscores (_) or hyphens (-).
  - **Use date formats** (YYYYMMDD) and version control (`V01` for versions).

Case Law on Electronic Records

- **Arjun Panditrao Khotkar vs. Kailash Kushanrao Gorantayal (2017)**:
  - **Issue**: Admissibility of **electronic evidence** under **Section 65B** of the **Indian Evidence Act**.
  - **Ruling**: **Electronic evidence** admissible if authentic, with proper **certification** under **Section 65B(4)**.

Setting Up a Record Room

- **Location**: Choose a secure, dedicated space separate from other administrative units.
- **Size**: Ensure the room is large enough to store all relevant documents.
- **Environment**: Keep the room clean and controlled with respect to:
  - **Humidity**: Maintain 30%-40% humidity to prevent fungus or brittleness.
  - **Temperature**: Opt for normal temperature, comfortable for human activity.
  - **Light**: Use UV filters for windows and store documents in dark places when not in use.
- **Security**: Ensure the room has **fire extinguishers**, appropriate paint, and regular security checks.
- **Regulatory Compliance**: Follow the **Public Records Act, 1993** for proper management and preservation of public records.

Privacy of Records and Its Control

- **Confidential Documents**: These include:
  1. **Customer & Employee Information**: Personal data like Aadhar numbers, addresses, credit card info.
  2. **Internal Office Plans and Procedures**: Sensitive internal layouts and procedure manuals.
  3. **Contracts, Commercial Documents, and Trade Secrets**: Sensitive agreements, proprietary business information, etc.
- **Data Protection**: Implement secure practices for managing and sharing confidential documents:
  - Store confidential data in **locked cabinets**.
  - Protect electronic data using **firewalls, encryption, and passwords**.
  - Ensure proper **disposal** of sensitive documents (e.g., shredding physical copies).

Steps to Protect Confidential Information

1. **Physical Security**:
   - **Lock files** containing confidential information.
   - **Clear desks** of confidential information after work hours.

    - **Label documents** as "confidential."
2. **Digital Security**:
    - Use **passwords, encryption, and firewalls** to protect electronic data.
    - **Shred or wipe** old data from computers and storage devices before disposal.
3. **Employee Awareness**:
    - **Discuss confidential information** in private settings, not public areas.
    - **Avoid e-mail** for sensitive or controversial information.
    - Limit the **acquisition** of sensitive client data to what's absolutely necessary.
4. **Document Disposal**:
    - **Shred documents** before disposal.
    - **Use software** to securely wipe data from electronic devices before disposal.

Case Study: FDA Warning Letters on Data Integrity

- **Ranbaxy Laboratories**: Received a warning letter for failing to maintain **batch production** and **control records** at two facilities.
- **Canton Laboratories**: Violated **GMP** standards by reporting unperformed tests.
- **Wockhardt Limited**: Failed to ensure **data integrity** at its plant, leading to issues with the **master production records**.

Preservation of Records

1. **Preservation Strategies**:
    - **Physical & Electronic Records**: Categorize and preserve documents based on their nature and legal requirements.
    - **Backup & Security**: Regularly back up records and ensure access control.
2. **Regulatory Requirements**:
    - Follow **SEBI (LODR) Regulations, 2015** for document preservation:
        - **Permanent** preservation for some documents.
        - **Eight years** retention for other documents post-transaction.
3. **Litigation-Related Documents**: Keep documents related to legal matters for **eight years** after case resolution.

Model Policy on Preservation of Documents

1. **Document Classification**:
    - **Permanent**: Corporate records, property deeds, etc.
    - **Eight Years**: Books of account, employee records, etc.
    - **Three Years**: Legal files, tenders, contracts, etc.
2. **Employee Responsibility**:
    - Employees must understand their role in preserving and properly disposing of documents.
3. **Suspension of Disposal**:
    - If the company faces **litigation** or a **regulatory audit**, suspend disposal of related documents.

Archival Policy

1. **Disclosure**:
    - Ensure **disclosures** to the stock exchange are hosted on the company's website for at least **five years**.
2. **Document Preservation**:
    - Implement a **policy** for systematic identification, retention, and destruction of documents as per business needs.

Advantages of Proper Document Management

1. **Improved Efficiency**: Reduces errors, improves accessibility.
2. **Legal Compliance**: Ensures the company adheres to relevant regulations.
3. **Security**: Protects sensitive and proprietary data from unauthorized access.

Note: Ensure compliance with SEBI and other regulatory frameworks, implement document management systems, and establish clear policies for handling, storing, and disposing of both physical and electronic records.

Ch-3

Pre-Certification and Authentication of E-Forms under the Companies Act, 2013

Introduction

- **E-Forms Authentication**: The Companies Act, 2013 mandates that e-forms filed by companies must be authenticated by authorized signatories, including directors or the Company Secretary, using **digital signatures**. Practicing professionals, such as Company Secretaries, are responsible for certifying the compliance and accuracy of these documents.
- **Responsibility**: The authorized signatories and certifying professionals are responsible for ensuring that the e-forms comply with the provisions of the Companies Act, 2013, and the rules made thereunder. They must verify that all required attachments are complete and legible.
- **Penalties**: False certification or omission of material information in the forms by a professional can lead to punishment under the Companies Act, 2013 and disciplinary action from the Institute of Company Secretaries of India (ICSI).

Pre-Certification Process

- **What is Pre-Certification?**: Pre-certification involves a professional, typically a Company Secretary, certifying the correctness of documents before they are filed with the Registrar. The professional ensures that the contents of the forms align with the company's records.
- **Purpose of Pre-Certification**: Introduced to avoid delays in document registration and ensure that the forms are correct, complete, and compliant with the law. This process reduces the need for further examination by the Registrar and helps in self-regulation by companies.

Certification of Documents

- **What is Certification?**: Certification refers to the process of confirming the authenticity of documents by a qualified professional. In India, certifications are required for documents filed with various regulatory bodies.
- **Pre-Certification by Company Secretaries**: This includes verifying e-forms and ensuring they are correct, based on the company's records. The Company Secretary issues a declaration confirming that the form and its attachments are complete and accurate.
- **Declaration for Pre-Certification**: The certifying professional signs a declaration, confirming that:
    - The records are prepared and maintained in accordance with the Companies Act.
    - The attachments are complete and legible.
    - The professional takes responsibility for any incorrect certification.

📚 GET COMPLETE NOTES – ₹300 PER SUBJECT

✔ Covers all subjects except for cr portion in crvi
✔ Made from 6 coaching notes + module, refined with AI
✔ Crisp, exam-focused & easy to revise

For more free notes join telegram channel - **https://t.me/csprofessionalnote**

👉 To purchase:

1. Pay ₹300 via UPI (**9024770603-2@ibl**)
2. Fill this form with payment proof:
   https://forms.gle/u4k3XxEy8nCJiXVs9

📩 Notes will be delivered to your WhatsApp within 12 hours.