Chapter 4

Topics

- Cybersecurity and Contracting
  - Cybersecurity clauses in third-party contracts, vendor-customer contracts (e.g. General Data Protection Regulation (GDPR) compliance) Contract review and negotiations
- Cybersecurity Policies and Compliance
  - Developing cybersecurity policies
  - Compliance frameworks (e.g.. GDPR, HIPAA)
  - Reporting requirements for different industries
  - Role of compliance in incident response

Type Of Vendors

- Providing General Services (Non-Data Processing)
- Providing On-Premises Software
- Developing an Application/Device
- Providing Cloud Service (SaaS, PaaS, IaaS)
- Acting as a Data Processor

Providing General Services (Non-Data Processing)

Key Considerations

- Limited Data Access: Evaluate whether the vendor's access to sensitive information is restricted or entirely eliminated.
- Physical/Network Security: Verify the implementation of robust security measures if the vendor has on-site presence or access.
- Confidentiality Agreements: Require non-disclosure agreements (NDAs) to safeguard sensitive business data.

Key Clauses to Include

- Confidentiality and Non-Disclosure
- Security Awareness Training for Vendor Staff
- Incident Reporting Obligations
- Background Checks for Vendor Personnel

Providing On-Premises Software

Key Considerations

- Software Security Updates: Require timely application of patches and proactive vulnerability management to maintain security.
- License and Usage Restrictions: Clearly outline acceptable usage terms and ensure compliance with licensing agreements.
- Access Control and Audit: Define access permissions and establish monitoring mechanisms to oversee software usage.

Key Clauses to Include

- Software Update and Patch Management
- Licensing Terms and Compliance
- Vulnerability Remediation Timelines
- Audit Rights for Security and Compliance
- End-of-Life and Decommissioning Procedures

Developing an Application/Device

Key Considerations

- Intellectual Property (IP): Define ownership of the code, design, and associated IP.
- Secure Development Practices: Require adherence to secure coding standards (OWASP, NIST).
- Testing and Vulnerability Management: Mandate penetration testing and vulnerability assessments.
- Data Security by Design: Ensure security is embedded in the application/device architecture.
- Source Code Escrow: Consider a source code escrow clause to secure future access.

Key Clauses to Include

- Security and Privacy by Design
- IP Ownership and License Rights
- Vulnerability Management and Patching Timelines
- Audit and Review Rights
- Incident Response Requirements

Providing Cloud Service (SaaS, PaaS, IaaS)

Key Considerations

- Shared Responsibility Model: Clearly outline the division of security duties between the vendor and the customer to avoid ambiguity.
- Data Encryption: Mandate robust encryption protocols for both data in-transit and at-rest, ensuring confidentiality and integrity.
- Data Residency and Sovereignty: Comply with regulations regarding the geographic location of data storage and its legal implications.
- Service Availability and Disaster Recovery: Include SLAs specifying uptime guarantees, backup schedules, and efficient recovery processes.
- Audit and Compliance Reports: Require certifications like SOC 2 or ISO 27001 to verify adherence to industry security standards.

Key Clauses to Include

- Data Encryption and Access Controls
- Service Level Agreements (SLAs)
- Security Certifications and Audit Rights
- Incident Response and Breach Notification
- Data Retention and Deletion Policies

Acting as a Data Processor

Key Considerations

- Regulatory Compliance: Confirm adherence to relevant data protection regulations, such as DPDP, GDPR and CCPA.
- Processor Obligations: Ensure inclusion of GDPR Article 28 clauses, as vendors act as processors handling data for the controller.
- Sub processor Restrictions: Limit vendor use of sub processors and require formal approval prior to engagement.
- Data Breach Notification: Set clear deadlines for reporting data breaches to ensure swift response and mitigation.

Key Clauses to Include

- Obligations of Data Fiduciaries
- Data Processing Agreement (DPA)
- Sub processor Management and Approval
- Security Controls and Encryption
- Data Retention and Deletion
- Breach Notification and Incident Response

Over all Compare

Vendor Type	Data Sensitivity	Primary Security Concerns	Common Regulations
General Service Provider	Moderate	Confidentiality, Access Control	NDAs, Internal Policies
On-Prem Software Provider	Moderate-High	Patch Management, Licensing Compliance	ISO, PCI-DSS
App/Device Developer	High	Secure Development, IP Protection	ISO, OWASP, NIST
Cloud Service Provider (SaaS, PaaS, IaaS)	High	Data Security, Shared Responsibility Model	ISO, SOC 2, GDPR
Data Processor (GDPR/CCPA)	High	Data Processing, Sub processor Control	GDPR, CCPA

Cybersecurity in Contracts

- Why Cybersecurity Clauses Matter
  - Rising cyber threats in supply chains
- Few Types of Contracts Involving Cybersecurity
  - Vendor-customer contracts
  - Service-level agreements (SLAs)
  - Cloud service agreements (CSA)
- Key Regulatory Frameworks
  - DPDP: Focus on Data Fiduciaries
  - RBI : Cyber Security Framework
  - GDPR: Focus on Data Processing Agreements (DPAs)

Key Cybersecurity Clauses in Contracts

- Data Protection and Privacy Obligations
  - Data ownership, processing, and storage requirements
  - Cross-border data transfers
- Incident Response and Notification
  - Timelines for breach notification
  - Vendor responsibilities in case of an incident
- Security Controls and Standards
  - Compliance with industry standards (ISO 27001, NIST, CIS)
  - Requirement for penetration testing and audits

Key Cybersecurity Clauses in Contracts

- Subcontracting and Vendor Management
  - Ensuring subcontractors adhere to security standards
  - Chain of accountability
- Right to Audit and Compliance Monitoring
  - Frequency of audits and compliance checks
  - Remediation timelines and penalties

Contract Types

- Master Service Agreement (MSA)
  - Defines the overarching relationship between the organization and vendor, establishing broad terms that apply to various agreements.
- Data Processing Agreement (DPA)
  - Adherence to data protection laws (like GDPR, CCPA) when vendors handle personal data for the organization, acting as its controller.
- Service Level Agreement (SLA)
  - Establishes clear performance metrics, security requirements, and consequences for not meeting the agreed service levels.

Contract Types

- Software Licensing Agreement
  - Specifies the conditions for vendor software licensing to the customer, outlining both usage terms and security obligations.
- Cloud Service Agreement (CSA)
  - Defines the conditions for accessing a vendor's cloud services (like SaaS, PaaS, IaaS) while outlining shared security roles.
- Non-Disclosure Agreement (NDA)
  - Safeguards confidential information by requiring both parties to uphold the secrecy of proprietary data exchanged during the partnership.

Contract Types

- Penetration Testing Agreement
  - Outlines the scope, conditions, and protective measures for performing penetration tests, vulnerability scans, and security evaluations.
- Managed Security Services Agreement (MSSA)
  - Defines the duties of an MSSP in overseeing security operations, identifying threats, and taking action to address security incidents.
- Third-Party Risk Agreement
  - Sets clear security and compliance standards for third-party vendors with access to organizational systems or data.
- Incident Response Agreement
  - Specifies roles, duties, and timelines for addressing and reporting security incidents or data breaches effectively.

Contract Review and Negotiation Basics

- Understanding Risk Allocation
  - Limitation of liability clauses
  - Indemnification and insurance coverage
- Negotiating Security Requirements
  - Minimum acceptable security controls
  - Continuous compliance verification
- Handling Breach Notification Timelines
  - Establishing realistic timelines for reporting incidents
- Termination and Exit Clauses
  - Data return, deletion, or transfer upon contract termination

Cybersecurity in Contracts

DPDP COMPLIANCE IN CONTRACTS

DPDP Compliance in Contracts

- Overview of DPDP Act, 2023 (India)
  - **Objective:** To regulate the processing of personal data in India while safeguarding the privacy of individuals.
- Applicability:
  - Applies to processing personal data collected online or offline in India.
  - Also applies to foreign entities processing data related to Indian individuals.

Key Clauses to Include in Contracts Under DPDP

- Lawful Processing and Consent
  - Explicit, informed, and revocable consent
  - Validity of consent obtained under contracts
  - Handling sensitive personal data with additional safeguards
- Data Processing Obligations
  - Purpose limitation: Process data only for the intended purpose.
  - Storage limitation: Define data retention and deletion timelines.
  - Data minimization: Collect and process only necessary data.
- Cross-Border Data Transfers
  - Government-approved jurisdictions for data transfers
  - Safeguards through contractual clauses and agreements

Key Clauses to Include in Contracts Under DPDP

- Data Principal Rights (Similar to GDPR Data Subject Rights)
  - Right to access, correction, erasure, and grievance redressal
  - Clause specifying timelines for honoring these rights
- Data Breach Notification
  - Mandatory reporting to the Data Protection Board of India (DPB)
  - Timelines for notifying data principals and authorities
- Obligations of Data Fiduciaries and Processors
  - Compliance with security safeguards and regular audits
  - Vendor liability and accountability for subcontractors

Some real-world examples

- IT and Cloud Services Agreements (DPDP-Compliant Contracts)
- **Service Provider:** Infosys or TCS providing cloud services to Indian banks.
- **Purpose:** To process customer and financial data for hosting and managing cloud infrastructure.
- DPDP Clauses Included:
  - Explicit obligations of the service provider as a **Data Processor**.
  - Cross-border data transfer restrictions.
  - Breach notification timelines
  - Subprocessor approvals and liability clauses.

Some real-world examples

- E-Commerce Platform Vendor Contracts
- **Service Provider:** Flipkart/Amazon India contracting with third-party vendors.
- **Purpose:** To process customer purchase data, address information, and payment details.
- DPDP Clauses Included:
  - Vendor compliance with data protection and security standards.
  - Data retention policies aligned with DPDP timelines.
  - Grievance redressal and customer complaint mechanisms.

Some real-world examples

- Healthcare Data Processing Agreements
- **Service Provider:** Practo or 1mg contracting with diagnostic labs and telemedicine platforms.
- **Purpose:** To process sensitive health data of patients for diagnostic and consultation services.
- DPDP Clauses Included:
  - Safeguards for processing **sensitive personal data**.
  - Data fiduciary and processor obligations.
  - Mandatory breach notifications and audit rights.
  - Rights to erasure and correction of data as per DPDP requirements.

Some real-world examples

- Banking and Financial Services Contracts (Data Outsourcing Agreements)
- **Service Provider:** ICICI Bank or HDFC outsourcing payment processing to Razorpay or PayU.
- **Purpose:** To process customer transaction data, KYC information, and credit card details.
- DPDP Clauses Included:
  - Cross-border data transfer clauses with jurisdictional approvals.
  - Processor obligations to follow security controls.
  - Right to audit and verify compliance.
  - Deletion of personal data after contract termination.

Some real-world examples

- BPO/IT-Enabled Services (ITES) Contracts
- **Service Provider:** Genpact or Wipro managing customer service and KYC processes for telecom or insurance companies.
- **Purpose:** To process customer queries, complaints, and sensitive information.
- **DPDP Clauses Included:**
  - Restriction on using data for unauthorized purposes.
  - Data breach reporting to Data Fiduciaries.
  - Customer grievance redressal assistance.
  - Return or deletion of data upon contract completion.

Some real-world examples

- SaaS and Application Development Agreements
- **Service Provider:** Zoho or Freshworks developing CRM software for Indian businesses.
- **Purpose:** To process customer interaction data, user behavior, and business insights.
- DPDP Clauses Included:
  - Customer rights to access and delete data.
  - Audit rights to ensure compliance with DPDP.
  - Limitation of liability for data breaches.
  - Mandatory employee training on DPDP compliance.

Some real-world examples

- Social Media and Digital Marketing Contracts
- **Service Provider:** Facebook/Instagram India providing targeted marketing for Indian businesses.
- **Purpose:** To process behavioral data for targeted advertisements.
- DPDP Clauses Included:
  - Lawful processing and consent requirements.
  - Explicit clauses on withdrawal of consent.
  - Grievance redressal mechanisms and penalties for violations.

Key DPDP Clauses

- Explicit Consent and Purpose Limitation
- Cross-Border Data Transfer Restrictions
- Data Breach Notification and Liability
- Right to Erasure and Correction
- Grievance Redressal Mechanisms

DPDP Compliance in Contracts

GDPR COMPLIANCE IN CONTRACTS

GDPR Compliance in Contracts

- Ensure personal data transfer, processing, and protection align with GDPR by including required clauses in agreements between data controllers, processors, and third parties.
- Understand the importance of GDPR compliance in contracts.
- Identify key clauses required in contracts involving personal data.
- Ensure that data protection obligations are appropriately allocated between parties.

Key Roles Defined in GDPR

- **Data Controller:** Decides why and how personal data is processed. Ensures GDPR compliance.
- **Data Processor:** Processes data for the controller as per agreed terms, ensuring lawful handling.
- **Data Subject:** The individual whose data is processed, with rights like access, correction, and deletion.

GDPR Requirements in Contracts

- **Data Processing Agreement (DPA):** A contract between the controller and processor ensuring GDPR compliance.
- **Purpose of Processing:** Define purpose, nature, and duration.
- **Types of Data:** Detail data categories and subjects.
- **Confidentiality:** Ensure confidentiality by employees and subcontractors.
- **Sub-processing:** Restrict or authorize subcontracting.

GDPR Requirements in Contracts

- **Data Subject Rights:** Support rights like access, correction, and erasure.
- **Security Measures:** Implement safeguards to protect data.
- **Breach Notification:** Notify controller promptly of data breaches.
- **Audit Rights:** Permit compliance audits/inspections.
- **Data Return/Deletion:** Delete or return data after processing ends.

Clauses for Controller-to-Processor Contracts

- **Article 28 GDPR Obligations:**
- **Data Processing:** Only act on documented instructions from the controller.
- **Security Measures:** Apply safeguards under Article 32 for secure data handling.
- **Compliance Assistance:** Support controllers in meeting GDPR requirements.
- **Data Return/Deletion:** Delete or return personal data once services conclude.

International Data Transfers

- **Data Transfers Outside the EEA:**
- **Standard Contractual Clauses (SCCs):** Incorporate EU-approved SCCs in agreements to legitimize data transfers.
- **Additional Safeguards:** Use measures like encryption or pseudonymization if needed for added protection.
- **GDPR Chapter V Compliance:** Ensure all transfers align with the rules set out in Chapter V of the GDPR.

Additional Important Clauses

- **GDPR Contractual Essentials:**
- **Liability & Indemnity:** Establish clear terms for accountability in case of GDPR non-compliance and specify indemnification for breaches.
- **Data Retention & Deletion:** Define retention timelines and processes for secure deletion of personal data.
- **Audit & Compliance Checks:** Grant controllers the right to conduct audits ensuring processor adherence to GDPR obligations.

GDPR Compliance in Contracts

DEVELOPING CYBERSECURITY POLICIES

Developing cybersecurity policies

- Introduction, Scope, and Objectives
  - Introduction
  - Scope
  - Objectives
    - Protect Confidentiality, Integrity, and Availability (CIA)
    - Regulatory Compliance
    - Risk Mitigation
    - Incident Preparedness and Response
    - Security Awareness and Accountability

Developing cybersecurity policies

- Governance and Risk Management
    - Governance Framework
        - Board Oversight
        - Security Steering Committee
        - Cybersecurity Leadership
    - Risk Management
        - Risk Assessment Methodology
        - Risk Treatment Plans
        - Third-Party Risk Management
    - Policy Review and Updates

Developing cybersecurity policies

- Compliance and Legal Frameworks
  - Applicable Regulations and Standards
    - General Data Protection Regulation (GDPR)
    - Health Insurance Portability and Accountability Act (HIPAA)
    - Payment Card Industry Data Security Standard (PCI-DSS)
    - ISO/IEC 27001
  - Compliance Audits and Reporting

Developing cybersecurity policies

- Access Control and Data Security
  - Identity and Access Management
    - Role-Based Access Control (RBAC):
    - Privileged Access Management (PAM):
    - Multi-Factor Authentication (MFA)
  - Data Classification and Encryption
    - Data Classification Levels
    - Encryption Standards:
  - Endpoint Security

Developing cybersecurity policies

- Incident Response and Reporting
  - Incident Response Plan
    - Incident Identification and Classification
    - Containment and Mitigation
    - Eradication and Recovery
  - Compliance in Incident Reporting
    - GDPR
    - DPDP
    - HIPAA
    - PCI-DSS
  - Post-Incident Review

Developing cybersecurity policies

COMPLIANCE FRAMEWORKS

Digital Personal Data Protection (DPDP) Act, 2023

- **Region:** India
- **Focus:** Protection of personal data and ensuring digital privacy
- **Key Principles of Data Processing:**
  - **Consent**: Explicit consent required before handling personal data.
  - **User Rights**: Access, correction, and deletion of personal data guaranteed.
  - **Purpose**: Data collection limited to specific, lawful objectives.
  - **Retention**: Data must be deleted after fulfilling its purpose.
  - **Cross-Border Transfer**: Allowed to approved countries only.
  - **Complaints**: Organizations must address user grievances effectively.

General Data Protection Regulation (GDPR)

- **Region:** European Union (EU)
- **Focus:** Data privacy and protection of personal information
- **Key Requirements:**
    - Lawful processing of personal data
    - Consent management
    - Data subject rights (e.g., right to access, erasure)
    - Data breach notification within 72 hours
    - Appointment of Data Protection Officer (DPO)

Health Insurance Portability and Accountability Act (HIPAA)

- **Region:** United States
- **Focus:** Safeguarding protected health information (PHI)
- **Key Requirements:**
  - Privacy Rule: Defines permissible use of PHI
  - Security Rule: Protects electronic PHI (ePHI)
  - Breach Notification Rule: Requires timely notification
  - Risk assessments and staff training

ISO/IEC 27001

- **Region:** Global
- **Focus:** Information Security Management System (ISMS)
- Key Requirements:
  - Risk assessment and treatment
  - Security policies and controls
  - Asset management and access control
  - Continuous monitoring and improvement

Payment Card Industry Data Security Standard (PCI DSS)

- **Region:** Global
- **Focus:** Securing cardholder data during payment transactions
- Key Requirements:
  - Maintain a secure network and systems
  - Implement strong access control measures
  - Encrypt transmission of cardholder data
  - Regularly monitor and test networks

Sarbanes-Oxley Act (SOX)

- **Region:** United States
- **Focus:** Corporate governance and financial transparency
- Key Requirements:
  - Internal controls and auditing procedures
  - Certification of financial statements by executives
  - Documentation and review of controls

India’s IT Act, 2000 & CERT-In Guidelines

- **Region:** India
- **Focus:** Cybersecurity and incident reporting
- **Key Requirements:**
  - Protection of sensitive personal data
  - Mandatory breach notification to CERT-In
  - Compliance with security practices for critical infrastructure

SOC 1, SOC 2, and SOC 3 Reports

- **Region:** Global
- **Focus:** Internal controls and data security for service organizations
- Key Reports:
  - SOC 1: Focuses on financial reporting controls
  - SOC 2: Evaluates security, availability, processing integrity, confidentiality, and privacy
  - SOC 3: Public-facing version of SOC 2

Compliance frameworks

REPORTING REQUIREMENTS FOR DIFFERENT INDUSTRIES

Reporting Timelines by Framework

Framework	Incident Reporting Timeline	Audit/Compliance Reporting
CERT-In	6 hours	Annual cybersecurity audit
RBI	2-6 hours	Quarterly audit reports
PDPB/DPDP	Reasonable time for breach notification	Periodic audits after enactment
DoT	12 hours for critical infra breaches	Quarterly audit submission
Central Electricity Authority(CEA)	24 hours for power system incidents	Annual SCADA audits
National Critical Information Infrastructure Protection Centre (NCIIPC)	6 hours for critical infra attacks	Periodic security protocol review

Reporting Timelines by Framework

Framework	Incident Reporting Timeline	Audit/Compliance Reporting
HIPAA (US)	60 days for breaches (500+ affected)	Annual Security Rule compliance audit
GDPR (EU)	72 hours	Annual DPIA and compliance audits
PCI-DSS	Immediate reporting of card breaches	Quarterly scans and audits

Reporting requirements for different industries

ROLE OF COMPLIANCE IN INCIDENT RESPONSE

Prevention and Preparation

- **Risk Assessment** – Regular checks to identify vulnerabilities (e.g., ISO 27001, HIPAA, GDPR).
- **Security Controls** – Implement technical, administrative, and physical measures to protect data.
- **Training Programs** – Periodic employee training to handle and respond to incidents (e.g., HIPAA, PCI-DSS).
- **Example:**
    - **HIPAA** – Mandates risk assessments to protect Protected Health Information (PHI) by identifying and mitigating risks.
    - **PCI-DSS** – Requires encryption, access control, and regular vulnerability scans to minimize data breach risks.

Detection and Identification

- **Monitoring and Logging** – Regulations (e.g., CERT-In, ISO 27001, PCI-DSS) require logging and monitoring to identify anomalies.
- **Early Warning Systems** – Compliance often mandates IDS/IPS and SIEM solutions for proactive threat detection.
- **Audit Trails** – Logs must be maintained for forensic analysis and incident tracing as per regulations.
- **Example**:
  - **CERT-In Guidelines** – Logs must be retained for 180 days to aid post-incident investigations.
  - **PCI-DSS** – Enforces real-time monitoring and immediate responses to suspicious activity.

Response and Containment

- **Incident Response Plan (IRP)** – Mandated by ISO 27001 and NIST 800-61 to outline steps for containing incidents.
- **Defined Roles** – Compliance frameworks require assigning specific roles (e.g., incident manager, forensic investigator, legal advisor).
- **Communication Protocols** – Escalation and communication procedures (internal and external) are required.
- **Examples:**
  - **ISO 27001 (Annex A.16)** – Establish and regularly test incident response plans.
  - **GDPR (Art. 33)** – Document incidents and notify authorities within 72 hours.

Reporting and Notification

- **Breach Notification Timelines** – Compliance frameworks specify deadlines for notifying regulators, stakeholders, and affected individuals.
- **Accurate Disclosure** – GDPR and HIPAA require reporting incident details, including scope, impact, and remediation efforts.
- **Documentation** – Detailed records and audit trails of response actions are mandatory.
- **Examples:**
  - **GDPR** – Notify supervisory authorities within 72 hours.
  - **HIPAA** – Notify affected individuals within 60 days if 500+ individuals are impacted.
  - **CERT-In** – Report incidents within 6 hours.

Mitigation and Remediation

- **Post-Incident Review** – Root cause analysis (RCA) and lessons-learned exercises are required by frameworks like ISO 27001 and NIST 800-61.
- **Security Patching** – Compliance mandates applying patches and resolving identified vulnerabilities after incidents.
- **Process Improvement** – Post-incident findings must lead to updates in security policies and controls to prevent recurrence.
- **Examples:**
  - **ISO 27001 (Clause 10)** – Stresses continual improvement and corrective actions following security incidents.
  - **PCI-DSS** – Requires remediation of vulnerabilities based on root cause analysis of data breaches.

Audits, Review, and Continuous Improvement

- **Post-Incident Audits** – Periodic audits ensure corrective actions are effectively implemented.
- **Continuous Monitoring** – Regular vulnerability scans and penetration tests are required to assess cybersecurity posture.
- **Policy Updates** – Post-incident findings drive updates to security policies, risk management, and response protocols.
- **Examples:**
  - **NIST 800-61** – Highlights post-incident evaluations to address gaps and enhance response processes.
  - **CERT-In Guidelines** – Require submission of root cause analysis reports and compliance verification after incidents.

Why Compliance Matters in Incident Response

- **Legal Compliance** – Meet reporting timelines to avoid significant penalties.
- **Reputation Management** – Transparent and timely disclosures help reduce reputational harm.
- **Customer Trust** – Show dedication to data protection and privacy to build confidence.
- **Response Efficiency** – Predefined processes ensure a swift and effective incident response, minimizing impact.