What we will discuss today?

1. Brief on Information Technology in last two decades
2. Information Technology a necessity for business?
3. Why we cannot avoid IT in business & Corporate?
4. What is the impact of advancement in technology on business?
5. What are the challenges associated with use of Information technology.
6. What happened in last one decade (mega scandal)?
7. How we can prevent, detect and respond to these challenges
9. Compliance risks associated with e-commerce
10. Employment Agreement & Communication with Competitors & Customers
11. Cyber Security and Privacy Laws
In the early 1980s with the first desktop computers, information technology has played an important part in the U.S. and global economies. Companies started to rely on IT for fast communications, data processing, and market intelligence.

IT has played an integral role in every industry, helping companies improve business processes, achieve cost efficiencies, drive revenue growth and maintain a competitive advantage in the marketplace and mega corporate growth in last two decades like Microsoft, Netflix, Google, Yahoo, Face book, Amazon, Oracle, SAP, Watsapp, Netflex, Uberect.

Information Technology helps businesses in a number of ways that are generally centered on doing things bigger, better, and faster than you could without technology. Different industries and companies rely on technology in different ways, but widespread uses include business communication, optimized production, inventory management, and financial record-keeping.

Cross Borders Customers & Business: In last two decades business got freedom from borders without geographic limitations. By crossing borders, businesses have new markets with new customers in new socio-economic environment. Information technology further accelerated this revolution with introduction of worldwide web and then smart phones.

Compact Disc Replaced Heap of Paper Files: Business transformed from big paper files warehouses, to compact server, cloud technology and then big data warehouses.

Your Smart Phone is Mega Retail Store Display & Bank Cash Register: Large retail stores converted into window display and to smart phone one click online shopping tools. Business world transformed at speed of light in last two decades from paper currency to plastic cards, and then a new horizon of Crypto currency transaction.

Smart Phone & Gadgets Broadcasting Machines: Smart phones are converted in walking and talking real time news room that reached the entire world within seconds of recent past incidents.

1. Business growth
2. Market share & business survival
3. Increase their market share
4. Right decision making with accuracy and speed
5. Customers needs and expectation
6. Easy access to customers & suppliers
7. Communication with customers
8. Efficiency of operations by data analysis
9. Business culture and class relations
10. Security, research capacity
11. Global presence and cross borders sales
12. Systematic management and resource planning
13. Real time monitoring of business performance
14. Effective marketing with target customers
15. Accurate business planning customers target group based
16. Customer support timely, instant with immediate solutions.

Why we cannot avoid IT in business & Corporate? Businesses are driven by customers needs, expectations, trends, behaviors and satisfaction level.
What is impact on business with advancement in technology?

Based on research conducted in year 2017, and researchers calculated that in 2016 & 2017 global e-commerce website based sales reached more than $22 trillion across the globe. There is a 6% annual increase in sales and in 2020 estimated sales will reach to $27 trillion with potential growth of 17% by 2020.

Imagine where we will stand after 2020?

What if there is abuse of e-commerce transactions just only 0.1% of 27 Trillions USD business transactions, minimum translated impact would be USD 2700 Billions.

These losses may include bad corporate reputation, market position, trade of stocks in market and legal expense etc.

Federal Trade Commission (FTC) and Department of Justice Reported that in Year 2017, 1 in 5 people is affected by IT related Fraud and scams, where they lost money.

In year 2017 Total Business IT related scams were 27,000 in USA Only.
In Year 2018 22,704 scams added to the “BBB Scam Tracker” (Better Business Bureau)

What are Compliance Challenges associated with use of Information technology?

Information technology has also brought a compliance challenges for businesses. Major risks due to failure of IT system leads to legal action by customers and regulatory bodies, financial forfeiture and even bankruptcy. Business face these challenges when they are fail to adopt industry laws & regulations, internal policies or prescribed best practices i.e. breach of data confidentiality, customers complaints and legal actions, doing business with bad organizations etc.

New examples are:

From 2001, the number of scams in America has grown dramatically, with consumers now losing a hefty $257 billion to $337 billion a year to fraudsters, according to an organization Marketdata.

Western Union: Federal Trade Commission (FTC) and Department of Justice reached multistate settlement with Western Union of $586 million.

Equifax Data Breach: Equifax is one of the nation’s three major credit-reporting agencies.

Google lost $5.1 billions anti-trust case in European Union.

Facebook Recent Crises– Russian Meddling in USA Election (Alphabet and Facebook).

Uber – Data Breach Cases and incident sexual harassment goes viral lead to customer trust and business loss.

Yahoo! – Accounts Hacked. They admitted in October 2017 that 3 billion users compromised.

Samsung’s Bribery Charges – Where top management is behind the bars.

Corporate Sexual Harassment & #METOO hash tag (Harvey Weinstein’s Case). Loss of share value.

Compliance Risks Associated With E-Commerce & ERPs

E-commerce business started in late 90s by Amazon which then followed by eBay, Bestbuy, Alibaba and now uncountable online e-commerce business. Now every single business enterprise started online buying and selling. There are number of incidents discussed in earlier slides, which give a glimpse of compliance and fraud issues related to e-commerce and online transactions. Major identified e-commerce and online business compliance risks are associated with following:

Anonymous Buying & Selling: by online customers without authentication and identity checks. Anonymous online buying and selling is highly connected with identity theft incidents where fraudsters used stolen identity information for online buying and selling. A complete consumer information shall be taken before transactions processing.

Money Laundering By Cross Border Transactions: are identified recently, where a number of sales transactions raised red flags of “Money Laundering” because there was no actual physical transaction of products. Sales of goods were just an option and bilateral payments made by cross borders seller and buyers. Criminals are using open source online buying and selling platform for money laundering because online platform never inquire source of income from international cross border customers. Online platform use fake transactions to show sales volume and subsequent benefit in stock markets as an organized fraud.
Absence of due diligence about compliance of product sourcing, warehousing & supply chain are not declared by online business to customers and regulators i.e. open source trading platforms where you cannot track source of products and compliance with supply chain either product is sourced from companies and countries with financial sanctions by international institutions. Either seller or buyer supply chain is compliant with health safety, environment and labour laws.

Invoicing & Taxation: issues with cross state and cross border transactions are subject to tax evasion manipulating different tax rates in different states, tax exemption and plea of dual taxation treaties. Online transactions shall be designed in a way to be compliant with taxation law of every jurisdiction either between states or a cross border transactions.

Payments Terms & Conditions: most of the times are not defined in a manner where customers may understand product price, service charges, applicable taxation, order cancellation charges, processing fee, services charges on refund. A number consumers reported misrepresentation regarding services charges apart from delivery services charges. Payment terms and conditions shall be clear and must be acknowledged by customers before formal processing of order.

Disclaimers: about Buying & Selling are not communicated, product availability, tentative and conditional availability and cancelation of orders with penalties.

Digital Signature: or biometric identification must be part of every online transnational transactions.

Personal & Protected Information data: is one of biggest issue of ecommerce. There are number of data breach cases reported where customer personal and protected information stolen and shared publically. These risks cost corporate huge monetary and reputational losses in recent past examples are Equifax’s and Uber Data Breaches cost millions to users, Alphabet & Facebook issues costs billions of USD and investigation of USA current government administration.

Price Manipulation, Bid Rigging & Cartelization: are identified in B2B e commerce transactions by sharing customer/buyer information with competitors to create demand and supply gaps. Retailers share price quoted by suppliers with competitors for fixing and exclusivity.

Crypto Currency influx in ecommerce transactions. Taxation issues about money without identification.

How many of us read online agreements before acknowledging terms and conditions?

Online Transaction Agreements: are one of most importance compliance risks that leads to a legal action by regulatory bodies and consumer protection organizations. Terms and conditions of online agreements are not exhaustive covering all aspect of payment terms, services charges including delivery and transaction fee, taxes, mode of delivery and tentative time of delivery etc.

For cross or international transactions international conventions on transnational business transactions must be included i.e. Warsaw Convention, Hague Visby rules, Montreal Convention, New York Convention Must be considered in agreements.

Dual Acknowledgement: of terms & conditions shall be taken by seller and customer with clear statement of compliance with local law, and international conventions particularly in reference to transnational transactions.

Implied Consent: is one of major risks that lead to dispute between and online seller and buyers, which results in fight against and subsequently damage corporate reputation.
Ecommerce Compliance Program must be in place in every organization in ecommerce business with focus on
compliance risk management with proactive and timely identification of potential compliance risks, related to
transactions with extensive training of employees with high risk exposure i.e. sales and buying team.

Compliance Risk Management by risk identification, risk profiling, mitigation plan, detection and response to crises
are usually absent in corporates that turned to disasters in above examples and scams.

Compliance Surveys/Audits to detect any potential breach and gap identification and mitigation.

Compliance Governance Mechanism shall be in place in purview of compliance survey findings, risk assessment,
mitigation measures and control structure & mechanism to ensure implementation IT related compliance risks.

How we can Identify These Compliance Challenges

<table>
<thead>
<tr>
<th>Prevent</th>
<th>Detect</th>
<th>Respond</th>
</tr>
</thead>
</table>

Corporate Compliance Governance Mechanism People, Policies & Procedures to mitigate challenges

Information technology related compliance risks can be mitigated by an effective compliance governance
mechanism (CGM). CGM mainly consists of three pillars.

Compliance Professionals with Competency to understand relationship of your business and information
technology, pace of change in business environment and make it compatible with management policies.

Corporate Policies is most important pillar of CGM. Policies are driving force to streamline business
environment change to be compliant with updated corporate code of conduct and ethical business operations
aligned with laws.

Business Operation Procedures are updated and aligned with IT changes i.e. fiduciary responsibility of
investor/shareholder and business management. Procedures to handle corporate information while interacting
with employees, customers, suppliers and competitors. What we need to communicate and what not.

Proactively Compliance Risk Management and Role of Employees

Employees are first point to mitigate compliance risks and employment agreements are first step to resolve issues.

Organizations shall design employment agreements in such a way that all compliance risks related to IT
and ecommerce are managed along with systems i.e. non-disclosure agreements, data confidentiality,
non-compete clause, ethical conduct, responsibility to whistle blow and clear guidelines to interact with
customers, competitors and suppliers.

Declaration of Risks for Employees

- Risk of high fines against your company and against you
- Risk for Your Organization reputation also for your reputation
- Risk of high costs for defence against you
- Risk of damage claims by our customers against company and you
- Risk of invalidity of contracts for your company and for you
- Personal risk of disciplinary action against you by regulators
Role & Duties of Compliance Professional
- Risk Identification, Assessment and Evaluation
- Risk Response
- Risk Monitoring
- Information Systems Control Design and Implementation
- Information Systems Control Monitoring and Maintenance
- IT Policies/Governance and Compliance
- Disaster Recovery System and Coordination with regulators and customers
- Audits and Reviews Preparation and Facilitation
- Direct involvement in IT related projects and business initiatives

Detailed Compliance Professional Duties are available

Major Information Technology Related Reported Scams
IT scams hit corporate and individual in different ways and impacted corporate business and customers beyond repair. As per online data available following are major IT scams are:

1. Airbnb Scam
2. “Can You Hear Me” and “Yes” Calls
3. Car Scams
4. Cryptocurrency Scams
5. Death Threat Hoax
6. Fake Bank Apps
7. Grandparent Scams
8. IRS Scam
10. Medicare Card Scam
11. Netflix Scam
12. Parking Scams
13. Romance Scams
14. Secretary of State Scam
15. Shimmer Scams
16. Tax Arrest Scam
17. Tax Prep Scam
18. Tech Support Fraud
19. Veterans Scams

Thank You