

PMG 611

Enterprise Risk Management

Prepared by Dr. Abdullah Jameel Halawany

جامعة الجميع الذكية

تسعى لتكون الكيان الأول الذي يتبنى مبدأ المجتمع التعليمي
التعاوني ويقدم العلم مقابل العمل لتنمية وبناء المجتمعات.

Lecture 6

Compliance Issues Today



جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY

Lecture 6

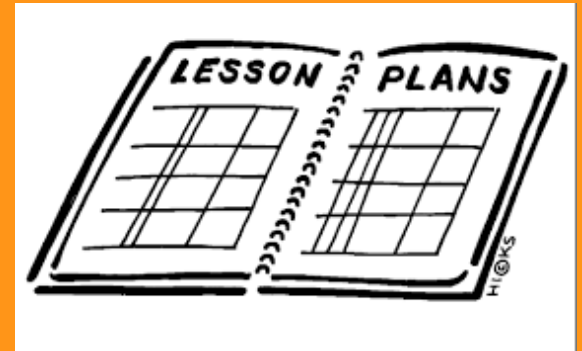
Session Outline

Compliance Issues
Today

Establish A
Compliance
Assessment Team

Compliance Risk
Assessments and
Compliance
Program Reviews

Work Unit–level
Compliance
Tracking and Review
Processes



Lecture 6

Introduction



جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY

- Dictionary definition, compliance is either a state of being in accordance with established guidelines, specifications, or legislation, or the process of becoming so.
- For enterprise management, compliance is the process of adhering to a set of guidelines or rules established by *government agencies*, *standards groups*, or *internal corporate policies*.

- Adhering to compliance-related requirements is a *challenge* because of the many and varied laws, rules, and standards that an enterprise faces on a local, national, international, and industry-wide basis.
- *Failure* to comply with some of these matters can result in fiscal, legal, or even criminal penalties.

- Techniques for an enterprise to assess its *current compliance requirements* and then to establish processes to *monitor* its compliance with significant rules and regulations *affecting its operations*.

- An enterprise will *probably never be in full compliance* with the myriad, often conflicting, rules and procedures it faces.
- It must develop a program to be generally in compliance with its *most important and significant rules*.

- A strong compliance program will help to build an effective **GRC** culture and set of principles.
- Techniques for an enterprise to **assess** its current compliance requirements and then to establish processes to **monitor** its compliance with *significant rules and regulations* affecting its *operations*.

Lecture
6

Compliance Issues Today



جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY

- Levels of compliance rules have always been with business enterprises.
- It is almost a natural response for a business manager to say that rules are a lot worse “now” than in past years.
- But this a typical response over time.
- Hearings leading up to the Sox legislation identified that *some existing compliance rules were ignored or there were no rules in other areas.*

- Multiple new rules were established for financial reporting and auditing, public accounting firms, board governance, and more.
- ***The level and complexity of these new compliance rules continues.***
- An enterprise should develop an **overall compliance program** to identify *new* and *existing* rules, to *identify* and *reduce* the risk of breaching such rules, and to rapidly and effectively remedy any breaches that may occur.

- A successful **Compliance Program** will engender a culture of compliance within an enterprise and assist it to become or remain a good corporate citizen.
- There is ***no single generic compliance program*** as each enterprise's circumstances are different.

- Depending on the size and risk profile of the company, a compliance program can be as
 - *Simple* as implementing an effective complaints handling system and providing all relevant staff with trade practices training tailored to the business activity
 - It could be more *comprehensive*

Lecture 6

Compliance Program Activities

- Establish or set up a team of dedicated compliance staff.
- Conduct regular trade practices compliance risk assessments and compliance program reviews.
- Design detailed guidelines and procedures for different business units that face all unique operational, financial, or trade practices risks.
- Establish systems to keep track of the enterprise's legal and regulatory requirements.
- Develop and maintain compliance-related staff education programs.

Lecture 6

Justification for a Compliance Monitoring and Control

1. Enterprise should take steps to comply with legal obligations they must “comply or die”;
2. The need for statutory due diligence defenses;
3. Statutory and common law obligations of directors/officers to exercise reasonable care;
4. The duty of directors to assure themselves that they are reasonably informed of material events concerning the corporation, including possible breaches by it of legal obligations;
5. Avoidance of corporate criminal responsibility for breaches by individual officers and employees;
6. Mitigation of penalties in the event of breach;
7. Maintenance of market integrity;
8. Numerous statutory legal requirements.

Lecture 6

Establish A Compliance Assessment Team



جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY

- There are typically three different groups of functions that should have responsibility for monitoring and directing an enterprise compliance performance:
 - *Legal*
 - *Internal audit*
 - Other *Specialized Compliance Assessment Functions*
- There are significant differences between these three groups.

- *Specialized Compliance Assessment Functions*
- Is more of a foot on the ground type of function that better understands specialized areas of operations such as
 - issues on the export requirements for dealing with some specialized products or
 - customer complaints over a hotline type of telephone referral system regarding product quality or pricing compliance rules.

- There can often be a significant overlap between a *Compliance Function* and *Legal*.
- These two departments share responsibility for ensuring the enterprise complies with its legal and regulatory obligations and will often jointly undertake the functions.
- In some industries, such as in the financial services industry, the corporate law department often performs both legal and compliance functions.

- *Compliance Function* cannot act as legal representative for the organization and therefore does not draw up contractual documentation, act in litigation, or give formal legal opinions.
- A *Corporate Law Department* generally acts in a representative or advisory capacity and does not get involved in the administration of systems and procedures nor in their monitoring and surveillance.

- *Internal Audit* is a risk control function that is responsible, among other duties, for testing the adequacy of internal control systems and recommending improvements.
- These will overlap with some areas that also fall within the responsibility of a *Compliance Function*.

- *Internal Audit* generally carries out its reviews based on an annual plan and selects areas to review based on an audit sample and test basis.
- The monitoring and surveillance undertaken by a *Compliance Function* should generally be done on a real-time basis.
- *Recommendation* here is that an enterprise should establish a specialized compliance function or operating department, separate from either legal or internal audit.

Lecture 6

Essential Ingredients of an Effective Compliance Program

- **Total Commitment**
- **Compliance policy**
 - clear statement of the enterprise's commitment to compliance
- **Compliance-Related Operational Procedures**
 - that will address the problems identified through audits and ensure breaches of the law will be avoided.
 - documented procedures / due diligence procedures / incentive and reward programs / vetting trade practices
- **Active, Ongoing Program to Maintain Compliance Processes**
 - The compliance program and systems should be monitored, maintained, well documented, and communicated to staff to ensure the program continues to be both effective and efficient.

Lecture 6

Compliance Risk Assessments and Compliance Program Reviews



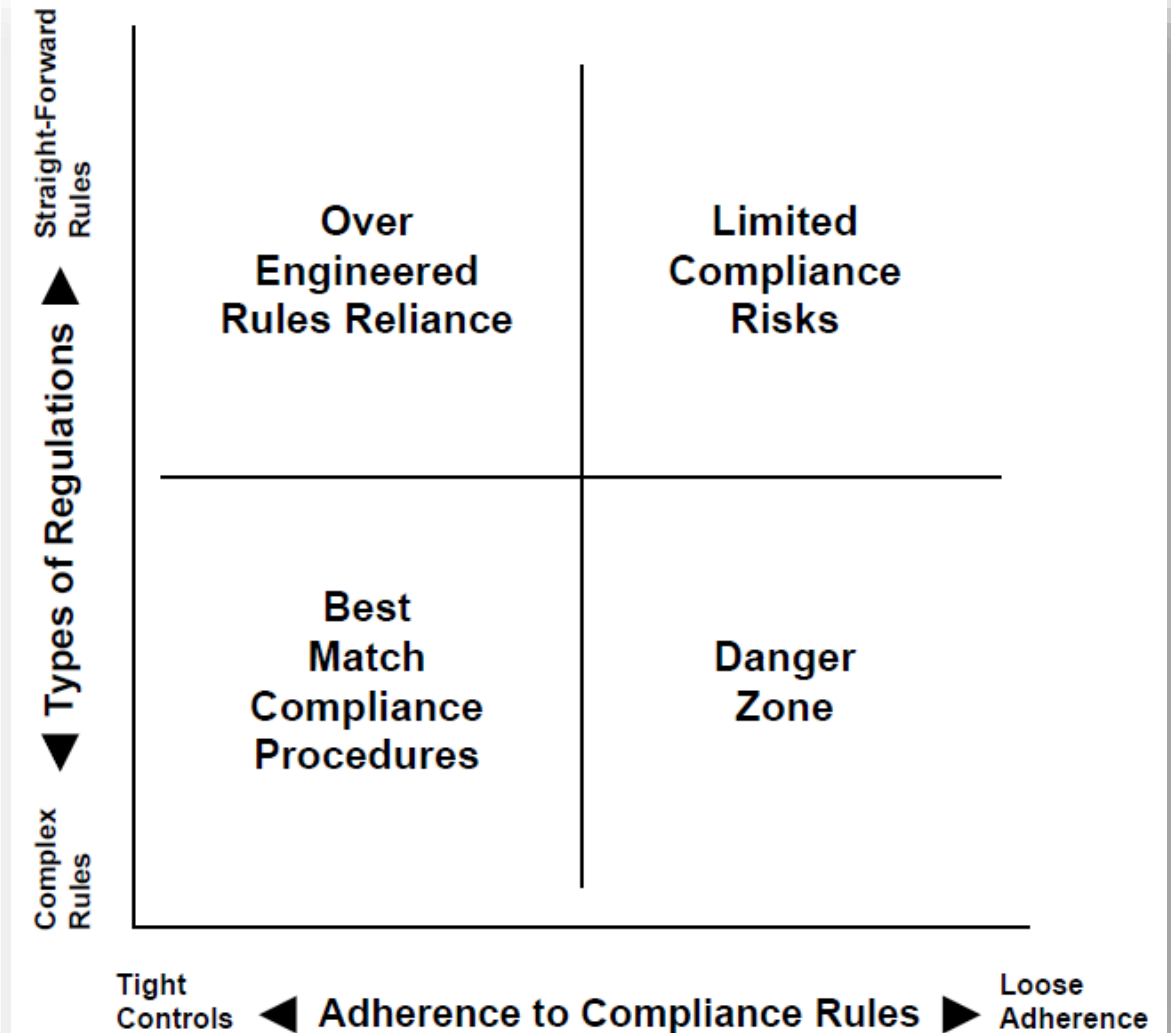
جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY

- Businesses must make **Compliance Decisions** when faced with the multiple rules in the many areas where they operate.
- **Compliance Decisions** is somewhat based on their appetite for risk
- **Risk Appetite**
 - Is the amount of risk an enterprise is willing to accept in the pursuit of its objectives.
 - Can be measured in quantitative or qualitative terms

Lecture 6

Enterprise Rules Versus Compliance Options

- The horizontal axis shows an enterprise's levels of adherence to compliance rules and regulations.
- The vertical axis covers the complexity of compliance rules.
 - Nuclear Power Plant
 - Retail Merchant



- Both of these horizontal and vertical measures are judgmental and represent both general attitudes and management policy.
- A CEO cannot announce at an annual meeting that the enterprise will only comply with most of its legal rules.
- Enterprises should identify those compliance issue risk areas that may have significant impacts on them and should use these identified risks to provide the infrastructure for the development of a compliance program.

Lecture 6

Identify A Compliance Risk Assessment Process

Step 1: Identify the Compliance Risks and Exposures

- Develop a list of all the compliance risks that can affect the successful achievement of the work unit's goals and objectives.
- Determine the applicable laws, rules, regulations, policy, or procedure driving the identified risks.

Step 2: Measure the Identified Compliance Risks

- The impact of the risk (also in terms of high or H, medium as M, or L for low), when it happens, on the achievement of the work unit goals and objectives.
- The probability of the risk becoming a reality (High, Medium, or Low).

Step 3: Prioritize the Identified Compliance Risks

- All risks that have an HH "measurement value" should be placed at the top of the risk inventory, followed by HM, HL, MH, MM, ML, LH, LM, and LL groups in that order.
- Rank order each "measurement value" group from most to least significant via a paired elimination process.

Step 4: Develop a Risk Assessment Matrix for Each "Measurement Value"

Step 5: Review the Risk Assessment Matrix

Lecture 6

Severity	Consequences				Increasing Likelihood				
	People	Assets	Environment	Reputation	A	B	C	D	E
					Never heard of before in the Industry	Heard of in the Industry	Has happened in the Company or more than once per year in the Industry	Has happened at the Location or more than once per year in the Company	Has happened more than once per year at the Location
0	No Injury or health effect	No damage	No effect	No impact					
1	Slight injury or health effect	Slight damage	Slight effect	Slight impact					
2	Minor injury or health effect	Minor damage	Minor effect	Minor impact					
3	Major injury or health impact	Moderate damage	Moderate effect	Moderate impact					
4	PTD or up to 3 fatalities	Major damage	Major effect	Major impact					
5	More than 3 fatalities	Massive damage	Massive effect	Massive impact					

- The concept behind this risk assessment matrix is that each significant organizational or budget-level work unit should inventory all of their applicable policies, procedures, rules, and regulations.
- This can be accomplished by asking each unit:
 - “What are the problems you recognize, concerns you have, and risks you perceive regarding compliance with the federal and state laws and regulations, and corporate and systems-related policies and procedures in this work unit?”

- **High Impact.** If the risk happens, the work unit will probably not achieve its objectives or to do so will require major damage control.
- **Medium Impact.** If the risk happens, the work unit will have to do extra work or will be more inefficient but can still achieve its goals and objectives.
- **Low Impact.** If the risk happens, the work unit will be aware of it, but it will have little or no effect upon operations or the achievement of the objective.

- Beyond just designating a work unit as being responsible for a risk, there should be one employee (management or staff) who is delegated as responsible for the management of a particular compliance risk or risk area.
- The whole concept here is to empower enterprise work units with their responsibilities for compliance issues to help assure the enterprise continues to operate in compliance with key laws, rules, and other procedures.

Lecture 6

Work Unit–level Compliance Tracking and Review Processes



جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY

- An enterprise needs processes to track and review their compliance activities at both a total enterprise level and by individual budgetary departments or work units.
- There is always a need for *education programs* throughout the enterprise to communicate compliance rules at ***all levels*** as well as corrective action processes to make adjustments when work units are found to be not in compliance with rules and regulations.

- **Internal Audit Departments** have had a major responsibility to assess the status of internal controls in various areas of their enterprise
- Report their internal audit review findings as well as recommendations for corrective actions to management and their audit committee.
- They plan to review on risk-based internal audit planning approaches
- Because of limited time and resources, they will tend to focus their reviews on more major issues, such as compliance with specific internal controls rules.

- Planned internal audits and the audit programs developed to support the areas to be removed tend to support the more major internal controls concerns, such as do-the-debits-equal-the-credits internal accounting rules.
- The problem is that there are so many laws with compliance-related rules that it is very difficult to even maintain a level of full compliance with some of these applicable rules.
- Internal audit will typically not review a given area or location on a regular basis because of time and resource constraints.

- An effective way to assess compliance in many enterprise work units is to request that managers in operating units perform self-audits in the area of operations and report their results back to the enterprise compliance function or to internal audit.
- Compliance self-audits will migrate the ownership of compliance monitoring and assessment to business units to raise the awareness and understanding of compliance risks in routine processes and activities.

Lecture 6

Compliance Program Transformation

- COVID-19 accelerated the digital agenda for many financial institutions, but the work is not done.
- Decisions made under the pressure of adapting to the COVID-19 environment will need to be revisited to determine:
 - If they are optimal and sustainable
 - If there is alignment between technologies that have been deployed and the institution's target operating model
 - If the existing compliance workforce understands and can explain the technologies being deployed
 - What the impact has been on the customer journey
- Both management and regulators will likely be looking more closely at the choices that were made and how the benefits of those choices can be optimized, and the risks mitigated.

Lecture
6

Summary

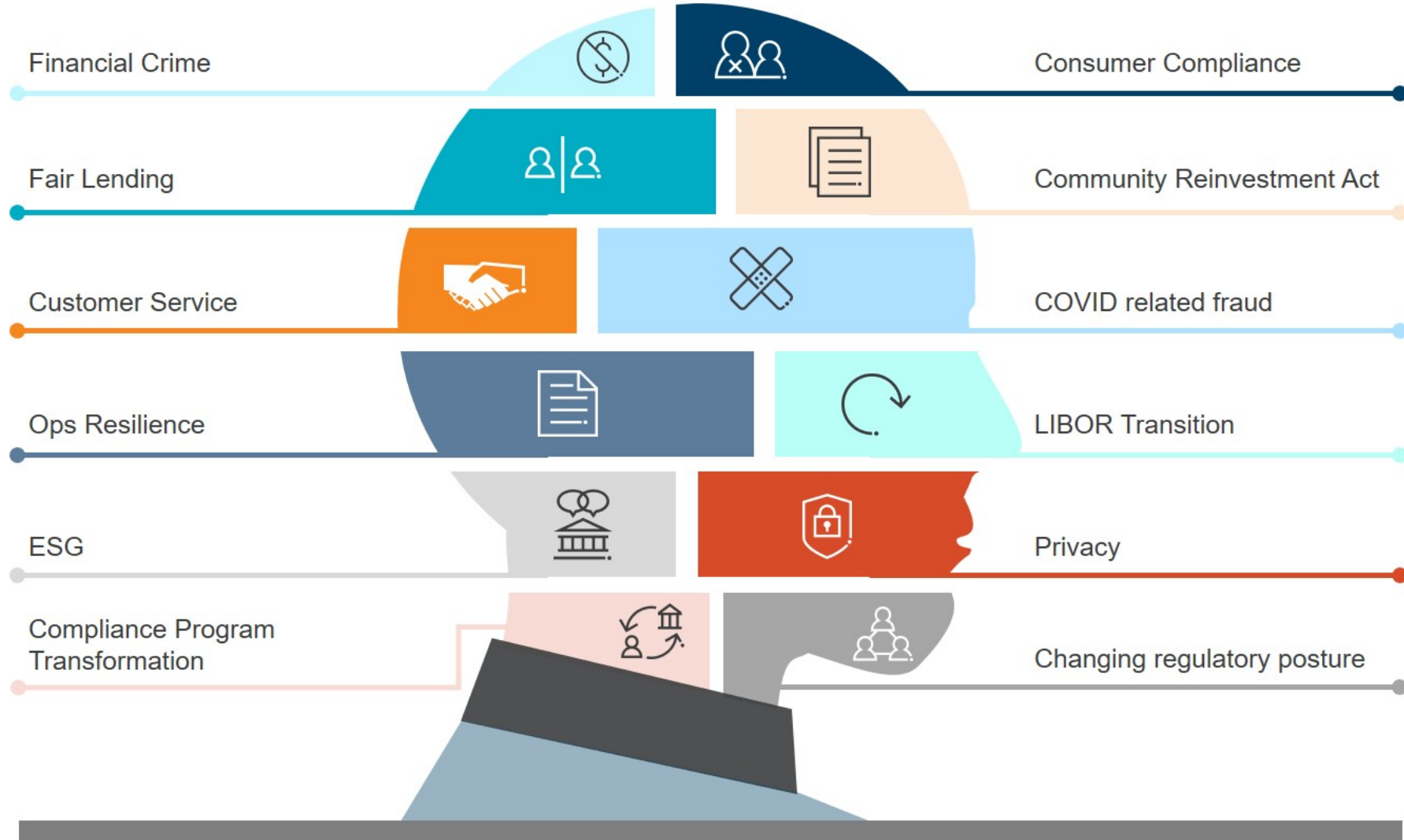


جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY

Lecture 6

- Compliance issues are often the most difficult element of establishing effective enterprise GRC programs.
- An enterprise can establish a governance framework where it understands the governance rules it will need to follow.
- Risk management is somewhat easier as we have established some good procedures for estimating and taking actions to manage risks, but compliance can cause some major challenges.
- The problem with compliance is that there are so many often conflicting legal and procedural rules that it is difficult to determine the most significant or important of them.

Lecture 6



Lecture 6

References

- COSO Enterprise Risk Management: Establishing Effective Governance, Risk, and Compliance Processes. *Robert R. Moeller*.



جامعة القصيم الذكية
EVERYONE'S SMART UNIVERSITY