



**IIMTS**  
Awarding Body

# IIMT STUDIES LTD **CENTRE POLICY**

IIMT Studies Centre Policy | Copyright- IIMT Studies Ltd. (IIMTS AB)

## Risk Assessment Policy

### Policy Compliance:

This policy complies with Ofqual,  
Handbook 3.



# IIMTS

## Awarding Body

### Awarding Quality Qualifications through Global Recognition

Document Code No. IIMTS\_AO\_OGCR\_RA\_01\_2020

<b>Title of the Policy:</b> Risk Assessment Policy	<b>Authorised by</b> Responsible Officer	<b>Created: Version 1</b> 1 November 2023
<b>Conditions of Recognition:</b> General Conditions of Recognition		<b>Current version: 3</b>  <b>Next Review Date:</b> 1 April 2026

#### Important contact-

Any query or concern related to this policy may be directly addressed to the Responsible Officer or the HR Manager-

IIMT Studies Ltd]  
Company number 11649333

Registered office address  
[Havelock Hub  
14 Havelock Place  
Harrow  
London  
HA1 1LJ  
Ph- +44-7466650066

Email- [info@iimtsab.co.uk](mailto:info@iimtsab.co.uk)  
Website- [www.iimtsab.co.uk](http://www.iimtsab.co.uk)]

**Awarding body:**

*IIMT Studies Ltd-* [www.iimtsab.co.uk](http://www.iimtsab.co.uk)

*Acronym used to represent IIMT Studies Ltd (IIMT Studies):*  
*IIMTS AB*

**Regulating Body:**

*OFQUAL*

*Ofqual.gov.uk*

**Index**

<b>Sr No.</b>	<b>Titles</b>
1	Policy Code
2	Policy Statement
3	Objectives of Policy
4	Definitions
5	Policy Framework

**(A) Policy Code: [IIMTS\\_AO\\_OGCR\\_RA\\_01\\_2020](#)**

**(B) Policy Statement :**

**The policy ensures the definition of the risk associated**

Every business is initiated to achieve any of, some of, or all of the following objectives/ goals:

- a. Profit and revenue earning.
- b. Social service and CSR.
- c. Service delivery and not-for-profit.

The business may be in any of the following sectors :

- a. Service & IT industry.
- b. Manufacturing.
- c. Retail and e-commerce.
- d. Banking and finance.
- e. Infrastructure and Logistics.
- f. Education and Learning.

Irrespective of the difference in goals and objectives or sector of business, as explained above, one of the common factors which remains critical to any business or any business goal is the risk factor involved. Every professional organisation, be it in any sector, always invests time, effort and other resources to identify risks involved in that business and the process and

methods to mitigate the risks identified.

**(C) Objectives of Policy:**

This policy aims at:

1. The core objective of the policy is business continuity amongst the risks that may interfere with business activities.
2. To ensure a smooth flow of delivery to the stakeholders, even during the obstacles, concerns and challenges that may thwart business, in any form.
3. To identify all potential risks that may have a negative impact on business operations or service deliveries, at any stage, in any form.
4. To identify all possible areas that may have a challenging time or risks involved, and to have processes and resources identified to mitigate the impact.
5. To have alternate plans ready or identified for the risk areas of the business.
6. To create an organisation, a Risk Ready organisation by :
  - Having an effective and efficient mechanism ready for risk identification and mitigation.

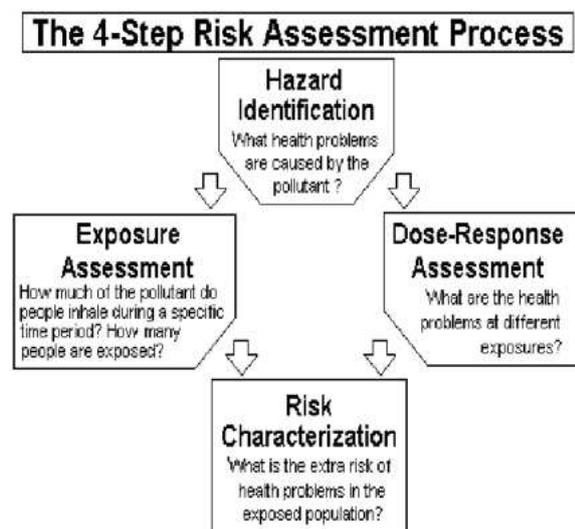
- Keeping the optional plan B ready for every plan that may face a risk or threat to continuity or delivery.
- Having a set of competent professionals for each role so that in case of any risk or threat to any business or business activity, they ensure that the risk or threat is mitigated and business and business activities continue in a near-normal way.

#### (D) Definitions :

**Risk:** Any person and/or activity and/or resource and/or situation which may cause or has a potential to cause or has caused any threat/challenge to the organisation or business activity or business operations or its service delivery- making it difficult or impossible or challenging to be carried on or carried out or to be continued. This risk or threat may be intentional or unintentional, natural or caused by someone planned or unplanned, internal or external and can cause or may cause financial/non-financial tangible or intangible damage/s to the organisation, immediately or in future.

**Assessment:** The risk assessment Process is a process to determine possible mishaps, the possibilities of mishaps and their probable impact on business or stakeholders. The process is always aimed at finding out the immunity and tolerance against possible risks.

The Risk Assessment Process can be defined as "The process of identifying, estimating, analysing and prioritising types of risks or potential risks to an organisation/institution/nation/individual or group and their probable impact. The assessment process also determines the vulnerability of an organisation to internal or external risks and its immunity level and tolerance level against potential or existing risks.



**Mitigation:** It's a well-defined and organised plan of action, process or method through which the potential or existing threat, risk or challenge can be nullified, diluted, eradicated or subsided- totally or partially so that the business operations or business-related activities can be continued with no interruption or minimum possible interruptions.

Risk can be defined as the 'Uncertainty of Outcome.' This uncertainty arises either from the possibility of a future positive opportunity or the presence of an existing negative threat while achieving a current business objective.

IIMT Studies' Risk Management and Contingency Policy is designed to identify, assess, and mitigate the impact of these uncertainties that may affect the achievement of its overall aims and objectives.

The primary objective of this policy is to enhance the regular management processes and safeguard the broader interests of stakeholders. It provides a framework to aid in the identification of possible risks, escalating, emerging, or common themes or the understanding and Management of the organisation's strategic risks at all levels.

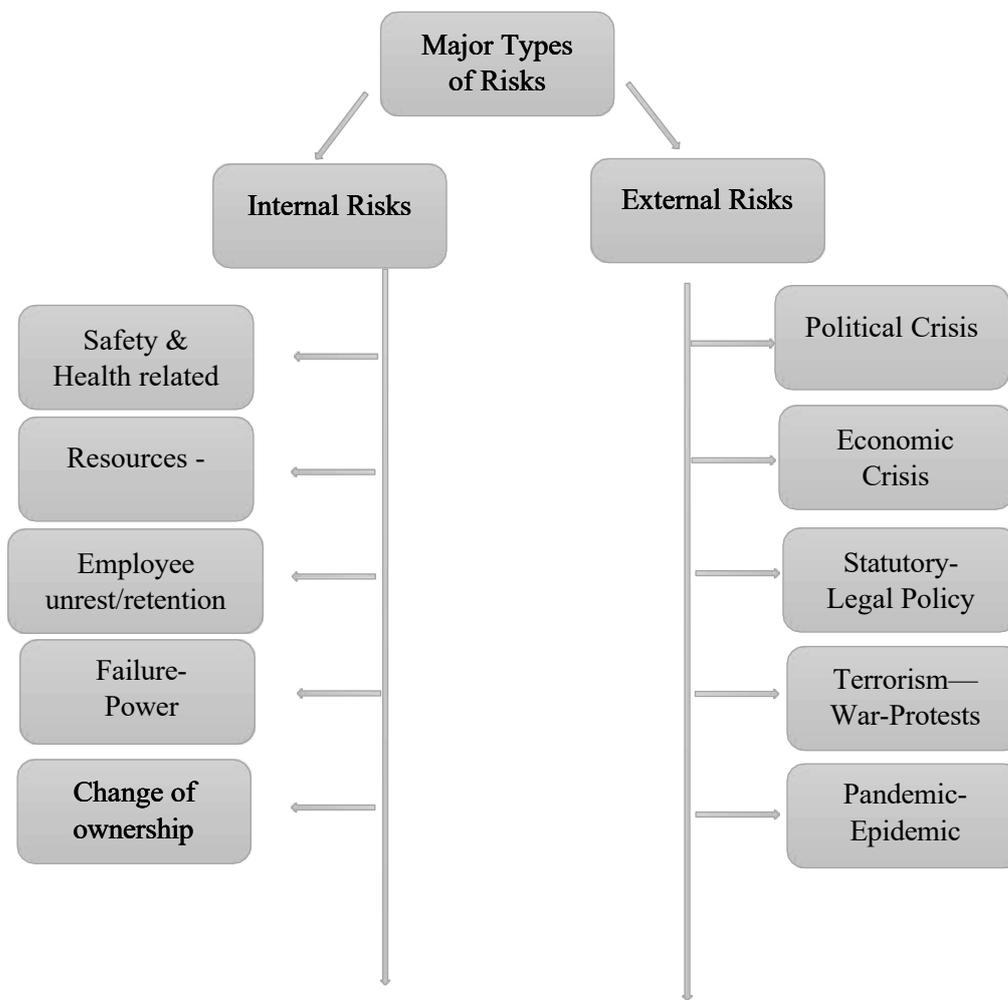
**(E) Policy Framework :**

This policy will have the following major segments :

- Identifying key deliverables & key business-critical operations to address and deliver the end objectives of stakeholders.
- Identifying key critical resources required
- Identifying and listing down all possible threats to the key critical resources
- Identifying alternates to key critical resources- keeping Plan B Ready.
- Regular reviews of risks and threats.
- Identifying competent senior professionals accountable for all steps.

**IIMT Studies' risk approach :**

The sole objective of this policy is to ensure flawless service delivery continuity irrespective of any kind of threats and risks against the business activities and operations; however, this broader scope can cover the following areas to anticipate, assess, manage and mitigate every possible risk and threats :





### Type of risks:

- Financial Risk: Any risk that creates a shortage of or blockage of revenue generation and income generation, resulting in the inability of the organisation to manage expenses, make payments and take care of its stakeholders, including employees.
- Resources Risk: Any concern, challenge or threat that creates a shortage of resources which are required to do business, deliver services and manage operations. These resources may include:
  - Infrastructural resources – assets and facilities.
  - Human Resources – skilled, semi-skilled, and unskilled manpower.
  - IT & Virtual Resources – internet connectivity. Communication network. Data and MIS. Power and electricity failure. Portal infrastructure and web-based platform.
  - Customer and stakeholders – losing any of them due to any reason.
  - Logistics and supply chain.

Additionally, business risk areas are:

- Natural calamities and unforeseen circumstances- include floods or earthquakes, pandemic/epidemic situations, fire, etc.
- Political turmoil and economic failure in a country or across the globe.
- Legislative changes or statutory amendment policy changes by the government cause a negative impact on business.
- Theft- burglary or any such casualty.
- Acquisition- merger- change in ownership due to any reason.
- Statutory actions and legal issues resulting in the closure of the business or a major setback.
- Employee unrest or trade union movement is causing a halt to business operations.
- The war between countries, terrorism, strikes of public utility services, public protest, or any such event.

The IIMT Studies risk management process is undertaken through the following steps:

- Identifying Key Strategic Risks: identification of strategic risks critical to the potential hindrance of achieving objectives.
- Assigning Responsibility: Allocating responsibility for coordinating the Management of risks.
- Recording All Risks: Ensuring registration of all identified risks.
- Evaluating Risk Significance: Assessing the significance of each identified risk.
- Articulating Risk Appetite: Clearly defining IIMT Studies's stance on risk appetite.
- Identifying Responses to Risks: Determining appropriate responses for each identified risk.

- **Internal Control System:** Ensuring the internal control system plays a critical role in managing identified risks.
- **Developing Assurance Mechanism:** Establishing an assurance mechanism for the regular review of the risk management framework.

To ensure the coordination of this process, oversight is an effort involving the Board of Governors and the Management team. Board members review the activities with relevant staff within their areas, and take ownership of managing specific risks of respective departments. The Director of Operations, in coordination with the entire team, is responsible for preparing a Risk Schedule outlining how specific risks are managed.

### **IIMT Studies Risk Register:**

The Risk Register is the base for actionable plans and broader contingency strategies, addressing control weaknesses and mitigating risks as necessary for a suitable business.

#### **Risk Register Maintenance:**

This register is developed in line with key strategic risk areas and remains a critical document subject to at least monthly review by designated risk owners/managers. This process ensures the ongoing relevance and effectiveness of risk identification, assessment, and mitigation strategies. The risk registered is, after review, submitted to the General Manager/CEO of the organisation 12 times every year.

### **Risk Compliance:**

#### **Assurance Responsibility:**

Within the Management team, the Head of Compliance has the crucial role of providing periodic assurance to the Board of Governors regarding the adequacy of risk management. This involves an assessment and validation of the risk management framework, ensuring its alignment with organisational objectives and regulatory requirements.

#### **Strategic and Operational Oversight:**

The General Manager/CEO in the management team takes the lead in providing strategic direction on the significant operational and strategic risks confronting the organisation. This proactive approach is to identify emerging risks, formulate mitigation strategies, and align risk management efforts with overarching organisational goals.

**Departmental Responsibility:** Department Heads play an important role in the risk management process. They are responsible for managing all risks within their respective areas of control. This role ensures the creation and maintenance of systems for identifying, assessing, managing, and reviewing risks, all in strict compliance with the IIMT Studies Risk Management process. This approach ensures that risks are addressed at the operational level, promoting a risk-aware culture.

**Reporting and Escalation:** A primary responsibility of the risk management framework is the timely reporting and escalation of risks. When risks exceed the scope of manageable thresholds or require specialised attention, a reporting and escalation mechanism is needed. This approach ensures the risks are appropriately communicated, assessed, and addressed in accordance with procedures within this policy.

Annual Internal Audit: Making sure to have transparency and accountability, an annual internal audit of the risk management process is mandated. This audit is headed by the Head of Compliance and remains an evaluation of the effectiveness and efficiency of the risk management framework. The findings and recommendations are specified in a detailed report submitted to the Board of Governors. This audit process is a part of continuous improvement and refinement of risk management strategies in line with the requirements of regulators.

### Impact Chart:

#### Risk impact criteria:

#### **10 Critical**

Critical impact on the achievement of IIMT Studies' aims, objectives, and overall performance.

Service severely affected, major loss of income and/or reputation, or a significant increase in costs. Very difficult and long-term to rectify.

Financial loss >40% of the annual budget.

Ofqual enforcement action; loss of delivery centres; >50% of learner numbers.

#### **9 Critical**

Major impact on costs, income, and certain key organisational objectives.

Affects a significant part of the organisation.

Serious impact on output, levels of service, and external relationships.

Medium to long-term effect on reputation and expensive to recover.

The financial loss of 26-40% of IIMT Studies' annual budget.

Loss of a number of high-profile staff/ad hoc contractors.

#### **8 Major**

Major impact on costs, income, and certain key organisational objectives.

Affects a significant part of the organisation.

Serious impact on output, levels of service, and external relationships.

Medium to long-term effect on reputation and expensive to recover.

The financial loss of 16-25% of IIMT Studies' annual budget.

Loss of a high-profile member of staff/research group.

### **7 Major**

Significant waste of resources and impact on operational efficiency, output, quality, and goals in more than one work area.

External contacts may be affected, and reputation damaged.

Medium-term effect, and may be expensive to recover.

The financial loss of 6-15% of IIMT Studies' annual budget.

Loss of a high-profile member of staff/research group.

### **6 Serious**

Significant waste of resources and impact on operational efficiency, output, quality, and goals in more than one work area.

External contacts may be affected, and reputation damaged.

Medium-term effect, and may be expensive to recover.

The financial loss of 6-15% of IIMT Studies' annual budget.

Loss of a high-profile member of staff/research group.

### **5 Significant**

Significant waste of resources and impact on operational efficiency, output, quality, and goals in more than one work area.

External contacts may be affected, and reputation damaged.

Medium-term effect and may be expensive to recover.

The financial loss of 6-15% of IIMT Studies' annual budget.

Loss of a high-profile member of staff/research group.

### **4 Moderate**

Medium impact on output, time lost, finance, or assets.

Short to medium-term effect.

The financial loss of 6-15% of IIMT Studies' annual budget.  
Loss of a Key Member of staff.

### **3 Medium**

Medium impact on output, time lost, finance, or assets.  
Short to medium-term effect.  
The financial loss of 6-15% of IIMT Studies' annual budget.  
Loss of a Key Member of staff.

### **2 Minor**

Minimal financial or other loss, delay, interruption, or inconvenience.  
Little or no damage or effect on IIMT Studies' reputation. It can be easily and quickly put right.  
Financial loss <5% of the organisation's annual budget.  
Loss of a Key Member of staff.

### **1 Minimal**

Minimal financial or other loss, delay, interruption, or inconvenience.  
Little or no damage or effect on IIMT Studies' reputation. It can be easily and quickly put right.  
Financial loss <5% of the organisation's annual budget.  
Loss of a Key Member of staff.

### **No Risk**

No financial losses, no delays,  
Smooth operations  
No financial losses  
An accurate workforce is present in the organisation

## **Risk Identification:**

Preparing a statement of risk necessitates considering the cause, impact, and effect on the overarching objective. This overall approach ensures a thorough understanding of the risk associated. Risks should be identified at a level that enables the specific impact to be clearly discerned and facilitates the determination of effective actions to address the risk. This detailed identification process ensures an understanding of the potential consequences and allows for targeted risk mitigation strategies.

Upon identification, risks should be promptly assigned to an owner who is responsible for overseeing the proper Management and ongoing monitoring of the risk. This ownership ensures accountability and proactively addresses and mitigates the identified risks throughout their lifecycle.

## **Risk Measurement**

The recording of the risk assessment exercise is critical within IIMT Studies' risk management framework.

Usually, the big risk (raw/uncontrolled risk) is already reduced to some extent by certain actions. So, instead of looking at the original risk, the assessment looks at the *remaining* risk (residual risk) after those actions. The focus is on checking how well the current controls are working.

When checking the remaining risk (residual risk), we look at how well the current controls are working. They might be:

- Fully effective
- Effective
- Adequate but needs some improvement
- Inadequate

This step is very important because it shows how strong the controls really are. After that, the risks are also judged based on **how serious the impact could be** and **how likely they are to happen**.

This full check helps in understanding both the strength of the controls and the seriousness of the risks. It gives a clear base for making smart decisions in the next steps of risk management.

## **Risk Assessment:**

A risk assessment is a systematic and scientific stepwise process carried out by an expert who is competent and experienced to :

- Identify
- Analyse
- Evaluate
- Control

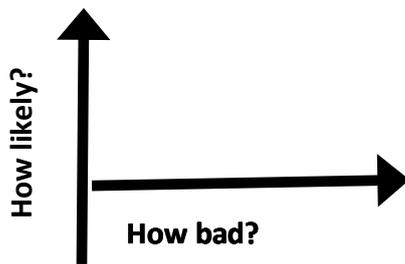
- Prioritise
- Eliminate various types of existing or potential risks/hazards and evaluate their probable impact on an organisation/institution/stakeholders.

During the assessment process, two major factors are considered for the evaluation of risk:

1. Likelihood
2. Severity

This helps the organisation in prioritising risks based on the above two.

### Where do our risks fit on the spectrum?



### Risk Process:

**Risk Analysis:** It's a stepwise process, aimed at tracing/tracking and analysing various kinds of potential hazards/risks/concerns that may have a detrimental impact on the business. Risk analysis is a continuous process.

**Risk communication** is the next step in the process of Risk Assessment and Risk Analysis. It's the process of sharing information with all stakeholders and taking their feedback/inputs/views. It's an important process as Risk Communication creates accountability as well as awareness amongst all stakeholders, leading to the ownership to fight the risks.

**Action Planning:** Following the identification and assessment of each risk, a detailed action plan is recorded on the risk register. For example, if the risk is a key employee departure, the action plan might include talent retention strategies and succession planning.

**Treating or Controlling Risk:** Risks can usually be reduced to an acceptable level by incorporating control mechanisms into daily operations. For instance, if the risk is a data breach, implementing stringent cybersecurity measures and employee training can help control and minimise the risk without disrupting daily operations.

**Transferring or Sharing Risk:** The Board of Governors plays a critical role in the transference of risks. If a risk is transferred, documenting the method and recipient of the transfer is a must, although certain risks, like reputation, may be untransferable. For example, if there is a risk of financial loss due to market fluctuations, transferring the risk through financial instruments like hedging may be considered.

**Tolerating or Accepting Risk:** Identifying, understanding, and acknowledging risks that are tolerated or accepted is important. This option involves the development of contingency

Plans to manage the impact if the risk materialises. For example, if there is a risk of a product recall, accepting the risk may involve having a robust recall plan and customer communication strategy in place.

**Terminating or Avoiding Risk:** In situations where a risk cannot be adequately controlled or transferred, and the risk level is unacceptable, the only viable course of action may be to eliminate the risk by discontinuing all or part of a particular activity. For instance, if a product poses a significant safety risk and cannot be brought up to safety standards, the organisation might decide to terminate its production.

**Risk Owners:** Every Risk must have a designated owner responsible for ensuring the identified control or mitigation action is implemented. Typically, the owner is someone who would bear the consequences if the risk materialises. Regular reporting on progress in managing the risk is expected from the owner. For example, if the risk is a potential regulatory violation, the compliance officer may be the designated owner responsible for implementing and overseeing compliance measures.

Infrastructural and IT resources:

Risk Assessment is critical for IIMT Studies as an awarding organisation. These resources decide and have a direct impact on:

- Development, Delivery and Award of Qualifications.
- Operations activities.
- Service deliveries.
- Communication and connecting with stakeholders and business associates.
- Documentation management and MIS are critical for business activities.
- Support in the Management of all resources.

The absolute/critical risk identification can also be found in the Business Continuity Plan.

Considering the above, IIMT Studies ensure that the following mitigations are put in place:

- Highly advanced and technically efficient infrastructure and equipment are in place.
- Highly competent professionals are engaged to take care of and look after important resources.
- The resources are upgraded and updated, keeping the next five years' requirements in mind.
- Alternate plans are in place to ensure continuity of work in case of an emergency situation.
- Data back-up, MIS security and data protection are ensured as a part of the business continuity plan.

Identifying and listing down all possible threats/risks to the key critical resources, as mentioned above.

**Review and Monitoring:**

The responsibility for ensuring the presence of stringent and effective controls to manage risk lies with all staff involved in an operation. Early warnings must be clearly communicated to those responsible for taking corrective or preventive action and to the head of the department.

Risk management will consistently be a standing agenda item in management meetings, affirming its importance within the organisational framework.

An annual review of the Risk Register and Action Plan will assess the Management of all levels of risks from the previous year. The review, reporting by exception, will form part of the recommendations for the subsequent period. This includes:

- Evaluation of controls that either failed or exhibited exceptional success during the year, accompanied by an in-depth analysis of the reasons behind such outcomes.
- Scrutiny of unforeseen risks, delving into why they occurred and why they were not anticipated.
- Assessment of changes in the external environment that have altered the risk profile.
- Analysis of changes in the internal environment influencing the risk profile.
- Identification of risks expected to emerge during the following year.

**Training and Development:** To ensure the effective implementation of the Risk Management Policy and Procedures, regular awareness training and skills development will be conducted for all staff members. These training sessions will be recorded as evidence for regulatory agencies, ensuring the commitment to ongoing staff development in risk management practices.

### **Risk Management Responsibilities**

The Board of Governors ensures the implementation of suitable risk management policies, taking decisive action to mitigate key risks. They provide direction and guidance to all relevant managers and officers within IIMT Studies.

IIMT Studies has developed key processes for effective governance as well as effective business operations and ensured that:

- Every process has a review date and a review committee
- Every process has a Process Owner whose key accountability is to ensure not only process compliance but also a process review at a regular interval.
- An Approver of each process whose responsibility is to ensure compliance, review and effective coverage of all possible parameters in that process.
- Inbuilt checks and controls in every process.

The Management team is required to ensure that all risks within their respective areas of responsibility are appropriately managed. They also coordinate actions on risks that impact multiple areas of responsibility.

### **Role of the Board of Governors**

The Executive ensures the implementation of suitable risk management policies and takes actions to mitigate the key risks facing IIMT Studies. They provide direction and guidance to all relevant managers and officers.

Department Heads are responsible for ensuring the appropriate Management of risks within their respective areas. They also coordinate actions on risks that affect multiple areas of responsibility. In cases where risks cannot be managed within a specific department, the Board of Governors provides direction on IIMT Studies' approach to responding to the risk.

### **Evaluating Risks**

Risks are assessed based on the frequency of occurrence and their potential impact on the strategic aims and objectives of IIMT Studies should they materialise.

### **Risk Registers**

IIMT Studies maintains a Risk Register to effectively manage the risk process. The register records details of each risk, including:

- a) Risk ID
- b) Risk location/Category – Financial, Centres, Operations, third parties, etc.
- c) Risk Manager/Owner
- d) Date entered and logged
- e) Actions taken

This systematic approach ensures transparency and accountability in managing risks across the organisation.

### **Risk committee:**

IIMT Studies team of the Risk Mitigation Committee regularly meets and ensures to check all possibilities of risk associated with the business, and reports to the Board of Governors. The risk criteria to look at are:

- Risk register
- Overall business operations
- Revenue receipts as to the business forecast
- List of noncompliance within the organisation
- List of noncompliance within recognised centres/third-party
- Business plan achievements as forecasted
- IT infrastructure and its functioning
- Third-party contracts and delivery
- Conflict of Interest within the organisation
- Conflict of Interest outside of the organisation
- Recruitment strategy and workforce strength
- Updates on the conditions of recognition
- Adverse events registered
- Policy review

The Head of Compliance reports to the Risk Committee.

### **Role of Risk Review Committee :**

This committee remains available all the time in the organisation, and the role of the committee is:

- Review recommendations, observations, suggestions, inputs and proposals related to risks and threats to business, put forward by all stakeholders, including employees, business associates, process owners, consultants, advisors and governing body members.
- To appoint external expert resources with the expertise and competencies in the various functional areas related to business and proactively work on their tips, market-economic, economic-political-social predictions and inputs to avoid, manage and mitigate risks.
- To keep alternative resources for all key critical functions and disciplines readily available to thwart any risk situation at any point in time.
- To create a positive and healthy environment and an efficient, productive work culture to enhance commitment, morale and output at each level amongst all stakeholders and business associates.
- To ensure optimum utilisation- maintenance-up-gradation of all resources – internal as well as external to carry out all business activities to achieve all end objectives and goals.

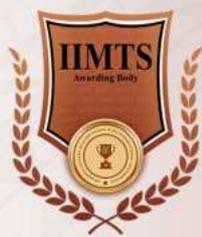
To continuously remain active and ensure :

- Proper growth-oriented revenue budget
- Ethical business practices
- Law-abiding and compliant work culture
- Fair and customer-friendly yet compliant policies to conditions of recognition and processes to ensure a positive brand image to promote and expand business growth

### **Roles & Responsibilities:**

**The Process Owner:** The department head is responsible for regular reviews of operations, compliance and execution to evaluate and assess any risk being observed and report to the Head of Compliance.

**Responsible Officer, also a Risk Manager:** Apart from a regular review of operations, compliance and execution to evaluate and assess any risk being observed or projected by the head of the department, the Responsible Officer will convene a regular meeting o in every six months, in a financial year along with the Risk Review Committee members, to invite views, opinions, suggestions and apprehensions on any risk which is visible in the near future or existing. Analysing upcoming changes in economic, political, social, technological and industrial sectors and keeping the Risk Review Committee in the loop at all times.



**IIMTS**  
Awarding Body

**Address** \_\_

IIMT Studies LTD  
Havelock Hub  
14 Havelock Place  
Harrow  
HA1 1LJ  
United Kingdom

**Call us on** \_\_

+44 7466650066

**Email us on** \_\_

info@iimtsab.co.uk

[www.iimtsab.co.uk](http://www.iimtsab.co.uk)