

IITA RISK APPETITE

RISK APPETITE STATEMENTS FOR IDENTIFIED RISKS

IITA Risk Management Committee

CONTENTS

- Definition of Risk Appetite
- Guideline for developing the Risk Appetite Statement
- IITA Risk Appetite Statements

DEFINITION OF RISK APPETITE

The concept of risk appetite embraces:

1. The level of exposure which is considered tolerable and justifiable should it be realized (when considering threats).
2. How much one is prepared to actively put at risk to obtain the benefits of the opportunity (when considering opportunities).

In either case the **risk appetite is best expressed as a series of boundaries**, appropriately authorized by management, which gives each level of the organization clear guidance on the limits of risk which can be taken, whether the consideration is of a threat and the cost of control, or of an opportunity and the costs of trying to exploit it.

This means that risk appetite can be expressed in the same terms as in assessing risk. An organization's risk appetite is not necessarily static; in particular, the Board will have freedom to vary the amount of risk which it is prepared to take depending on the circumstances at the time.

It should be noted that some risk is unavoidable, and it is not within the ability of the organization to completely manage it to a tolerable level – for example, many organizations have to accept that there is a risk arising from terrorist activity which they cannot control. In these cases, the organization needs to make *contingency plans*.

- From Orange Book of Risk Management

RISK APPETITE STATEMENT DEVELOPMENT GUIDELINES

- Risk appetite needs to be **measurable**
- Risk appetite is **not a single, fixed concept**.
- Risk appetite should be developed in the context of an organization's **risk management capability**
- The organization's risk management capability is a function of its risk capacity and **risk management maturity**
- Risk appetite must take into account differing views at a **strategic, tactical** and **operational** level
- Risk appetite must be **integrated** with the control culture of the organization

RISK APPETITE STATEMENTS

Risk Category	Risk Description	Risk Appetite
		Desired level of risk exposure
<ul style="list-style-type: none"> Project development & contractual 	<ul style="list-style-type: none"> - Performance of project leads to development partner's withdrawal of funds - Poor project execution due to delay in release of funds and partners' inability to: <ol style="list-style-type: none"> comply with contractual obligations deliver on assigned task separate project funds from other funds demonstrate commitment and be more engaged 	<p>Projects performing below 95% of agreed milestones are placed on watch list.</p> <p>Funds released to within 30 days of signing agreement with partners.</p>
<ul style="list-style-type: none"> Loss of bioresources 	<ul style="list-style-type: none"> - Non-attainment of project deliverables due to loss of R4D resources, such as farm trials, soil and plant samples or germplasm, microbial collections, pests, diseases, and farm destruction by animals 	<p>Not more than 20% loss of: field trials, plant samples, germplasm, etc.</p>
<ul style="list-style-type: none"> Resource mobilization 	<ul style="list-style-type: none"> - Operational disruption arising from overdependence on resources from a few core donors 	<p>50% of total project portfolio should not be from one development partner/donor.</p>
<ul style="list-style-type: none"> Finance & controls 	<ul style="list-style-type: none"> - Loss of liquid asset (Investment risk) - Loss of outstanding payments from donors (Receivable risk) 	<ul style="list-style-type: none"> - Not more than 0.05% loss on investment - Not more than 10% loss of donor receivables in a year.
<ul style="list-style-type: none"> Information & communication technology (ICT) 	<ul style="list-style-type: none"> - Loss of critical data due to failure of ICT system and policies - Data security is compromised and loss of sensitive information 	<p>100% of critical Institute data is fully backed up.</p> <p>Zero loss of sensitive information.</p>

<ul style="list-style-type: none"> Human capital 	<ul style="list-style-type: none"> - Non-adaptation of generic HR policies to local laws - Non-specification of which legal jurisdiction applies to individual international staff contracts - Exit of essential staff / staff turnover - Human and financial loss due to occupational hazard - Non-compliance with recruitment guidelines. - Employment of temporary staff in key NRS positions and Institute's vulnerable points - Non-adherence to Institute's compensation philosophy 	<ul style="list-style-type: none"> - At least 95% of HR NRS policy in all stations should be "domesticated" in line with host country labor laws. - Zero number of new and renewed IRS contracts without a jurisdiction clause. - Not more than 10% of essential staff leaving per annum. Not more than 10 incidents of non-compliance to safety standards by units/projects in the whole of IITA reported per month. - Zero incident of non-compliance with recruitment guidelines. - Zero occurrence of employment of short-term/temporary staff in key NRS positions. - Not more than 20% deviation from the chosen salary percentile.
<ul style="list-style-type: none"> Political & others 	<ul style="list-style-type: none"> - Operational disruption due to political unrest, insecurity, riots. - Station/campus vulnerability due to inadequate security infrastructure. 	<ul style="list-style-type: none"> - Temporary closure of stations should not be more than 3 months. - No international staff deployed where reports by security agents of host country indicates a significant level of threats.
<ul style="list-style-type: none"> Management/Administration 	<ul style="list-style-type: none"> - Poor management of change process which the Institute goes through almost every 4 years leaves room for speculation and confusion/blurring of roles - Crisis of cohesion in the Management Team (MT) - Strategic direction from the Board <ul style="list-style-type: none"> - Crisis of learning and accountability 	<p>More than 25% of Staff Satisfaction Survey respondents indicating job insecurity</p> <p>Not more than 2 instances of Management team inability to reach a consensus per quarter</p>

<ul style="list-style-type: none"> Critical infrastructure 	<ul style="list-style-type: none"> - Productivity loss due to infrastructural failure, i.e., prolonged power failure, breakdown of air conditioners, water treatment plant, laboratory equipment, road accidents, inadequate office/lab accommodation, loss of vehicles, destruction of screen/glasshouse, malfunction of old equipment, and natural disaster 	<ul style="list-style-type: none"> - For stations that have laboratories which require 24 hours of electric power, power failure from national grid and generated power combined should not exceed 5 hours. - Water supply should not be disrupted for more than 1 day. - -Not more than 12 demerit points accumulated within a 3 year contract period per driver
<ul style="list-style-type: none"> Supply chain 	<ul style="list-style-type: none"> - Operational disruption due to challenges of supply chain system, i.e., Lack of procurement plan, Delayed delivery of imported goods, Scarcity of needed supplies, High cost and low quality of essential resources, and Late payment of suppliers 	<ul style="list-style-type: none"> - Purchases made locally should be delivered within 1 week of request. - Purchases made internationally should be delivered within 6 months after purchase was made. This should include all necessary approvals as required by host country. - 70% of recurrently used items should be included in yearly procurement plan.
<ul style="list-style-type: none"> Operational/Reputation/Legal 	<ul style="list-style-type: none"> - Complications arising from unaligned and changing operational model in certain units, i.e., Poor planning from programming unit and changing prices of supplies - Control of risk in stations outside HQ - Potential reputational risk due to genetically modified organism (GMO) protest, chemical spillage, improper handling of waste, etc. <ul style="list-style-type: none"> - Loss of reputation due to non-compliance with regulatory laws - Reputational risk arising from evolving linkages among Research, Development, and business - Loss of assets due to robbery, theft, or accident by stakeholders 	<ul style="list-style-type: none"> - - All stations/hubs should have an updated risk register. - All stations/hubs should have an updated risk register. - Not more than 3 proven incidences of reputational risks related to this interrelationship R4D, P4D AND BIP per annum -Not more than one reported incidence of assets loss by stakeholder within a fiscal year. - 0.05% of media reports about the Institute, related to an issue is unfavorable. 0.05% of media reports about the Institute, related to an issue is unfavorable. - Zero tolerance.

	- Unauthorized use of Intellectual Property	<ul style="list-style-type: none"> - -. - - Zero occurrence of unauthorized use of Intellectual Property during the fiscal year or project life span
<ul style="list-style-type: none"> • Security 	- Station/campus vulnerability due to inadequate security infrastructure, i.e., inefficient profiling at the gate,	- 100% access control at all stations/hubs.