IETF LLC Risk Management Policy

Objectives

IETF Administration LLC (“IETF LLC”) practices good governance and recognizes that risk management is an essential component that supports the achievement of its strategic objectives. This policy establishes a shared responsibility for effective risk management throughout the IETF LLC by providing a risk management framework that ensures all significant risks associated with IETF LLC’s strategic objectives are effectively identified, assessed, and managed.

IETF LLC’s risk management objectives are to:

- Develop a "risk aware" culture that encourages personnel to identify risks and opportunities in a planned and coordinated manner and to respond to them with cost effective actions; and
- Provide assurance to the IETF community, IETF leadership, the Internet Society (ISOC), and broader stakeholders that an effective risk management program is in place.

Scope

This policy applies to all management, staff, and others employed by IETF LLC from time to time. It covers functions performed internally as well as those operated by external organizations under contract to IETF LLC.

Definitions

Risk: Risk is the effect of uncertainty on an objective where that effect may be a negative or positive impact on that objective.

Risk Management: Coordinated activities to direct and control an organization with regard to risk.

Impact: Impact of an event that affects the objectives. For this policy this is implemented as a measure of the severity of the impact.

Likelihood: Chance of something happening. For this policy this is implemented as a defined measure of that chance.

Responsibilities

Every person in IETF LLC has a role to play in ensuring that risks are managed, opportunities are taken, and objectives are met. Specific roles and responsibilities are set out in the table below.

	Roles / Responsibilities
The Board (and / or designated board committee)	• Approving and endorsing IETF LLC's risk management policy, and any proposed changes to it; • Approving IETF LLC's risk appetite and risk tolerance, and any changes to them; • Monitoring compliance with the risk management policy; • Provision of suitable capacity and capability to manage the Risks; and • Delegating operational authority to management, where appropriate.
Executive Director (ED)	• Accountable to the Board and other key stakeholders for the identification and effective management of strategic, operational, and project risks across IETF LLC.
Management / Staff / Contractors	• Assessing, managing, monitoring, and reporting risk to the ED for activities within their control.

Framework for Managing Risk

General Process

The general process for managing risk mirrors global best practice as set out in ISO 31000[1]:

Risk Definitions

Risk definitions, in terms of impact and likelihood, are required to ensure that risks can be consistently assessed and risk mitigation appropriate to the risk impact/likelihood can be identified. The two tables below provide definitions of impact and likelihood.

[1]ISO Standard No. 31000:2018 https://www.iso.org/standard/65694.html

Risk impact is defined as follows:

Factor	Insignificant	Minor	Moderate	Major	Extreme
IETF Work	IETF is unable to maintain any more than 95% of its normal work level.	IETF is unable to maintain any more than 90% of its normal work level.	IETF is unable to maintain any more than 80% of its normal work level.	IETF is unable to maintain any more than 60% of its normal work level.	IETF is unable to maintain any more than 40% of its normal work level.
Finances	Less than $50,000 financial impact on performance of the organization within one year.	Between $50,000 to $250,000 financial impact on performance of the organization within one year.	Between $250,000 and $2,000,000 financial impact on performance of the organization within one year.	Between $2,000,000 to $10,000,000 financial impact on performance of the organization within one year.	Greater than $10,000,000 financial impact on performance of the organization within one year.
Services	Unavailable or degraded services restored with minimal impact on the work of the IETF.	Unavailable or degraded services restored with minor impact on work of the IETF. Recoverable data loss or corruption with minimal impact on work of the IETF.	Unavailable or degraded services restored after a notable impact on the work of the IETF. Recoverable data loss or corruption with minor disruption to work of the IETF.	Unavailable or degraded services restored after a serious impact on the work of the IETF. Recoverable data loss or corruption resulting in serious disruption to the work of the IETF.	One or more key systems unavailable and deemed unrestorable. Serious and permanent data loss or corruption.
Meetings	Health and safety incident with no injuries and no loss of work hours.	Incident(s) requiring minor medical treatment and/or loss of work hours. IETF Meeting trivially disrupted.	Incident(s) requiring non-minor medical treatment. IETF Meeting notably disrupted.	Incident(s) with life-threatening injuries. IETF meeting canceled or abandoned.	Incident(s) leading to loss of life. Series of IETF meetings canceled or abandoned.

Factor	Insignificant	Minor	Moderate	Major	Extreme
Reputation	Minor grumblings in the media[2].	One-off negative media coverage.	Sustained negative media coverage and perception.	Relentless/sustained reputation issue leading to major degradation of confidence in the IETF.	Complete loss of public confidence in the IETF.
Legal	Subpoenas for information for third-party litigation.	Staff or key contractors formally deposed in third party legal action. Minor litigation, such as debt collection.	Audit by a government department. Significant contractual disagreement with potential for litigation. Litigation but largely handled by counsel.	Litigation requiring substantial board and ED resources. Formal criminal investigation. Significant regulator fine or court award.	Litigation with ISOC. Regulator or court action that shuts down the IETF or IETF LLC permanently or for an extended period.
Community	Minor disagreements between IETF LLC and ISOC, IETF Leadership or IETF participants. Community discord has negligible impact on IETF LLC.	Relationship issues between IETF LLC and ISOC, IETF Leadership or IETF participants lead to unexpected delays and/or costs for major decisions. Community discord serious enough for IETF Leadership to require IETF LLC support.	Degraded trust and/or cooperation between IETF LLC and one or more of ISOC, IETF Leadership, and IETF participants. Extensive community discord requiring IETF Leadership to seek ongoing IETF LLC support.	Breakdown in trust and/or cooperation between IETF LLC and one or more of ISOC, IETF Leadership, and IETF participants. Key people (board or ED) recalled, replaced or forced to resign by appointing bodies. IETF LLC significantly distracted supporting IETF Leadership in dealing with extensive community discord.	Community deems IETF LLC as no longer suitable to be the support organization for the IETF. ISOC takes control of IETF LLC.

[2] Includes individuals on social media, influencers, vloggers, etc as well as traditional media.

Factor	Insignificant	Minor	Moderate	Major	Extreme
Suppliers	Issues with one or more key suppliers with negligible impact on their service.	Degraded service from one key supplier.	Major disruption to service from one key supplier, or degraded services from multiple key suppliers.	Complete loss of their service from one key supplier, or major disruption to services from multiple key suppliers.	Complete loss of service from multiple key suppliers.
Staff	Minor health issues, stress or dissatisfaction	Significant health issues, stress or dissatisfaction affecting one staff member. One staff member leaves without notice.	Significant health issues, stress or dissatisfaction affecting multiple staff. One executive or 2 staff members depart without notice.	Majority of staff voice serious dissatisfaction. Multiple executives and/or staff depart without notice.	Majority of staff leave without notice

Risk likelihood is defined as follows:

Descriptor	Description
Almost Certain	The event could occur in most circumstances, e.g. 80% chance of occurring in the next 12 months
Likely	The event will probably occur in most circumstances, e.g. 60-79% chance of occurring in the next 12 months
Possible	The event should occur at some time, 30-59% chance of occurring in the next 12 months
Unlikely	The event could occur at some time, e.g. 5-29% chance of occurring in the next 12 months
Rare	The event may occur only in exceptional circumstances, e.g. less than 5% chance of occurring in the next 12 months

Risk Assessment

Risk assessment is designed to practically support the IETF LLC to achieve key objectives, rather than be used solely as a compliance exercise by ensuring that:

- All risks are detailed, explained, and communicated.
- Existing and planned mitigations and the responsibility for those are recorded.
- The Board defines the risk tolerance for the organization and this is then implemented in the risk assessment.
- The progress of risk management is measured and documented.

Risk Ratings

Risk definitions are used to rate their impact and likelihood to provide an overall risk rating, and to compare different risks with different impacts, using the following matrix:

	Impact				
Likelihood	Insignificant	Minor	Moderate	Major	Extreme
Almost certain	High	High	Critical	Critical	Critical
Likely	Medium	High	High	Critical	Critical
Possible	Low	Medium	High	High	Critical
Unlikely	Low	Low	Medium	High	Critical
Rare	Low	Low	Medium	High	High

Risk Tolerance

A formal risk tolerance is established to set agreed criteria for assessing risks and the level of risk that can be tolerated to achieve the organization's strategic objectives.

As depicted in the risk rating table above, the risk tolerance is expressed in terms of four risk rating zones:

- **Low (Green) and Medium (Yellow) zones**. Risks within these zones are automatically tolerated.
- **High (Orange) zone**. Some of these risks may be tolerated, where additional treatment is not cost justified, in return for specified benefits.

- **Critical (Red) zone**. Generally these risks are not tolerated, and an immediate mitigation is required.

Reporting and Review

The ED will provide an annual report to the Board for residual Critical and High-Level risks that includes:

- Risk Matrix
- Risk Register
- Risk Analysis and Evaluation

The ED will specifically note any key information that requires the attention of the Board following the risk assessment. This is likely to include:

- Identification of new risks and mitigation of prior risks reported;
- Risks that have changed (i.e. increased/decreased from high to critical, low to moderate, etc.); and
- Identification of key groups of risks and the broad controls in place for these.