

认证风险管理程序（BGFC-PF-17）

1 目的

为了确保绿林管理体系及其每一个过程和认证活动中都能考虑到相关的风险，该风险管理程序规定了实施风险识别、分析和评价的准则、方法、程序和管理要求。

2 适用范围

本程序适用于 BGFC 所有认证业务的风险管理。

3 职责

- 3.1 管理层制定风险管理程序文件并建立风险管理委员会；
- 3.2 管理者代表组织风险管理委员会负责识别、分析和评价 BGFC 的风险；
- 3.3 BGFC 所有员工承担减少和降低风险的责任。

4 原则

风险管理的目的是创造和保护价值，提升绩效，并鼓励创新和支持实现目标。有效的风险管理应包括整合的、结构化和综合性、定制化、包容性、动态的、最佳可利用的信息、人员和文化因素和持续改进。

5 要求

1.1 概述

建立风险管理程序是为了把风险管理整合到 BGFC 整个活动和职责中，与现有的管理体系相互融合。

1.2 领导力和承诺

高级管理层和风险管理委员会，为了确保风险管理被整合到所有组织活动中，在 BGFC 质量管理体系的 0.3 公正性声明及相关承诺章节中分别做了相应的承诺。

1.3 整合

风险需要在组织架构中的每一个部分都得到管理，在组织中的每一个人都对风险管理负责。BGFC 从最高管理层到风险管理委员会，再到每个部门的每个员工，对 BGFC 的所有活动都保持风险意识。

风险管理整合到组织中是一个动态的，迭代的过程，应根据绿林自己的需求和文化进行定制，让风险管理作为组织的一部分，而不是从组织的目的、治理、领导力和承诺、战略、目标和运作中分离。

1.4 设计

1.4.1 组织环境

绿林的外部环境，包括但不限于：

- a) 中国对木材行业的政策；
- b) 木制品行业的发展；
- c) 国际上对环保政策的倾向；
- d) 外部利益相关方的关系、认知、价值、需求和期望；
- e) 与客户的合同关系和承诺；
- f) 外包方的关系等。

绿林的内部环境，包括但不限于：

- a) 绿林愿景、使命和价值观；
- b) 组织结构、职责；
- c) 战略、目标和管理方法；
- d) 绿林内部的企业文化；
- e) 人员的能力，在资源和知识方面的理解；
- f) 数据和信息系统的安全性；

g) 与内部员工的关系；

h) 员工劳动合同关系和承诺等。

1.4.2 明确风险管理的承诺

详见 5.2.

1.4.3 分配组织角色、权力、职责和责任

专门成立《风险管理委员会》，由管理体系代表负责，并明确该委员会的职责和 BGFC 每个员工在风险管理过程中应该承担的责任和权利。

1.4.4 分配资源

组织应确保风险管理的资源，包括但不限于：

- a) 足够的人员和技能、保证其有经验和能力完成相应的工作，专门建立：
认证人员聘用管理流程、人员能力准则管理程序、认证人员培训管理程序
和认证人员能力评价管理程序；
- b) 建立一套完善的风险管理程序文件，明确管理过程，形成文件化的程序；
- c) 保持整个风险管理过程中的记录；
- d) 给予有关人员专业的培训并制定其相应的发展需求。

1.4.5 建立沟通和咨询

通过绿林官方网站与外部环境建立联系，通过绿林成立的风险管理委员会与内部环境建立联系，同时风险管理委员会需要对内外部环境产生的风险进行识别、分析和评估，从而制定进一步的实施方案和持续改进的方法。

6 风险管理程序

6.1 内外部环境的确定

绿林应在所运作的外部 and 内部环境的理解基础上，建立风险管理过程中的外部和内部环境，见 5.4.1.

6.2 风险的评价准则

绿林应明确与目标相关的接受或不接受的风险数量和类型，并定义风险准则，以便于评价重大风险和支持决策过程。制定风险准则，应考虑以上因素：

- a) 不确定的本质和类型影响结果和目标（有形的和无形的）；
- b) 如何来定义和衡量结果（积极和消极的）和可性能；
- c) 与时间相关的因素；
- d) 所应用衡量标准的一致性；
- e) 如何确定风险等级；
- f) 考虑多种的风险组合和顺序；
- g) 组织的能力（风险容量）。

6.2 风险的识别

为了发现、识别和描述有可能帮助或阻碍组织实现目标的风险，相关的、恰当的和最新的信息对识别风险非常重要。识别风险时，应考虑因素：有形和无形的风险源；原因和事件；威胁和机会；缺陷和能力；内外部环境的变化；突发风险的指标；资产和资源的本质和价值；结果以及对目标的影响；知识的局限性和信息的可靠性；时间相关的因素以及所涉及的偏见、假设和信念。

绿林应识别风险，不论他们来源是否可控，都应该考虑多种来源可能导致各种有形或无形的后果。

6.3 风险的分析

绿林应对识别出来的风险进行分析，风险的分析是为了理解风险的性质和特征，包括适当的风险等级。风险分析需要考虑：不确定性、风险源、后果及其本质和大小、可能性、复杂性和关联性、和时间相关的因素和变动性、敏感性和置信水平、事件、场景、控制及其有效性。

风险分析受分歧意见、偏见、风险观念和不同判断的影响。另外，还受到所利用信息的质量，假设、例外、技术的局限性以及如何应用这些技术的影响，这

些影响必须考虑在内，形成文件和决策者进行交流。

高度不确定的试件可能很难量化，当分析有可能有几个结果的事件的时候，这是一个问题，用综合的技术通常能提供更大的视角。

风险分析是风险评价的输入，用以确定风险是否需要应对以及用合适的风险应对战略和方法处理，这个分析结果为决策提供依据，在什么情况下，这些选择涉及不同类型和等级的风险。

6.4 风险的评价

绿林对识别出来的风险进行分析后，进而对其评价，以便以后做出相应决策。风险评价包括风险分析结果与制定的风险准则的比较以决定在什么情况下必须有进一步采取行动，可能的决策包括：

- （1） 不需要进一步采取行动；
- （2） 考虑风险应对方案；
- （3） 进一步分析以更好地理解风险；
- （4） 维持现有的控制；
- （5） 重新考虑目标。

风险评估的结果应该被记录、沟通，然后在绿林相应的管理层得到确认。

6.5 风险的应对

对评价后的风险应制定和选择应对风险的方案，进而采取实施行动，然后评估应对的效果，最后决定剩余的风险是否可以接受，如果不能接受，应采取进一步应对措施。

6.6.1 风险应对方案的选择

选择最适合的风险应对方案要平衡潜在的收益与为达目的所支付的成本和实施的弊端。风险应对方案并非相互独立或适用于所有情况，包括以下一个或多个：

- (1) 规避风险，通过决定不让产生风险的活动开始或继续；
- (2) 为追求机会接受或增加风险；
- (3) 消除风险源；
- (4) 改变可能性；
- (5) 改变结果；
- (6) 分担风险（如：通过合同，购买风险）；
- (7) 通过知情的决策来保留风险。

风险应对的理由不只是单独从经济考虑，而是应把所有的组织义务、自愿承诺和相关利益者的观念考虑在内，方案的选择应该和组织的目标、风险准则和可利用的资源相一致，并且应考虑利益相关者的参与和与他们的沟通和协商最合适的方式，这样的话，有些应对方案更容易被利益相关者接受。

虽然风险应对方案很认真地在设计和实施，但有可能达不到预期的结果或者产生不确定的后果，所以每年应进行一次监督评审，识别新的风险或者确保应对方案的实施效果或不同形式的应对方案的可行性。

如果没有合适的应对方案，或者应对方案不能显著改变风险，该风险应被记录并保持持续的检查。绿林和其它利益相关者应知道风险应对后剩余风险的本质和范围。剩余风险应该被记录并接受监督检查，如适当，应进一步应对。

6.6.1 风险应对方案的实施

风险应对方案选定后，就要具体实施。应对计划应正和到绿林的管理计划和过程中，与适当的利益相关者协商。应对计划应包括：

- (1) 选择应对方案的理由，包括预期的收益；
- (2) 负责批准和实施该计划的人（权利、职责）；
- (3) 提议的行动；
- (4) 所需的资源，包括应急；

- (5) 绩效测量;
- (6) 约束条件;
- (7) 要求的报告和监督;
- (8) 预计行动的采取和完成时间。

6.7 监督和检查

BGFC 应对风险管理过程及其结果应进行每年一次的持续监督评审，包括计划、收集和分析信息，并记录结果和反馈信息。

1.8 记录和报告

BGFC 应保留整个风险管理的过程和结果形成文件和报告。记录至少保持 5 年。

7 记录

BGFC-RF-31 风险评价准则

BGFC-RF-32 风险识别、分析和控制措施评估表

BGFC-RF-33 风险管理评估报告

BGFC-RF-34 公正性风险分析报告