## Risk Control Effectiveness Assessment Criteria

The effectiveness of current risk controls can be assessed using the criteria below.

Details of the Policy Assurance Compliance (PAC) model can be found in [this article on the essentials of auditing](https://www.juliantalbot.com/post/audit-reports-are-useful-but-auditing-is-essential).

| **Rating** | **Criteria** |
| --- | --- |
| 5. EFFECTIVE | * Controls are properly designed and operating as intended. Management activities are effective in managing and mitigating risks.   GUIDANCE FOR POLICY   * Policies and procedures are robust, up to date and have been through several iterations. * Relevant standards and guidelines have been identified or created. * The management framework is regularly reviewed, and any identified gaps are addressed within one review cycle. * Documentation supporting the management system is controlled with accountabilities and review dates specified.   GUIDANCE FOR ASSURANCE FRAMEWORKS ASSESSMENT   * Competency-based training is delivered is based on a comprehensive training program with >98% compliance. * Training delivery and assessment records are comprehensive and current for all staff, contractors, and visitors. * The training program is based on a current training needs analysis. * Business plans specify budget and resource requirements and are based on documented analysis. * Evidence shows that resources have been funded, and >98% are implemented within agreed timeframes. * Exercise and training cycles are fully documented and integrated with >98% compliance.   GUIDANCE FOR COMPLIANCE AND FEEDBACK MECHANISMS   * A structured audit plan addresses all elements of the management system. * Audit schedules are risk-based and completed in >98% compliance with the plan. * Recommendations from corrective action reports, audit findings and investigations are documented, and >98% of accepted actions are completed within agreed timeframes. * Systems are mature, and continuous improvement processes have been in place for several years of review cycles. |
| 4. LIMITED IMPROVEMENT. | * Limited improvement is needed. Controls and/or management activities are properly designed and operating somewhat effectively, with some opportunities for improvement identified.   POLICY   * Core policies and procedures are current and have been through at least one review. * Most procedures are supported by identified standards and guidelines. * The management framework is regularly reviewed and substantively complete. * Documentation supporting the management system is controlled with accountabilities and review dates specified.   GUIDANCE FOR ASSURANCE FRAMEWORKS ASSESSMENT   * Competency-based training and assessment is delivered in accordance with a comprehensive training program with >80% compliance. * The training program is based on a current training needs analysis. * Training records are current and comprehensive. * Business plans specify budget and resource requirements. * Evidence shows that resources have been funded, and most are in place. * Communication plans are documented.   COMPLIANCE AND FEEDBACK   * A structured audit plan addresses critical elements of the management system. * Audit schedules are risk-based and completed in >80% compliance with the plan. * Recommendations from corrective action reports, audit findings and investigations are documented, and >80% of accepted actions are completed within agreed timeframes. * Systems are mature and have been in place for at least two review cycles. |
| 3. SIGNIFICANT IMPROVEMENT | * Significant improvement is needed. Key controls and/or management activities in place, with significant opportunities for improvement, identified.   POLICY   * Management systems are in place but may be partially documented and inconsistently applied. * The management framework is in draft or incomplete. * The management system is incomplete or outdated, but plans are in place to develop policies, procedures, and guidelines to address these deficiencies. * Procedures and guidelines are in place but are not consistent in format or content across business areas.   ASSURANCE FRAMEWORKS   * Competency-based training is ad hoc or not fully documented. * The training program is based on a training needs analysis that is out of date or greater than three years old. * Business plans sometimes specify budget or resource requirements. * Evidence is available to show that some resources have been funded, and >60% are in place. * Communications are ad hoc, or plans are specified but compliance is <50%.   COMPLIANCE AND FEEDBACK   * An audit plan is evident but is not risk-based or does not address all areas. * Audit schedules are completed in >60% compliance with the plan. * More than 60% of corrective action reports, audit findings and investigations are completed within agreed timeframes. * Management systems may be new, but at least one review cycle has occurred with approved management systems and structures. |
| 2. INEFFECTIVE | * Limited controls and/or management activities are in place, high level of risk remains. Controls and/or management activities are designed and are somewhat ineffective in efficiently mitigating risk or driving efficiency.   POLICY   * Management systems are not documented in a coherent manner. * Action needs to be taken to review or update management documents of the framework. * Review cycles are specified but are not complied with.   ASSURANCE FRAMEWORKS   * Training is ad hoc, inconsistent, or not assessed. * Training records are incomplete. * Resources and budgets may be in place but are not documented in formal plans. * Management controls are not formally communicated.   COMPLIANCE AND FEEDBACK   * An audit plan is not evident or <60% compliance with plan. * Greater than 40% of continuous improvement activities (corrective action reports, audit findings, or investigations) are implemented within specified timeframes. * At least one review cycle has occurred with >80% of existing management systems and structures. |
| 1. HIGHLY INEFFECTIVE | * Controls and/or management activities are non-existent or have major deficiencies and do not operate as intended. Controls and/or management activities as designed are highly ineffective in efficiently mitigating risk or driving efficiency.   POLICY   * Management systems are not documented, remain in draft, or do not address the requirements of the indicator. * Management systems are reviewed but remain in draft for more than one review cycle. * Review cycles are not specified.   ASSURANCE FRAMEWORKS   * Evidence of assurance activities is limited or non-existent. * Training, capability, communication, or logistics activities are ad hoc or non-existent. * Training needs analysis is not evident. * Resourcing plans and budgets do not reflect requirements.   COMPLIANCE AND FEEDBACK   * Little or no evidence of continuous improvement. * Audits are ad hoc, limited in scope, or non-existent. * Feedback systems are not evident. * No review cycles are evident. |
| 1. UNKNOWN | * Insufficient information available to assess the effectiveness of this control. |

**Table:** Risk Control Effectiveness Assessment Criteria

[www.juliantalbot.com](http://www.juliantalbot.com) © 2022

Non-commercial use approved. This Item is protected by copyright and/or related rights. You are free to use this Item in any way that is permitted by the copyright and related rights legislation that applies to your use. In addition, no permission is required from the rights-holder(s) for non-commercial uses. For other uses you need to obtain permission from the rights-holder(s).

This table was extracted from a risk assessment exported from the SECTARA risk management platform (sign up for a free plan at <https://sectara.com/free-plan/>)