LogicManager

ERM Program Audit Guide: Risk Maturity Model

Assessing the Adequacy and Effectiveness of Risk Management

+1 617 530 1210 | logicmanager.com | info@logicmanager.com

©LogicManager, Inc.

Table of Contents

Introduction

The Institute of Internal Auditors (IIA), effective January 2013, has revised its International Professional Practices Framework (IPPF) to assess the effectiveness of enterprise-wide risk management programs. These mandated changes clarify Internal Audit's role in communicating risk and require auditors to validate the most timely and most significant risks, especially those that impact the achieving of the organization's strategic objectives.

Auditors need a method to assess the adequacy of the risk management program at their organizations. The IIA stresses that though existing IIA guidance is helpful, additional tools are needed because without a structure to assess where an organization is with respect to risk management, a CAE may have to rely too much on intuition.

What does enterprise risk management (ERM) effectiveness mean? Boards of Directors are now being held responsible for material, front line risks to their organization, despite their lack of involvement in the day-to-day running of the company where most operational risks occur. Boards must now leverage their risk oversight role to ensure that the risk management program's policies and procedures are effective at identifying material risks and demonstrating assurance of operational controls. Internal Audit fulfills a critical role in evaluating the effectiveness of an organization's framework, and ensuring policies and procedures are being followed as intended.

The Risk Maturity Model (RMM) for Enterprise Risk Management is a solution to help auditors evaluate the effectiveness of their organization's ERM program. The RMM is broken down into seven sections, each focusing on a different core attribute of ERM. These seven areas are further broken down into 25 success components and 71 competency drivers that show exactly where your ERM program stands on five levels of maturity, ranging from ad hoc to managed. To date, thousands of organizations have used the RMM to baseline their capabilities, and the connection between the RMM and better business performance is proven statistically.

Universal Framework

The Risk Maturity Model for ERM is not a standard, but rather an umbrella framework that measures organizations on their adoption of enterprise risk management (ERM) best practices from the most widely used risk management standards: ISO 31000, OCEG "Red Book", BS 31100, COSO, FERMA, SOLVENCY II and AS/NZS 4360:2004. The Risk Maturity Model for ERM is an effective evaluation tool regardless of which standard your organization has adopted, and solves the problem of how to evaluate the adoption of existing standards over time, and how to benchmark that adoption verses other organizations. It identifies the areas where your organization is weakest, as the weakest links are ultimately what drive down ERM program effectiveness.

About the Risk Maturity Model

LogicManager's Risk Maturity Model (RMM) has become the global standard for benchmarking the effectiveness of Enterprise Risk Management and is on the forefront of Enterprise Risk Management research on corporate governance. In 2008, the RMM scores were proven to be directly correlated to Standard and Poor's corporate credit rating. In 2014, The Journal of Risk and Insurance (JRI) published the research findings that an organization's scores on the Risk Maturity Model were directly correlated to a 25% market value premium due to its ability to provide evidence of mature risk management practices. Read more about LogicManager's Risk Maturity Model (RMM).

As of 2020, the Risk Maturity Model is now hosted and operating directly within LogicManager's application.

The Risk Maturity Model, available as a complimentary, automated tool on-line, will help you score your organization's Enterprise Risk Management program on 25 key components and their underlying competency drivers. You will receive a real-time, personalized benchmark report on your existing maturity level. Each of the five maturity levels includes specific and actionable recommendations to support your findings and develop an action plan to take your risk management program to the next level.

After completing the RMM, a summary report is automatically generated for your board on the state of your organization's ERM program. This report summarizes your organization's ability to manage risk effectively, broken down into seven attributes and 25 success drivers. Further, the summary provides a benchmarking index that shows you how your program compares to those of other organizations.

End Result: Meet the IIA Guidelines for Assessing the Adequacy and Effectiveness of Risk Management

- ✓ Determine if risks arising from business strategies and activities are identified and prioritized.
- ✓ Ascertain if management and the audit committee have determined the level of acceptable risk.
- ✓ Ensure there is a process by which controls are designed to reduce or manage risks to levels deemed acceptable by management and the audit committee.
- ✓ Periodically monitor and reassess the organization's risk and the effectiveness of controls to manage it.
- ✓ Ensure managers responsible for risk management periodically provide the audit committee with reports on results of the risk management program."

Risk Maturity Model Summary

- 25 ERM success components and 71 competency drivers that are mapped and benchmarked to ISO 31000: 2009; OCEG "Red Book" 2.0: 2009; BS 31000: 2008; COSO: 2004; FERMA: 2002; and Solvency II: 2012 risk standards.
- Analysis report covering the overall maturity of an organization's risk management program and by attribute.
- Quantitative risk maturity index that is directly linked to better business performance (i.e., greater stock value and better credit ratings).
- An Auditor's Guide on how to evaluate and verify the effectiveness of the organization's risk management programs (as is required by the IPPF).
- Detailed findings and potential recommendations, based on assessment results of an organization's risk program.
- Action plan to substantiate that an audit plan covers risks to achieving strategic objectives as outlined in the International Standards for the Professional Practice of Internal Auditing.

How Internal Auditors should Use the Risk Maturity Model

Internal Auditors should request that their ERM/GRC Manager complete the Risk Maturity Model and provide the self-assessment report to their Internal Audit department. This Maturity Level Summary Report can also be valuable to present to the Board. The Internal Audit department can use the following Internal Auditors Guide, and specifically the comments in the "Auditor's Notes" section, to determine if ERM Maturity is being measured effectively and accurately, according to best practices.

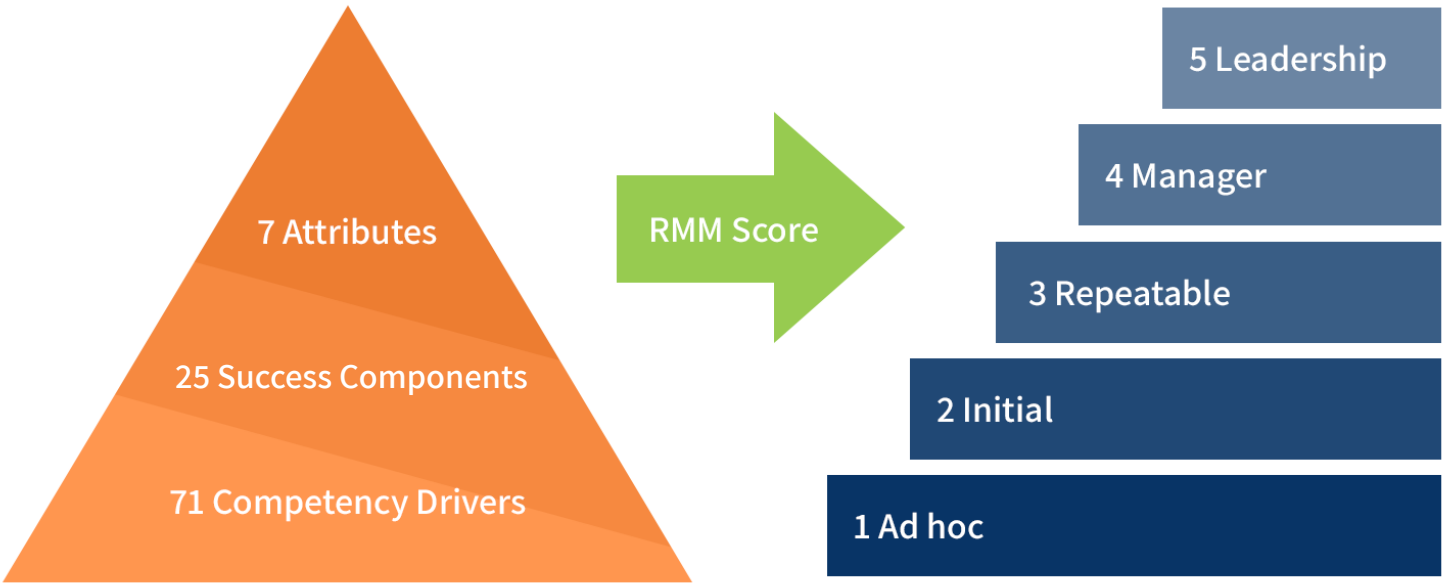
If the ERM program has existed for over a year, and the risk manager's score is ad hoc or initial, this is considered inadequate. Internal Audit should meet with the risk manager to discuss their plan for bringing the ERM Program to a repeatable, increased level of maturity. If the self-assessment is equal or greater than Repeatable, Internal Auditors should request the measures suggested in the Notes section of this Guide to fact check the validity and reasonableness of the self-assessment score, and generate findings when there is a discrepancy. The "Auditor's Notes" provide hard line, best practices of policies and procedures of advanced ERM programs. While initial or ad-hoc programs may lack much of the criteria, the notes represent what governing bodies will measure a program to, and in effect, the penalties they will levy in the event of risk manifestation.

ERM Compliance and Enforcement

Under the SEC Rule Proxy Disclosure Enhancements, in February 2010, Boards of Directors and companies in certain industries and geographies can be found negligent for having inadequate ERM programs or not knowing or accurately disclosing the state of their ERM Programs. Therefore, the Board of Directors must be informed of the state of risk management, even if the program is in the ad hoc or initial stage. ERM Programs in their 1st year of existence typically have the Initial maturity score.

Typically, the disclosure of having an immature risk management program with a demonstrable plan for improvement exempts or greatly reduces companies from penalties under the Federal Sentencing Guidelines and other regulatory actions. Reporting adequate risk management oversight when actual governance is inadequate, or not doing the due diligence to determine the adequacy of the risk management program, provides regulators and shareholders grounds for taking action.

To discuss this Guide or the Risk Maturity Model, please contact a LogicManager risk management specialist at: 617-649-1325 or email info@logicmanager.com.



Attribute 1: Adoption of ERM-Based Approach

Description: Degree of executive support within the corporate culture for an ERM-based approach to manage risks at all levels within the organization. Adoption of an ERM-based approach goes beyond regulatory compliance and extends across all processes, functions, business lines, roles and geographies.

Component: Business Process Definition and Risk Ownership

Competency Drivers:

- Are business areas, functions, and processes formally defined throughout the organization?
- Does each business area, function, and process identify their own risks in the context of a common risk language?
- Are risks reassessed and evaluated by business process owners on a recurring basis?
- Do business process owners reassess and evaluate their opportunities on a recurring frequency?
- Do business process owners use the results of risk assessments and monitoring in order to identify and act on areas for improvements?
- Are the risk issues face by the organization formally documented, escalated and prioritized for timely remediation?

Component: Frontline and Support Process Owner Participation

Competency Drivers:

- Are risk assessments conducted in all business areas?
- Are the relationships between issues and findings and their associated risks, controls, and monitoring activities explicit and well understood?

Component: Far-sighted Risk Management Vision

Competency Drivers:

- Do business areas create long-term action plans to meet risk management goals?

Component: Executive ERM Support

Competency Drivers:

- Does the organization promote accountability by having frontline management identify, own, assess, and revisit risks on a recurring basis?
- Are qualitative risk assessments required for every big project, new product, business model change, etc.?
- Is there recent, material, evidence of risk priorities made by the Risk Committee to the board that have been accepted and implemented?
- Is risk management competence part of performance reviews at all levels of the organization?

Auditor's Notes: How to Measure Maturity

☐ Business Process Definition and Risk Ownership

A formal common naming convention and hierarchy of all material business processes in the enterprise at least 1 level down from the department level is listed. Risk, performance and compliance readiness standards must be managed in context to the nature of what activity is being done. The context includes the level where risks, compliance or goal achievement could develop and materialize. The more granular the assessment, the more accurate and useful the result and therefore the more mature the ERM competency. Context is set around a sub-process, project, customer, vendor or other element of the business and then combined and aggregated to an enterprise level.

☐ Frontline and Support Process Owner Participation

Formal risk assessments have been completed in the past year for each business process area. Each assessment will have a subset of risks selected from an enterprise wide library. The context for this participation is gathered in an ERM Plan which is the basic communication platform that is used throughout the ERM Process to gather, organize and report information. It includes activities for assessing risk vulnerabilities, readiness compliance standards, and performance goals and their associated financial elements, standard operating procedures, controls, notes, tasks and documents.

☐ Far-sighted Risk Management Vision

Risk indicators are generic and can apply to more than one process area. "What could go wrong" effect or outcome responses to these indicators are for the period 12 months in the future of the date of assessment rather than prior loss data. Many risk systems were built to record losses, and therefore primarily collect historical information. While previous loss incidents provide a degree of insight during steady state operations, when dynamic change is introduced into the organization, an ability to assess future risk is needed.

☐ Executive ERM Support

Risk priorities are determined by an assessment scoring. A unique score for each of these three dimensions is expected: impact, likelihood and effectiveness of controls. Objective and standardized qualitative and quantitative criteria define each score range and are used for all assessments. Risk assessment results are regularly reviewed for accuracy, completeness and timeliness. Risks are linked to actual operational procedures and to related control activity. Is risk management effectiveness a formal component of employee performance reviews for key business processes? Has disciplinary action or recognition been given formally for deficiencies or excellence in risk management? Has the number of findings in a business process audit been correlated with that business process owner's risk management competency reviews?

Attribute 2: Uncovering Risks

Description: Degree of quality and penetration by risk assessment activities in uncovering and documenting risks and opportunities. Risk assessment activities include collecting knowledge from employees, subject matter experts and data contained in databases and other electronic files such as Microsoft® Word, Excel®, etc. to uncover dependencies and correlation across the enterprise.

Component: Risk Ownership by Business Area

Competency Drivers:

- Is risk identification decentralized and cascaded out to process owners most familiar with the risk and corresponding mitigation activities?

Component: Formalized Risk Indicators and Measures

Competency Drivers:

- Is standardized evaluation criteria for risk impact, likelihood, and control effectiveness used to objectively rank and prioritize action items?
- In addition to enterprise-level assessments, are targeted risk assessments (e.g., critical processes and high risk projects) conducted, analyzed and reviewed by front-line risk owners?

Component: Follow-up Reporting

Competency Drivers:

- Does the organization consider both the upsides and downsides of identified risks in its ERM reporting?
- Are mitigation and control activities regularly tested to ensure they are in place and effectively reducing risk?

Component: Adverse Events as Opportunities

Competency Drivers:

- Are strategic opportunities and objectives identified and assessed as part of the enterprise risk management process?

Auditor's Note: How to Measure Maturity

☐ Risk Ownership by Business Area

Risk ownership means the person closest to the management of the risk regardless of the level determines the ownership. These front line process owners know their risks and control environment the best and are therefore the most qualified to assess the risk. All resources a company relies on should be assessed to determine criticality. These resources include Relationships (vendors or customers), Physical Assets, IT Applications, Data (paper or electronic data and vendor services) and Financial Elements all mapped to the business processes that rely upon them. Assessments scores should be able to roll up to a single overall summary score for each business process that combines the individual scores for each resources and financial item. With this information, you can prioritize and focus your ERM efforts. Linking these resource elements together provides a holistic picture. For example, a vendor can have multiple products and services of different quality and risk. Assessing the products and services individually and linking those assessments to the vendor profile provides a much clearer picture on the combination of products, services and vendors used by a processes owner.

☐ Formalized Risk Indicators and Measures

Risk assessment of business plans on three dimensions: Impact, Likelihood and Controls (Assurance), in addition to providing a financial impact. Prioritization by assessment scoring is based on a scale from 1 to 10, with 10 having the most unfavorable consequences to the organization. For example, a 10 score for Impact means the highest negative impact; a 10 score for Likelihood means the highest likelihood that the Impact will occur; and, a 10 score for Assurance means that controls and mitigation strategies have the least positive effect on reducing risk impact or likelihood. For Impact and Likelihood, do not grant credit for existing controls or mitigating strategies. Instead, rate as if the risk manifests itself in the absence of controls activities. Only one of the criteria listed for an impact level has to be met in order to rate a risk factor at that level. For each component, the two dimensions of impact and likelihood for that component are multiplied together to calculate an inherent risk index. This inherent index multiplied by the third dimension, assurance or effectiveness of controls, calculates a residual risk index. The average of all components' indices creates the plan's risk index.

☐ Follow-up Reporting

Test designs of key controls must to be connected to the risks that the corresponding controls mitigate. Business metrics that track risk reduction impact and goal achievement should accompany formal tests that validate key control effectiveness. Reporting must allow for risk information filtering with the ability for business users to create custom columns of data for analysis. It also must not require detailed knowledge of the data or IT involvement.

Continued.

Auditor’s Note: How to Measure Maturity

☐ **Adverse Events as Opportunities**

Business sustainability and resilience planning should include representatives responsible for strategic planning, and new product and service groups should participate in scenario/brainstorming sessions. Customer and customer complaints should be reviewed for business development analysis.

Attribute 3: ERM Process Management

Description: Degree that the ERM Process is woven into business processes and using structured ERM steps to identify, assess, evaluate, mitigate and monitor risks and opportunities.

Component: ERM Program Oversight

Competency Drivers:

- Does each business area have a designated individual held accountable for identifying risk vulnerabilities, maintaining regulatory compliance, and meeting performance goals?
- Is the accountability for risk management delegated throughout the organizational structure (e.g. business processes, product lines, geographies, etc.?)
- Do managers actively participate in the ERM program?

Component: ERM Process Steps

Competency Drivers:

- Is a common risk management framework (e.g. root cause risk library, risk assessment criteria, etc.) available to and used by all business areas?
- Are sequential and iterative steps of risk identification, assessment, evaluation, mitigation, and monitoring utilized to improve performance, decision making and budget allocation?
- Do qualitative assessments determine the need and priority for further quantitative analysis or modeling?

Component: Risk Culture, Accountability and Communication

Competency Drivers:

- Are risk management procedures and risk culture understood and embedded at all levels of the organization?
- Are strategic opportunities evaluated on multiple dimensions such as impact, timing and confidence that the positive results can be achieved?

Component: Risk Management Reporting

Competency Drivers:

- Are reports measuring the progress of the ERM program and activities provided to stakeholders at a set frequency?

Component: Repeatability and Scalability

Competency Drivers:

- Are risk assessments regularly aggregated and reviewed by an enterprise risk committee?
- Are the criteria and assumptions used when conducting risk assessments periodically reviewed and updated?

Auditor's Note: How to Measure Maturity

☐ ERM Program Oversight

The number of assessments completed within the last 3 months should be equal to the number of sub-processes from Attribute 1: Adoption of ERM-based Approach, Component: Business Process Definition and Risk Ownership. All divisions, departments, or business processes should have completed a risk assessment in the past year. If assessments are not completed on time or are incomplete without adequate explanation, this is a concern for escalation to your organization's governance committee for ERM.

☐ ERM Process Steps

All material business processes should have all its critical resources and upstream and downstream dependent sub-processes mapped to it, including appropriate contact procedures to communicate material changes in risk profile. Risk identification should include the 3 dimensions of risk assessment: impact, likelihood and control assurance. Financial reporting compliance should be based on key controls with prior risk assessments to determine priority. All key mitigation activities should be connected to risk assessments and formalized monitoring activities (tests/metrics). Monitoring activities should be up to date, completed, and reviewed by the proper authorization levels.

☐ Risk Culture, Accountability and Communication

All sub-processes from Attribute 1: Adoption of ERM-based Approach, Component: Business Process Definition and Risk Ownership should have an appointed risk owner. All material risk should have documented corresponding mitigation activities, and all mitigation activities should have a corresponding risk. If key risks are not linked to verifiable operating procedures, this is a concern to escalate to your organization's governance committee for risk management.

☐ Risk Management Reporting

Metrics of coverage, completeness and timeliness for each material sub-process must be published and updated quarterly. Reports should include the percentage of key risks with controls, key controls with risks, key controls with monitoring, key resources linked to one or more sub-processes and risk ownership. Reporting should include the capability to focus on the specific data that is of interest to the executive. A risk taxonomy is the practice and science of naming, classifying and defining relationships within a body of information, and provides focus in any area of interest and enable fast, flexible reporting. Ask the question, "How long does it take to construct a new report or dashboard?" Users need the right information at the right time. When an information request has to be submitted, the report often arrives after it is no longer needed.

Continued.

☐ Repeatability and Scalability

The ERM committee should meet formally 4 times a year and risk Committee members should be committed. No more than 20% of risk committee members should have appointed subordinates to attend as a surrogate or have missed meetings. Performance management (corporate goals) should be formally linked to all key risks.

Attribute 4: Risk Appetite Management

Description: Risk appetite defines broadly the boundaries of acceptable risk whereas risk tolerance defines the tolerable variation that management deems acceptable.

Component: Risk Portfolio View

Competency Drivers:

- Is the organizational view of risk dynamic (e.g. by business process, risk category, and strategical goal)?
- Is risk tolerance formally defined for each business area and category of risk?
- Is risk assessment information aggregated, analyzed and are dependencies addressed?
- Are differences between defined risk tolerance and materialized risks regularly addressed?

Component: Risk-Reward Tradeoffs

Competency Drivers:

- Are risk-reward tradeoffs understood and does leadership use them to drive their actions?
- Are risk appetite and risk-reward tradeoffs considered throughout each iterative step of the ERM process?
- When a risk event occurs, are risk assessments evaluated to determine if the event had been previously identified, and if the assessment was accurate?
- Are risks reassessed when key risk and performance metrics change?
- Is resource allocation based on risk-reward analysis?
- Are risk assessments that consider the effects of mitigation activities measured against the organization's risk tolerance?

Auditor's Notes: How to Measure Maturity

☐ Risk Portfolio View

All key risks must have risk tolerances. Does your ERM Program report the number of risk tolerance exception requests? If the number of risk tolerance exceptions requests reviewed by the ERM Committee, or instances of assessments exceeding risk tolerance, is less than 5% of the total number of key risks, then the risk tolerances set may be inappropriate (high or low). Are dependencies of key resources, such as vendors, technology, facilities, customers, etc. linked to key risks? Are portfolio views of risks analyzed by tolerance levels? Are key controls determined by the level of risk they mitigate?

☐ Risk-Reward Tradeoffs

Are business metrics and tests formally connected to key risk assessments? Are business metrics linked to key risks monitored and demonstrated to be within tolerance? Ask for examples. Are manager performance goals linked to risks formally at the business process level? Are business metrics linked to the assessment score for the risks controlled by the activity being measured? Are risk assessments formally submitted along with the budgeting process?

Attribute 5: Root Cause Discipline

Description: Discipline applied to (a) measuring a problem's root cause; (b) binding events with their process sources; and, (c) selecting root cause categories that will prevent redundancy in identifying and addressing risks while ensuring that similar risks from varied sources are explored and uncovered. Best practice root cause categories include: people, external, systems, processes and relationships.

Component: Root Cause Consideration

Competency Drivers:

- Are all risks identified by using a root cause approach to ensure that the problem and not the symptom is addressed?
- Are root cause categories used to distinguish between risks within risk assessments? (e.g. external vs. internal fraud)
- Are the upstream and downstream causes and effects of risks understood?

Component: Risk and Opportunity Information Collection

Competency Drivers:

- Are risk assessments and action plans developed in the context of concrete examples and scenarios?
- Are the root causes of incidents or loss events tracked and used to determine the effectiveness of controls?

Component: Information Classification

Competency Drivers:

- Are specific financial risks (e.g. credit, liquidity, equity, etc.) identified, assessed, mitigated, monitored, and reported over time?
- Are root causes of operational risks identified, assessed, and monitored?
- Are organizational and business area goals documented, measured, reported, and managed?
- Is uniform enterprise risk management vocabulary and information classification used by all departments?

Component: Dependencies and Consequences

Competency Drivers:

- Are risk assessments used to determine potential effects (i.e. losses and gains) on goals?
- Are the root causes of all incidents and loss events used to drive the allocation of resources for implementing stronger controls?
- Is it clear how the risk from one department could affect other departments, as well as the entire organization?

Auditor's Note: How to Measure Maturity

☐ Root Cause Consideration

Is the risk register formally classified into discrete, mutually exclusive root cause categories rather than event outcomes (i.e. fire is an outcome, faulty wiring is a root cause). Ask for examples. Examine assessments to see if this categorization was made clear to the process owners doing assessments? Are risk indicators grouped by subcategories? In a typical risk register, there should be approximately twenty subcategories with one or more risk indicators rolling up to that category. Identifying the source of the risk defines the control strategy. For example, fraud from employees requires a different mitigation/control strategy than fraud from an external or vendor source.

☐ Risk and Opportunity Information Collection

Are controls linked to the root cause of the risks that they mitigate? It is only possible to know if a Mitigation Activity is effective and efficient if the objective of this activity is known. Review key operational controls. Key mitigation activities or controls should have descriptions (approximately 500 words) and meet the following planning scenarios:

- Change Management: How do you manage change to the activity over time?
- Compatibility: Is the activity aligned with other activities?
- Corporate Objectives: Are performance goals advanced by this activity?
- Cost: Does the cost exceed the benefit derived from it?
- Dependencies: Are the relevant resource elements linked to the activity?
- Effectiveness: Does it address specific risks?
- Efficiency: Is it easy to implement and monitor?
- Leverage: Can it be provide benefit in other areas?
- Ownership: Who is responsible for maintaining this activity?
- Regulatory: Does it address compliance readiness standards?

Continued.

Auditor’s Note: How to Measure Maturity

☐ Information Classification

Risks are linked to different management interests with specific mapping of information to each specific business unit. Data driven means that the map can change at any time by changing the data driven linkages. Lack of a robust taxonomy requires IT resources to create new computer code to develop a new query or to write a report in support of a business problem. Management must often go through the data and supply linkages after the fact. Lack of a data driven taxonomy means that Management must commission a special project to get the answers they need to make critical business decisions. The inability to get the information needed in a timely fashion often results in first making the decision and then getting the required analysis after it is no longer relevant.

☐ Dependencies and Consequences

Incidents must be linked to the operating controls that failed to mitigate effectively. Incidents that are cross-functional in nature must be cross-referenced to all the related business processes and resources involved. The cost of key controls oversight should be linked to the inherent risk, typically achieved by superimposing control assessments over inherent risk profiles on three dimensional heat maps.

Attribute 6: Business Resiliency and Sustainability

Description: Extent to which resiliency and sustainability considerations are integrated into operational planning and risk management. Business Resiliency and Sustainability evaluates the degree of ownership and planning beyond standalone disaster recovery and business continuity initiatives. Examples include vendor and distribution dependencies, supply chain disruptions, dramatic market pricing changes, cash flow volatility, business liquidity, etc.

Component: Risk-Based Planning

Competency Drivers:

- Do risk assessments drive the balance between daily deliverables and longer-term business priorities?

Component: Understanding Consequences

Competency Drivers:

- Do risk assessments conducted by front-line risk owners drive business continuity analysis and planning?
- Are upstream and downstream dependencies on key resources (people, vendors, IT applications) understood across business areas, and considered during the ERM process?

Component: Resiliency and Operational Planning

Competency Drivers:

- Are root cause risk categories (people, process, external environment, relationships, systems, etc.) considered in planning?
- Are assessments, policies, and procedures well documented, readily available, and regularly updated?
- Do business units report on how external and internal events impact their business models and strategic goals?
- Does the identification and evaluation of multiple scenarios play a role in strategic planning?

Auditor's Note: How to Measure Maturity

☐ Risk-Based Planning

Required actions must provide notification of the task status, and the list of tasks to be completed must be linked directly to specific risk, policy, control and test documentation to determine the accuracy, timeliness and completeness of risk management information.

☐ Understanding Consequences

Business functionality, including ERM, ORM, Compliance, BC, Vendor Management, IT Risk, IT security, SOX management, business measures and tracking, task management, team communications and management, relevant document tracking and business readiness are all accomplished in a core system. Data is common to and shared by all functions. Sharing of data across modules is difficult and often requires construction of hard to maintain bridge files and added complexity. Administration of training is greatly simplified for a single integrated system. Common data is only maintained once by the most authoritative department. Data quality is increased and departmental smoke stacking is greatly decreased. Data created once should be able to be viewed from multiple perspectives.

☐ Resiliency and Operational Planning

All risks related to business continuity (not just insurance and IT risk) should be cross-referenced with normal operating controls and quantified. Key operating controls should be formally linked to both risks and strategic corporate objectives. Documents must be stored and accessible in association with a particular risk. Change management due to emerging risks require related documents to be updated and cross-referenced. Beware of risk assessments separated from policy documentation or control documentation. Check the version updating notes to see if changes in one document are reflected in the changes of other related documentation.

Attribute 7: Performance Management

Description: Degree of executing vision and strategy, working from financial, customer, business process, and learning and growth perspectives, as are expressed in Kaplan's Balanced Scorecard. Performance management also addresses how an entity handles potential deviations from plans or expectations due to uncertainty.

Component: Communicating Goals

Competency Drivers:

- Are organizational goals tied to specific performance measures?
- Are employees at every level accountable for understanding and taking action on the risks that may prevent them from achieving their goals?
- Do all employees understand how evaluating risk-reward tradeoffs helps them achieve goals?
- Do employees understand the potential effects of the organization's top risks, should they materialize, on important strategic goals?
- Are resource allocation decisions based on formalized evaluation criteria such as impact on performance, timing of the benefits, and assurance that the positive results can be achieved?

Component: ERM Information and Planning

Competency Drivers:

- When setting priorities for strategic planning, is enterprise risk management taken into account?
- 2. Is risk management competence part of compensation and career development discussions across the organization?

Component: ERM Process Goals and Activities

Competency Drivers:

- Is enterprise risk management a formal part of goal setting?
- When evaluating new opportunities, does the organization measure and report the effectiveness of their risk management efforts to the board?
- Do business areas consider their impact on other areas of the organization when determining their goals (e.g. finance, compliance, and other strategic implications)?
- Do employees at all levels use a risk-based approach (i.e. regular risk assessments, controls, and monitoring), to achieve departmental and corporate goals?
- Are deviations in the expectations versus results of projects, initiatives, and operational milestones evaluated in the context of corporate and business unit-level goals?

Auditor's Note: How to Measure Maturity

☐ Communicating Goals

Business process owners must be able to demonstrate a formal link between their management objectives and corporate strategic goals. Strategic goals are cross-functional in nature. In order for resources to be allocated to the highest impact activities, all contributing activities needs to strategic goals must be formally tracked. Measures of those activities need to be identified and aggregated to track the progress the organization is making toward achieving these Strategic goals.

☐ ERM Information and Planning

Measures or business metrics for activities must be easily identified and enable clear measurement on the progress of achieving strategic plans. Key risk indicators, key performance indicators and compliance constraints must be formally linked with business process owner objectives that are agreed upon in performance reviews. Assessments for these indicators in planning phases must be able to be aggregated to strategic goals while remaining linked to compensation targets to keep activities and resources aligned with goal achievement.

☐ ERM Process Goals and Activities

Ability to compare risk-reward trade-offs by formally linking assessed key risk indicators with balanced scorecard business/key performance indicators to associate a specific risk with a particular business strategy. Linking performance goals and risks to mitigation activities identifies misalignment between incentives and corporate objectives. It also adds business value to risk and compliance work which results in engagement of both front line management and senior leadership.

Conclusion and Summary

This analysis, based on guidelines set forth in the model, will provide your organizations an objective benchmark to your peer organizations, an objective assessment of the effectiveness of your organization's ERM program, a basis for objective and actionable findings and a roadmap for improvement. The Risk Maturity Model for Enterprise Risk Management allows organizations to develop sustainable, effective Enterprise Risk Management programs. This analysis, based on guidelines set forth in the model, will provide your organizations a roadmap for improvement. No organization anticipates that minute operational failures will result in million dollar litigations, but by equipping your risk management function with the checks and balances that connect process owners to C-Level executives, you can ensure that all parties are protected and instill a preventative risk culture at an enterprise level.

About the Author, Steven Minsky

Steven Minsky is the Chief Executive Officer of LogicManager and the author of the RMM. Steven is a recognized expert and thought leader in ERM; he is a highly sought-after speaker, having led top-rated sessions for a variety of organizations. He regularly presents strategic and practical sessions at a variety of conferences, including the IIA All-Star Conference, American Bankers Association's Risk Management Conference, the RIMS Annual and ERM Conferences, the IIA & ISACA's GRC Conference, and the Risk Management Association (RMA)'s GCOR series. He has led educational webinars on a variety of risk-based topics for groups like OCEG, RIMS, PCIAA, and hosted board-level training sessions for many LogicManager customers.

Steven is also a patent author of risk and process management technology and holds MBA and MA degrees from the University of Pennsylvania's Wharton School of Business and The Joseph H. Lauder Institute of International Management. He is the Founder and Chairman of Board of Directors for Achieving Your Potential: an independent, not-for-profit organization, separate and distinct from the Elementary Public Schools System. Steven established this initiative to help dyslexic children get the evidenced-based curriculum, teaching and support they need to reach their own personal potential. In February of 2017, Steven was appointed President of the Lauder Institute Alumni Association (LIAA) to foster social connections and professional development for global alumni at the Lauder MBA/MA program at the University of Pennsylvania

About LogicManager

LogicManager provides configurable ERM software solutions and mentoring services to accelerate risk management effectiveness. LogicManager makes the job of risk management an integral part of operations so that resources can be prioritized to the areas most critical to drive performance. Managers across the enterprise can easily assess their risks and opportunities, create action plans and provide evidence of their successes to stakeholders.

To discuss this Guide or the Risk Maturity Model, please contact a LogicManager risk management specialist at: 617-649-1325 or email info@logicmanager.com. More information is available at: logicmanager.com.

Appendix

ATTRIBUTES	MATURITY LEVELS Level 5: Leadership Level 5: Managed Level 3: Repeatable Level 2: Initial Level 1: Ad Hoc Nonexistent
Adoption of ERM-based Approach	**Key Drivers: Degree of …** • support from senior management, Chief Risk Officer • business process definition determining risk ownership • assimilation into support area and front-office activities • far-sighted orientation toward risk management • risk culture's accountability, communication and pervasiveness
Uncovering Risks	**Key Drivers: Degree of …** • risk ownership by business areas • formalization of risk indicators and measures • reporting on follow-up activities • transforming potentially adverse events into opportunities
ERM Process Management	**Key Drivers: Degree of …** • each ERM Process step (see definition) • ERM Process's repeatability and scalability • ERM Process oversight including roles and responsibilities • risk management reporting • qualitative and quantitative measurement
Risk Appetite Management	**Key Drivers: Degree of …** • risk-reward tradeoffs • risk-reward-based resource allocation • analysis as risk portfolio collections to balance risk positions
Root Cause Discipline	**Key Drivers: Degree of …** • classification to manage risk and performance indicators • flexibility to collect risk and opportunity information • understanding dependencies and consequences • consideration of people, relationships, external, process and systems views
Business Resiliency and Sustainability	**Key Drivers: Degree of …** • integration of ERM within operational planning • understanding of consequences of action or inaction • planning based on scenario analysis
Performance Management	**Key Drivers: Degree of …** • ERM information integrated within planning • communication of goals and measures • examination of financial, customer, business process and learning • ERM process goals and activities

Attribute 1: Adoption of ERM-based Approach

Degree of executive support for an ERM-based approach within the corporate culture. This goes beyond regulatory compliance across all processes, functions, business lines, roles and geographies. Degree of integration, communication and coordination of internal audit, information technology, compliance, control and risk management.

Nonexistent

No recognized need for an ERM Process and no formal responsibility for ERM. Internal audit, risk management, compliance and financial activities might exist but aren't integrated. Business processes and risk ownership aren't well defined.

Level 1: Ad Hoc

Corporate culture has little risk management accountability. Risk management is not interpreted consistently. Policies and activities are improvised. Programs for compliance, internal audit, process improvement and IT operate independently and have no common framework, causing overlapping risk assessment activities and inconsistencies. Controls are based on departments and finances. Business processes and process owners aren't well defined or communicated. Risk management focuses on past events. Qualitative risk assessments are unused or informal. Risk management is considered a quantitative analysis exercise.

Level 2: Initial

Risk culture is enforced by policy interpreted as compliance. An executive champions ERM management to develop an ERM Process. One area has used the ERM Process, as shown by the department head and team activities. Business processes are identified and ownership is defined. Risk management is used to consider risks in a far-sighted manner.

Level 3: Repeatable

ERM risk plans are understood by management and the organization. Senior management expects that a risk management plan includes a qualitative risk assessment for significant projects, new products, business practice changes, acquisitions, etc. Most areas use the ERM Process and report on risk issues. Process owners take responsibility for managing their risks and opportunities. Risk management creates and evaluates far-sighted scenarios.

Continued.

Attribute 1: Adoption of ERM-based Approach

Level 4: Managed

Risk culture is associated with career advancement. The organization is self-governed with shared ethics and trust; promise-makers are held accountable. Risk management issues are understood at all levels and risk plans are conducted in all business process areas. The Board of Directors, CEO and Chief Risk Officer expect a risk management plan to include a qualitative risk assessment for significant projects, new products, business practice changes, acquisitions, etc. with reporting to the Board on priorities. All areas use the ERM Process to enhance their functions via the ERM framework, with frequent and effective communication on risk issues. Process owners incorporate managing their risks and opportunities within regular planning cycles. All areas create and evaluate far-sighted scenarios and follow-up activities.

Level 5: Leadership

Risk culture is analyzed and reported as a systematic view of evaluating risk. Executive sponsorship is strong and the tone from the top has sewn an ERM Process into the corporate culture. Board of Directors, senior management and the Chief Risk Officer communicate risk management's importance in daily decisions. Risk management is embedded in each business function. Internal audit, information technology, compliance, control and risk management are highly integrated and coordinate and report risk issues. All areas use risk-based best practices. The risk management lifecycle for each business process area is routinely improved.

Attribute 2: Uncovering Risks

Degree of quality and penetration coverage of risk assessment activities in documenting risks and opportunities. Degree of collecting knowledge from employee expertise, databases and other electronic files (such as Microsoft® Word, Excel®, etc.) to uncover dependencies and correlation across the enterprise.

Nonexistent

There might be a belief that the most important risks are known, although there is probably little documentation.

Level 1: Ad Hoc

Risk is owned by specialists, centrally or within a department. Risk information provided to risk managers is probably incomplete, dated or circumstantial, so there's high risk of misinformed decisions, with potentially severe consequences. Further mitigation, supposedly completed, is probably inadequate or invalid.

Level 2: Initial

Formal lists of risks for each department and discussions of risk are part of the ERM Process. Corporate risk indicators are collected centrally, based on past events. Departments might maintain their own informal risk checklists that affect their areas, leading to potential inconsistency, inapplicability, lack of sharing or under-reporting.

Level 3: Repeatable

An ERM team manages a growing list of business area specific risks, creating context for risk assessment as a foundation of the ERM Process. Risk indicator lists are collected by most process owners. Upside and downside outcomes of risk are understood and managed. Standardized evaluation criteria of impact, likelihood and controls' effectiveness are used, prioritizing risk for follow-ups. Enterprise level information on risks and opportunities are shared. Risk mitigation is integrated with assessments to monitor effective use.

Level 4: Managed

Process owners aggressively manage a growing list of business area specific risks locally to create context for risk assessment activities as a foundation of the ERM Process. Risk indicators that are deemed critical to their areas are regularly reviewed in collaboration with the ERM team. Measures ensure downside and upside outcomes of risks and opportunities are aggressively managed. Standardized evaluation criteria of impact, likelihood and controls' effectiveness are used to prioritize risk for follow-up activity. Risk mitigation is integrated with assessments to monitor effective use.

Continued.

Attribute 2: Uncovering Risks

Level 5: Leadership

Internal and external best practices, support functions, business lines and regions are systematically gathered and maintained. A routine, timely reporting structure directs risks and opportunities to senior management. The ERM Process promotes frontline employees' participation and documents risk issues' or opportunities' significance. Process owners regularly review and recommend risk indicators that best measure their areas' risks. The results of internal adverse event planning are considered a strategic opportunity.

Attribute 3: ERM Process Management

Degree of weaving the ERM Process into business processes and using ERM Process steps to identify, assess, evaluate, mitigate and monitor. Degree of incorporating qualitative methods supported by quantitative methods, analysis, tools and models. See ERM Process definitions.

Nonexistent

There's little recognition of the ERM Process's importance.

Level 1: Ad Hoc

Management is reactive and ERM might not yet be seen as a process. Few processes are standardized and are improvised instead. There are no standard risk assessment criteria. Risk management is involved in business initiatives only in later stages or centrally. Risk roles and responsibilities are informal. Risk assessment is improvised. Standard collection and assessment processes aren't identified.

Level 2: Initial

Management recognizes a need for an Enterprise Risk Management Process. Agreement exists on a framework, which describes roles and responsibilities. Evaluation criteria are accepted. Risk mitigation activities are sometimes identified but not often executed. Qualitative assessment methods are used first in all areas and determine what needs deeper quantitative methods, analysis, tools and models.

Level 3: Repeatable

The ERM Process accommodates all business and support areas' needs. ERM is a process of steps to identify, assess, evaluate, mitigate and monitor. ERM Process includes the management of opportunities. An Enterprise Risk Council exists and senior management actively reviews risk plans. The ERM Process is collaborative and directs important issues to senior management.

Level 4: Managed

Management is clearly defined and enforced at every level. A risk policy articulates management's responsibility for risk management, according to established risk management processes. An Enterprise Risk Council exists and management develops and reviews risk plans. The ERM Process is coordinated with managers' active participation. Opportunities associated with risk are part of risk plans' expected outcome. Authentication, audit trail, integrity and accessibility promote roll-up information and information sharing. Periodic reports measure ERM progress for stakeholders, including the Board of Directors.

Continued.

Attribute 3: ERM Process Management

Level 5: Leadership

ERM, as a management aspect, is embedded in all business processes and strategies. Roles and responsibilities are process driven with teams collaborating across central and field positions. Risk and performance assumptions within qualitative assessments are routinely revisited and updated. The organization uses an ERM process of sequential steps that improves decision-making and performance. A collaborative, enterprise-wide approach includes all supporters. Accountability for risk management is woven into all processes, support functions, business lines and geographies as a way to achieve goals.

Attribute 4: Risk Appetite Management

Degree of understanding the risk-reward tradeoffs within the business. Accountability within leadership and policy to guide decision-making to attack gaps between perceived and actual risk. Risk appetite defines the boundary of acceptable risk and risk tolerance defines the variation of measuring risk appetite that management deems acceptable.

Nonexistent

The need for formalizing risk tolerance and appetite isn't understood.

Level 1: Ad Hoc

Risk management might lack a portfolio view of risk. Risk management might be viewed as risk avoidance and meeting compliance requirements or transferring risk through insurance. Risk management might be a quantitative approach focused on the analysis of high-volume and mission-critical areas.

Level 2: Initial

Risk assumptions are only implied within management decisions and aren't understood outside senior leadership with direct responsibility. There's no ERM framework for resource allocation. Defining different views of business areas from a risk perspective can't be easily created and compared.

Level 3: Repeatable

Risk assumptions within management decisions are clearly communicated. There's a structure for evaluating risk on an enterprise-wide basis and for gauging risk tolerance. Risks and opportunities are routinely identified, evaluated and executed in alignment with risk tolerances. The ERM framework quantifies gaps between actual and target tolerances as part of the ERM Process. Portfolio views to balance risk positions are created and risk tolerance is evaluated based on portfolio analysis.

Level 4: Managed

Risk appetite is considered in each ERM Process step. Resource allocation decisions consider the evaluation criteria of business areas. The organization forecasts planned mitigation's potential effects versus risk tolerance as part of the ERM Process. Portfolio views are dynamic and risk tolerance is evaluated based on different views. Risk is managed by process owners. Risk tolerance is evaluated as a decision to increase performance and measure results. Risk-reward tradeoffs within the business are understood and guide actions.

Continued.

Attribute 4: Risk Appetite Management

Level 5: Leadership

A process for delegating authority to accept risk levels is communicated throughout the organization. Risk management uncovers risk, reduces uncertainty and costs and increases return on equity by risk awareness. The management team and Enterprise Risk Council define tolerance levels for all departments. A mechanism compares and reports actual assessed risk versus risk tolerance. The organization manages business areas and has portfolio collection to balance risk positions. Management prioritizes resource allocation based on the gap between risk appetite and assessed risk and opportunity. The established risk appetite is examined periodically as part of planning. Example: Take more risk and gain more market share versus a conservative hold position and protect the brand.

Attribute 5: Root Cause Discipline

Degree of discipline applied to measuring a problem's root cause and binding events with their process sources to drive the reduction of uncertainty, collection of information and measurement of the controls' effectiveness. The degree of risk from people, external environment, systems, processes and relationships is explored.

Nonexistent

The effects of risky events might be identified but not linked to goals. Events aren't associated with their process sources.

Level 1: Ad Hoc

Cost savings aren't evaluated based on risk-based consequences. Risks aren't consistently evaluated. Perceived risk's frequency isn't tracked or connected to a process. Risk indicators and goals aren't organized within a framework and aren't central to the ERM Process. Many root causes have a wide array of implications. Does not formally track root causes throughout the ERM Process.

Level 2: Initial

The cause and effect chain from the top-down and the bottom-up isn't defined. Only past risk events are considered, leaving most possible risk areas not covered. A terminology and classification for collecting risk information exists. Awareness of a root cause approach's importance exists, but no robust scheme organizes risk indicators or performance indicators as the core of a risk management framework and ERM Process.

Level 3: Repeatable

The cause and effect chain from the top-down and the bottom-up is understood. A terminology and classification for collecting risk information is used. The ERM framework is organized around root cause risk categories such as internal people, external environment, relationships, systems and processes. The root cause approach is important in each ERM Process step, from the Identify step, to ensure all risk sources' are reviewed, to the Monitor step, to verify that the problem -- not the symptom --is attacked. Scenarios are developed and the root cause that makes the difference in scenario outcomes between worse case and best case are uncovered.

Continued.

Attribute 5: Root Cause Discipline

Level 4: Managed

A terminology and classification for collecting risk information is fully implemented. Causes, rather than only results, are identified, measured and managed. Risk and performance information is collected from all areas to identify dependencies and root cause indicators' frequency. Residual risk's financial implications are managed without distortive double counting within risk assessments. Operational, financial and strategic risks' root cause drivers are investigated, defined, quantified and routinely monitored. Scenario analysis is used throughout planning. Events are associated with their process sources to drive progress and measure the controls' effectiveness.

Level 5: Leadership

Mitigation measures are determined and a method to quantify effectiveness is understood. There's an obvious focus on root cause to achieve goals and maximize risk's upside. The organization uses "post mortems" to deconstruct past events (either its own or others') into root cause categories to prepare for future events. Scenarios are developed to evaluate potential benefits and drawbacks on a risk adjusted basis. The organization tracks events and traces root cause in evaluating cost benefits of improvements. Risk elements' frequencies are identified and monitored. The discipline of reviewing all risky avenues is promoted to provide a comprehensive view of risk and opportunity. This is proactive risk management, rather than problem management.

Attribute 6: Business Resiliency and Sustainability

Extent to which the ERM Process's sustainability aspects are integrated into operational planning. This includes evaluating how planning supports resiliency and value. The degree of business ownership and planning beyond recovering technology platforms. Examples include vendor and distribution dependencies, supply chain disruptions, dramatic market pricing changes, cash flow volatility, business liquidity, etc.

Nonexistent

Resiliency and sustainability is limited to an IT infrastructure orientation of continuity and disaster recovery.

Level 1: Ad Hoc

Management is aware of resiliency-related risks and focused on infrastructure rather than the business. Users respond to disruptions with workarounds. The response to major disruptions is reactive. Departmental requirements to avoid risk often don't consider business needs. Impact of external and internal events on the business model isn't systematically reviewed.

Level 2: Initial

The organization recognizes broader planning's importance. This highlights the business aspects in addition to traditional disaster recovery. There's recognition that resiliency is an issue that needs consideration in each ERM Process step, and not just in mitigation, as is common with traditional business impact analysis. Achieving balance between quarterly deliverables versus mid-term and long-term value is considered.

Level 3: Repeatable

Resiliency uses far-sighted scenario analysis to document key drivers. The organization indexes priorities qualitatively and quantitatively, with consistent and objective criteria. Resiliency and sustainability are part of every risk plan and considered in each ERM Process step. Business model issues include geography, disruptive technology, competitors, leadership and environmental changes, with reporting and control by senior management.

Level 4: Managed

A comprehensive approach to resiliency considers the people, external, relationship, systems and process aspects. Logistics, security, resources and organization of response procedures are well documented. Resiliency and sustainability are part of the ERM Process and business continuity as mitigation. As a result of the risk process's evaluation, business-driven impact analysis is initiated. Reporting on how external and internal events might impact the business model is raised to the Board of Directors. Balance is achieved between quarterly deliverables and mid-term and long-term value.

Continued.

Attribute 6: Business Resiliency and Sustainability

Level 5: Leadership

All issues are framed within the context of continuity of services to all stakeholders. Resiliency or sustainability might be defined differently by each organization, with business-driven impact analysis initiated at all levels, based on priorities. Sustainability isn't a reachable end state; rather, it is characteristic of a dynamic and evolving system. Long-term sustainability results from continuous adaptation.

Attribute 7: Performance Management

Degree of executing vision and strategy, working from the financial, customer, business process and learning and growth perspectives, such as Kaplan's balanced scorecard, or similar approach. Degree of exposure to uncertainty, or potential deviations from plans or expectations.

Nonexistent

No formal framework of indicators and measures for goals and management exists.

Level 1: Ad Hoc

Not all goals have measures and not all measures are linked with goals. Strategic goals aren't articulated in terms that the frontline management understands. Compliance focuses on policy and is geared toward satisfying external oversight bodies. Process improvements are separate from compliance activities. Decisions to act on risks might not be systematically tracked and monitored. Monitoring is done and metrics are chosen individually. Monitoring is reactive.

Level 2: Initial

The ERM Process is separate from strategy and planning. A need for an effective process to collect information on opportunities and provide strategic direction is recognized. Motivation for management or support areas to adopt a risk-based approach is lacking.

Level 3: Repeatable

The ERM Process contributes to strategy and planning. All goals have measures and all performance measures are linked with goals. While compliance might trigger reviews, other components are integrated, including process improvement and efficiency. The organization indexes opportunities qualitatively and quantitatively, with consistent criteria. Risk management criteria are part of management's performance evaluations. Employees understand how a risk-based approach helps them achieve goals. Accountability toward goals and risk's implications are understood, and are articulated in ways that frontline personnel understand.

Level 4: Managed

The ERM Process is an integrated part of strategy and planning. Risks are aggressively considered as part of strategic planning. Risk management is a formal part of goal setting and achievement. Incentive for effective risk management is part of compensation and career development. Investment decisions for resource allocation examine the criteria for evaluating opportunity impact, timing and assurance. The organization forecasts planned mitigation's potential effect on performance impact, timing and assurance prior to use. Employees at all levels use a risk-based approach to achieve goals.

Continued.

Attribute 7: Performance Management

Level 5: Leadership

The ERM Process is an important element in strategy and planning. Evaluation and measurement of performance improvement is part of the risk culture. Measures for risk management include process and efficiency improvement. The organization measures the effectiveness of managing uncertainties and seizing risky opportunities. Deviations from plans or expectations are also measured against goals. A clear, concise and effective approach to monitor progress toward risk management goals is communicated regularly with business areas. Individual, management, departmental, divisional and corporate goals are linked with standard measurements.

Build an ERM Program with LogicManager

We've given you the steps and tactical insights you need to bring your risk management program to the next level. The next step will be choosing a software that's right for your business.

LogicManager believes performance is a result of effective risk management. Since 2005, LogicManager's ERM software has empowered organizations to uphold their reputation, anticipate what's ahead, and improve business performance through strong governance.

REQUEST A DEMO

AUDIT MANAGEMENT

BUSINESS CONTINUITY & DR

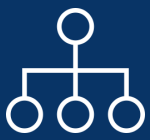
COMPLIANCE MANAGEMENT

INCIDENT MANAGEMENT

ENTERPRISE RISK MANAGEMENT

FINANCIAL REPORTING (SOX, MAR)

POLICY MANAGEMENT



VENDOR MANAGEMENT

IT GOVERNANCE & SECURITY

Get in touch:
+1 617 530 1210
info@logicmanager.com
5-11 Drydock Ave, Boston, MA 02210

Learn more:
logicmanager.com