

# Risk Assessment Do's and Don'ts

By: J. Efrim Boritz

School of Accounting and Finance, University of Waterloo, Waterloo, Canada N2L 3G1

© Copyright 2012 All Rights Reserved

## Risk Defined

Risk is the potential for loss to an enterprise due to error, fraud, inefficiency, failure to comply with statutory requirements, or actions which bring disrepute to the entity. Risk is a synonym for all the adverse outcomes that the organization wishes to avoid. Risk is a function of the probability that such consequences will occur, their magnitude, and their imminence.

## Risk Assessment

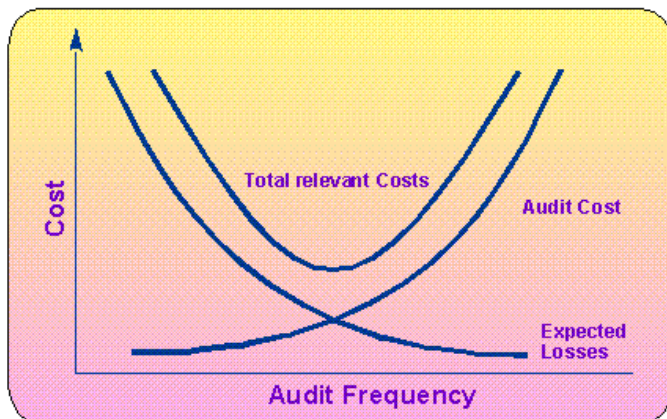
Risk assessment is a process of estimating a riskiness coefficient or score to be associated with each auditable unit within the organization. Risk assessment is typically undertaken to focus attention on significant audit areas, to allocate scarce audit resources to the most important audit areas, and to help with key audit prioritizing decisions such as audit frequency, intensity and timing.

Standards for the Professional Practice of Internal Auditing suggest that criteria used for setting audit priorities should include:

- the date and results of the last audit
- financial exposure
- potential loss and risk
- requests by management
- major changes in operations, programs, systems and controls
- opportunities to achieve operating benefits
- changes to and capabilities of audit staff.

These standards point out clearly that the riskiness of a specific auditable unit is only one of the key factors to be considered in establishing an audit coverage plan and schedule. A risk coefficient alone is not a sufficient basis for making appropriate audit planning decisions. It is also necessary to bring the cost of carrying out an audit into the picture; i.e., the riskiness coefficient of an audit unit must be "deflated" by the cost of eliminating, reducing, or maintaining that level of risk.

*A fundamental flaw in many risk assessment methods used in practice is their failure to take into account the fact that auditing is a costly activity and to systematically factor this consideration into the development of a long range audit coverage plan.*



Since relating costs and benefits is a fundamental principle of rational decision making, internal audit departments should focus not only on the riskiness of an auditable unit, but also on the cost of reducing risk through auditing.

One way of applying this cost/benefit approach is to simply calculate the ratio of the riskiness coefficient of a given auditable unit divided by the cost of auditing that auditable unit, yielding a measure of the benefits (in terms of risk reduction) to be derived from investing audit resources in a given activity (in terms of incurring the cost of the audit). The units assigned the highest audit frequency would be those with the highest "payoffs" as measured by their risk to cost ratios.

The following formula can be used to calculate the optimal inter audit frequency:

$$\sqrt{\frac{2}{\beta M/C}}$$

where  $\beta$  is an audit unit's riskiness coefficient,  $M$  is the audit unit's maximum loss potential, and  $C$  is the average cost per audit. In this formulation, the smaller the inter-audit interval, the higher the audit priority.

## Audit Frequency = Plan Horizon/Optimal Inter-Audit Interval

In Figure 1 the vertical axis represents cost, expressed in financial terms. The horizontal axis is audit frequency represented by the number of audits carried out over the period of time. That is the planning horizon. As the audit frequency increases (moves to the right) the curve representing the total expected losses, decreases. That is, the more frequently an auditor audits a unit, the less opportunity there will be for the expected losses to accumulate and, therefore, total losses will be lower. However, at the same time, the more frequently an auditor audits a given auditable unit, the more audit costs are incurred.

The total relevant cost is the sum of the audit cost and the cost attributable to the losses due to fraud, waste, error, and so forth incurred in the absence of auditing. It is in the best interests of the organization as a whole to minimize its total costs (i.e., the costs of auditing plus the costs of not auditing). The minimum point on the total relevant cost curve identifies the frequency which balances the cost of auditing a given unit a given number of times during its planning horizon against the cost of **not** auditing that audit unit, and incurring the expected losses instead. Since risk in this approach is a measure only of the cost of not auditing, it is not sufficient to merely look at risk ratings as the basis for developing audit coverage plans.

## Non-Systematic vs. Systematic Risk Assessment

There are two fundamental ways of establishing risk scores: non-systematic and systematic.

Systematic approaches involve systematic decomposition of risk into individual factors which are assessed individually, then combined into an overall score reflecting an audit unit's riskiness. The process requires identification of key areas of risk (i.e., termed risk factors) important to management, grouping risk factors into categories based on similar characteristics, and assigning weights to the risk factors indicating their relative importance in a model for setting audit scope (frequency, intensity and timing).

Clearly, the systematic approach is more onerous than the non-systematic approach. Why chose it? Well, research conducted into the reliability of subjective global judgments in a variety of fields shows that global judgments such as those required by the non-systematic approach are prone to significant errors. The general consensus of this research is that professionals should refrain from trying to make global intuitive judgments such as, "The riskiness of audit unit A is ..." Instead, they should apply their judgment to:

1. Decompose complex global judgments into component factors,
2. Assess these specific areas of risk and concern, and
3. Leave the combining process to mathematical models, since it has been found that computational models and algorithms consistently outperform even seasoned professionals.

## Benefits of Systematic/Formal Approaches

Virtually all of the important literature that deals with planning emphasizes that the formal process whereby individuals engage in a systematic consideration of important factors makes a key contribution to the quality of subsequent decisions.

## Formal/Systematic Approaches Do Not Eliminate Judgment

The use of a formal/quantitative approach to risk assessment does not eliminate the need for the exercise of judgment. On the contrary, it highlights some of the important judgments that are required:

- Identifying the key elements of the problem being considered.
- Characterizing the interrelationships among these elements.
- Selecting an appropriate quantitative model for expressing these relationships.
- Adopting appropriate ways for obtaining the values to be entered into a quantitative model.
- Assessing the values to be used with the parameters of the selected quantitative model.
- Evaluating the quality of the analysis and its applicability to the circumstances under consideration.

In summary, there need not be a conflict between the application of professional judgment and intuition and reliance on formal or systematic approaches to risk analysis. Indeed the best approaches to problem solving strive to combine elements of intuition and systematization in such a way as to take advantage of the best features of humans and computational models. The auditor applies expertise in identifying critical risk factors and using them to record key observations about issues such as internal control. A system can be used to combine these ratings consistently since that is something that an auditor cannot do as well.

## The benefits of systematic/formal approaches to risk assessment:

1. The train of logic can be documented.
2. Training is enhanced since trainees can study logic that is documented.
3. Review and consultation are facilitated.
4. Decisions may be easier to explain and justify, especially in the future when the auditor's memory of the circumstances fades.
5. Potential errors may be reduced by reducing the need to combine large quantities of data in one's head.
6. A direct linkage can be provided between the administrative structure and budget of the internal audit department and the characteristics of individual audit units; this linkage emphasizes the integrated nature of administrative and operational activities.
7. New data can be more easily incorporated into the analysis as it becomes available.
8. Consistency may be enhanced since it may be easier to set operational guidelines for quantitative risk assessment methods than for more global qualitative risk judgments.
9. Quantitative methods may be more easily defended; e.g., to audit committees, external parties, etc.
10. Quantitative judgments of risk can be incorporated into other methods to help ensure the appropriate intensity of auditing commensurate with the risk profile of the audit unit. This can help reduce the possibility of overauditing or underauditing.

# Key Audit Decisions Aided by Risk Assessment

## 1. Audit Frequency

In many organizations, it is assumed that all units will be audited at least so often during a planning horizon that typically covers 3 to 5 years. The issue is, "How often within this planning horizon should each auditable unit be audited?" The general opinion is that riskier audit units should be audited more frequently, although the actual audit frequency can be set in various ways.

A fixed frequency policy is based on the implicit assumption that there are natural frequencies associated with audit units. The problem then becomes finding the "right" fixed frequency for each unit. This approach is followed by many internal audit departments, although frequencies may be adjusted periodically. It may be argued, however, that if auditees "learn" the fixed frequency, they may be motivated to perform at peak levels only at or near the audit dates. In addition, to the extent that the frequencies are imperfect, some auditable units would be consistently overaudited, while others would be consistently underaudited.

Under a conditional audit frequency approach all auditable units are monitored continuously or at specified intervals for signs of abnormal activity. Two approaches to conducting such monitoring activities are analytical review and periodic risk assessment. Audits would be scheduled when units exhibited a deterioration along some key dimension. The reasoning is that when compliance with set policies and procedures or sound management practices deteriorates, this adversely affects the unit's activity. Abnormal activity may be an indicator of control failures, etc. and vice versa. Thus, by monitoring various relevant economic indicators, the internal auditor might be alerted to problems such as non-compliance with control procedures. Conversely, by monitoring risk factors such as adequacy of controls, the internal auditor might be alerted to impending deterioration of economic activity. A variety of indicators can be used individually or in combination with other factors.

## 2. Audit Intensity

Riskier units should be audited more intensely; however, audit intensity may be a complex function of time, samples sizes, seniority, skill, etc. There is no known simple or unique relationship between the riskiness of an audit unit and these intensity factors, since in some cases one factor can substitute for another, while in other instances it might not.

## 3. Audit Timing

No audit department has the resources to audit all of its auditable units simultaneously. Therefore, a third key audit decision is the timing of the audit. In the absence of other considerations, the riskier audit unit should be audited sooner than the less risky audit units. Unfortunately, direct application of such simple logic is rarely possible, since a variety of constraints intervene, such as limited availability of the appropriate audit personnel at a given point in time, personnel development considerations, management requests, auditee considerations, etc.

There are three main alternatives for scheduling audits: fixed, random or conditional timing.

### a. Fixed Timing Policy

A fixed timing policy is based on the assumption that there are fixed times best suited to the conduct of specific audits. As mentioned earlier, if auditees know the timing of audits, they may "dress up" for the occasion, giving an inaccurate impression of their effectiveness, efficiency, etc.

### b. Random Timing

Under this policy the frequency and timing of audits is unpredictable. Since auditees cannot guess when they will be audited, it is argued that they would be motivated to maintain their controls and procedures at reasonable levels. Surprise audits are examples of the use of this policy. If surprise audits are used to motivate compliance or deter non-compliance, randomization becomes an important technique for scheduling audits.

### c. Conditional Audit Timing

Under a conditional audit approach audits are scheduled when units exhibit a deterioration of controls or performance along some key dimension. In addition, other scheduling criteria could be used such as availability of human resources, personnel development criteria, the need to balance effort over a time horizon, etc.

As mentioned earlier, no internal audit department is of a sufficient size to carry out all the necessary audits simultaneously, or even within the time span of one fiscal year. A fundamental principle of internal audit administration is that the internal department be of a sufficient size and capability to address the areas of concern to management, with an adequate frequency, over a reasonable time horizon of 3-5 years. If risk factors reflect management concerns, then they can be used as a basis for establishing the department size required to address the most important audit units (i.e., those with the highest risks or those with the highest [risk/audit cost] payoffs).



## Implementing a Systematic Risk-Assessment Approach

A systematic approach to risk analysis consistent with the Professional Standards of the *Institute of Internal Auditors* entails a number of specific steps and techniques:

- Define the audit universe and identify the auditable units within the entity for which these analyses will be carried out.
- Identify appropriate risk factors designed to reflect management's concerns.
- Select an appropriate format for evaluating risk factors so that the more important risk factors play a more prominent role in the risk assessment process than less important risk factors.
- Develop a combination rule for each audit unit which will properly reflect its riskiness over several risk factors that have been identified, and a method of setting audit priorities for the audit units.
- Once audit units have been rated according to their riskiness, it is important to have a mechanism for assigning them to audit frequency categories; that is, to identify which units will be audited so often, say once every five years, and which units will be audited more often, say twice every five years, and which will be audited virtually continuously, say five or even ten times over a five year planning horizon; and, a mechanism for applying variable audit scope or intensity of auditing commensurate with the importance of the audit unit.
- Having carried out these analyses, it is useful to produce an audit coverage plan which indicates which audits will be conducted at what times throughout the planning horizon and the expected costs associated with those audits.
- The coverage plan provides a roadmap for the management of staff skills so that they are available to carry out audits of appropriate scope and intensity when they are needed; a basis for scheduling audits in such a way as to ensure a balanced workload and the availability of resources when needed; a basis for appropriate co-ordination with external auditors to ensure that areas of importance are appropriately covered and that total audit costs for the organization are minimized.
- An important part of a long term planning process is establishing the appropriate department size for the internal audit department commensurate with its mandate and responsibility. Zero-base budgeting can be used as a technique for incorporating staffing considerations and risk considerations in establishing the ideal department size.
- Finally, a system of quality assurance is required to make sure that these activities are properly carried out.

These steps are discussed in more detail next, with illustrations from practice.

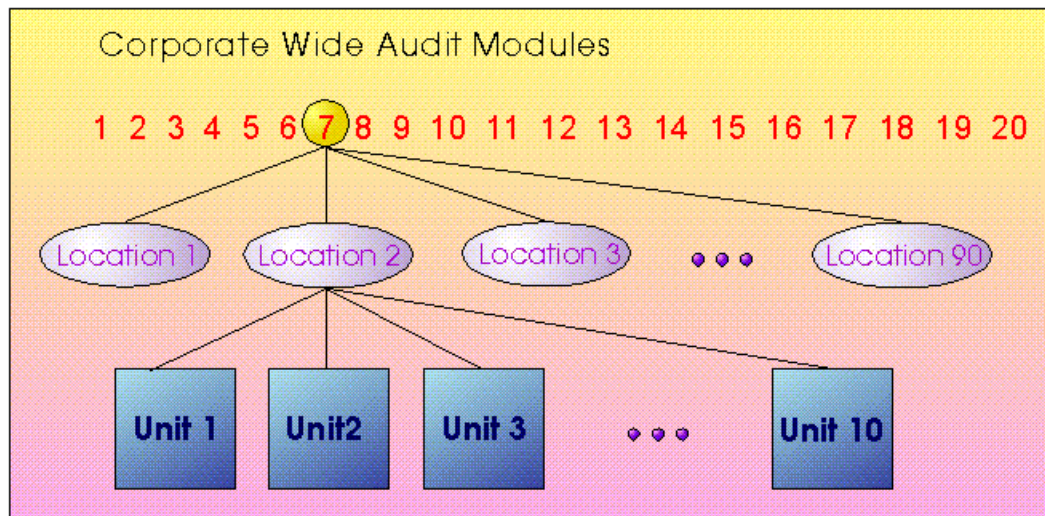
## Defining the Audit Universe

In today's corporate environment, a company may have several lines of business with operations across the globe, and may exhibit a myriad of authority/responsibility and reporting structures. In order that the auditor not get lost in the complexity of corporate structures, an organized "inventory" of all significant auditable units should be compiled. The definition of auditable units must depend on specific organizational characteristics; e.g., whether the enterprise is functionally organized or product-centered.

### Example

Figure 2 represents a banking organization, one of the case studies described in *Planning for the Internal Audit Function*, by J. E. Boritz (IIARF, 1983).

Figure 2: Defining the Audit Universe



This organization consists of 90 locations (branches). Within each branch there are 10 units (departments). In addition, there are 20 corporate-wide audit modules (programs) that are conducted within each location. Technically, this structure can be considered to have  $20 \times 90 \times 10 = 18,000$  auditable units, representing a very large number of potential audit activities.

There are many reasonable ways of defining the audit universe in this organization. One way to define the audit universe is to establish each location as an audit unit category, with the departments viewed as subsets of each location and the corporate-wide audit programs viewed as further subsets of those departments. A different way of defining the audit universe is to identify the departments as the audit unit categories, with locations being subsidiary to them, and the audit programs as further subdivisions at locations. Yet another way of defining the audit universe is to define the corporate-wide audit programs as the audit unit categories, with the 90 locations and their respective departments subsidiary to them.

**Don't:** simply accept the existing list of audit projects and activities, or worse yet, just list the names of audit files to compile the audit universe. Don't treat your audit universe as one big list — applying one risk model to heterogeneous audit units is likely to yield poor results.

**Do:** look at the entity the same way that management views the organization to identify the most appropriate definition of the audit universe and its elements to permit an effective evaluation of risks and concerns. Analysis of business objectives, management processes, organizational relationships, information systems, and interviews with top management could all help in establishing appropriate definitions of auditable units. Typically, this will mean identifying *families* of audits within the universe that share similar risk characteristics so that different risk models can be applied to them.

#### Case Study: Example, Inc.

Example Inc. is a small but diverse company. It has two divisions with very different risk characteristics. However, there is only one internal audit department, which performs the audits for both divisions. The internal audit manager in charge decided that two families of files should be used, one for each division. This facilitates having different risk models for each division.

It also has the benefit of separating calculations based on financial data where there might not be any direct relationship between the divisions. For example, the DOLLAR SIZE values for the audit units in Division 1 may be much larger than those for Division 2 and yet not represent higher risk for audit units in Division 1.

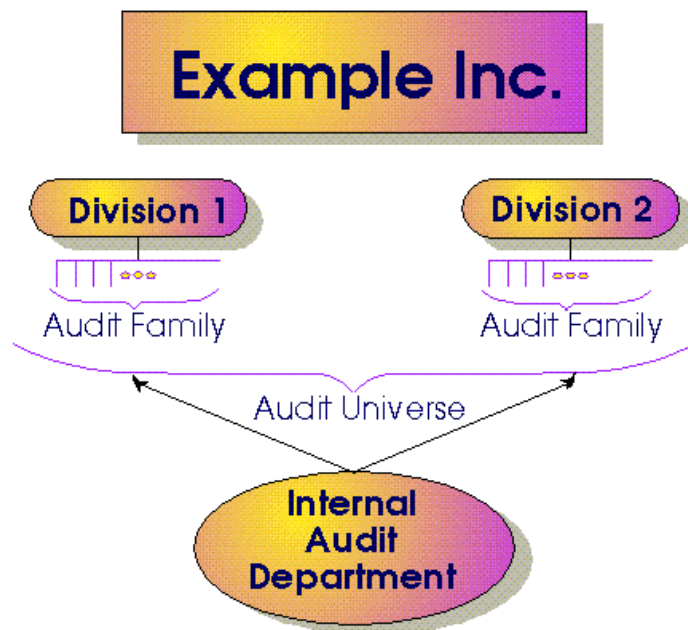


Figure 3 shows the structure of Example Inc.'s audit universe in detail.

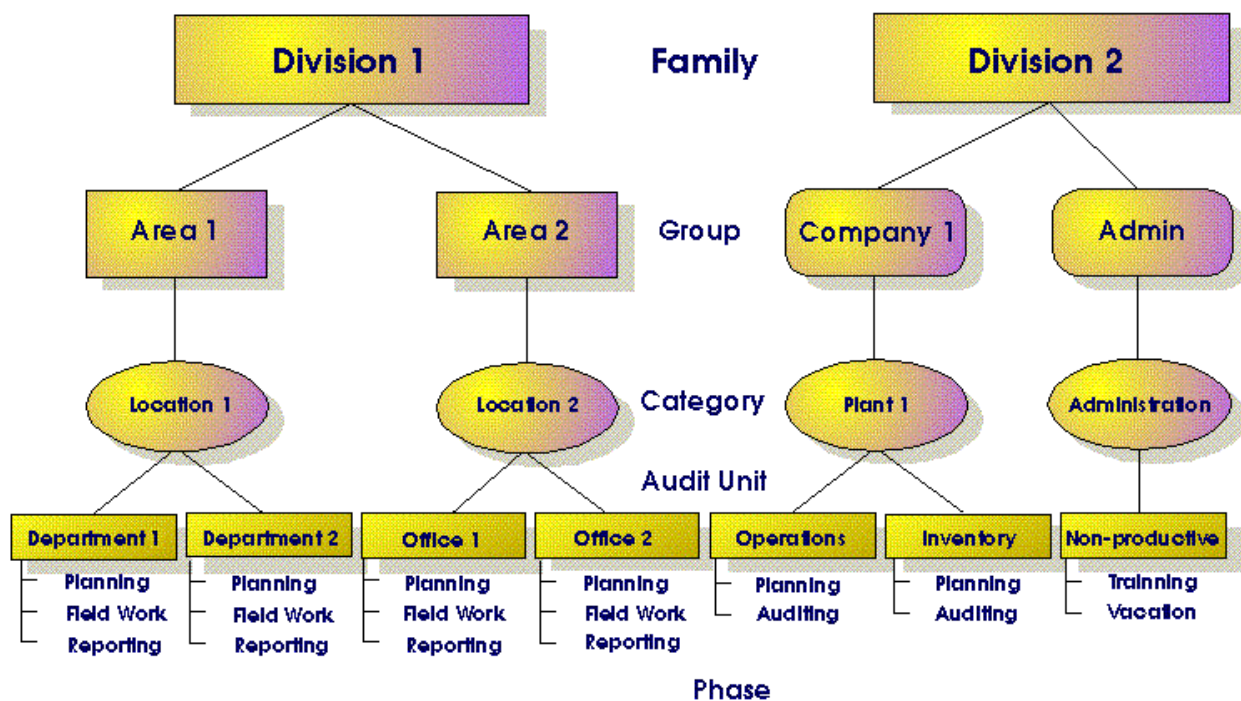


Figure 3: Example Inc. Audit Universe Structure

An auditable unit is the smallest entity in an organization which would be considered for risk assessment. This is also the level at which financial data can be recorded. Audit categories are collections of audit units that have some risk characteristics in common. Risk assessment can be performed at both the audit unit and the audit category levels. By performing risk assessment at the category level, you are indicating the risk characteristics of all the audit units in that category. The audit group is used for reporting purposes only. Reports can be sorted, selected, and sub-totaled by audit group.

Audit phases are steps in performing an audit. Phases can be used for purposes of detailed scheduling and time/cost tracking. The phase percentage makes it possible to break the budgeted hours for an audit up into the number of hours required for each Phase.

Tables 1 and 2 provide a breakdown of the audit phase percentages for DIV1 and DIV2 respectively.

**Table 1: Audit Phases for DIV1**

DIV1 Phases	%
Planning	20
Field Work	50
Reporting	30

**Table 2: Audit Phases for DIV2**

DIV2 Phases	%
Planning	40
Auditing	60
Non-Productive	%
Training	40
Vacation	60

Table 3: Audit Information for DIV1

Group: Area 1 – Category: Location 1 – Number: 1-1			
Unit Name: Department 1	Number:1-1-1		
Number of Employees:	35	Transaction Volume:	20,000
Dollar Size:	30,000,000	Dollar Throughput:	15,000,00
Standard Hours:	100	Standard Rate:	50
Standard Overhead:	3,000		
Last Audit Hours:	95	Last Audit Expenses:	2,750
Last Audit Start Date:	3/24/12	Last Audit Finish Date:	4/05/12
Unit Name: Department 2	Number:1-1-2		
Number of Employees:	23	Transaction Volume:	35,000
Dollar Size:	23,000,000	Dollar Throughput:	20,000,000
Standard Hours:	80	Standard Rate:	50
Standard Overhead:	1,350		
Last Audit Hours:	80	Last Audit Expenses:	1,500
Last Audit Start Date:	11/03/14	Last Audit Finish Date:	11/12/14
Group: Area 2 – Category: Location 2 – Number: 2-2			
Unit Name: Office 1	Number: 2-2-1		
Number of Employees:	54	Transaction Volume:	200,000
Dollar Size:	110,000,000	Dollar Throughput:	75,000,000
Standard Hours:	150	Standard Rate:	50
Standard Overhead:	7,500		
Last Audit Hours:	150	Last Audit Expenses:	7,000
Last Audit Start Date:	6/01/14	Last Audit Finish Date:	6/24/14
Unit Name: Office 2	Number: 2-2-2		
Number of Employees:	27	Transaction Volume:	95,000
Dollar Size:	45,000,000	Dollar Throughput:	23,000,000
Standard Hours:	110	Standard Rate:	50
Standard Overhead:	1,800		
Last Audit Hours:	110	Last Audit Expenses:	1,500
Last Audit Start Date:	4/10/15	Last Audit Finish Date:	4/27/15

Table 4: Audit Information for DIV2

Group: Company 1 – Category: Plant 1 – Number: 1-1			
Unit Name: Operations	Number:1-1-1		
Number of Employees:	210	Transaction Volume:	45,000
Dollar Size:	350,000,000	Dollar Throughput:	200,000,000
Standard Hours:	300	Standard Rate:	50
Standard Overhead:	2,500		
Last Audit Hours:	300	Last Audit Expenses:	1,500
Last Audit Start Date:	10/05/14	Last Audit Finish Date:	5/28/15
Group: Company 1 – Category: Plant 2 – Number: 1-2			
Unit Name: Inventory	Number:1-2-1		
Number of Employees:	95	Transaction Volume:	45,000
Dollar Size:	600,000,000	Dollar Throughput:	200,000,000
Standard Hours:	240	Standard Rate:	50
Standard Overhead:	1,500		
Last Audit Hours:	240	Last Audit Expenses:	1,500
Last Audit Start Date:	5/02/15	Last Audit Finish Date:	5/28/15
Unit Name: Non-productive	Number: 2-2-1		
Number of Employees:	0	Transaction Volume:	0
Dollar Size:	0	Dollar Throughput:	0
Standard Hours:	180	Standard Rate:	0
Standard Overhead:	0		
Last Audit Hours:	0	Last Audit Expenses:	0
Last Audit Start Date:	0/00/00	Last Audit Finish Date:	0/00/00



## Risk Criteria or Factors

A critical step in any risk assessment approach is to identify the risk factors which will be used for assessing risk. An auditable unit’s Risk Score should reflect the unit’s potential for causing or permitting losses to the enterprise, including the likelihood, magnitude, and imminence of potential losses.

### Example

The following risk factors were identified in a survey conducted by James M. Patton, John H. Evans and Barry L. Lewis in their 1983 IIA Research Monograph, *A Framework for Evaluating Internal Audit Risk*, as the most commonly used criteria for assessing risk.

- Quality of the internal control system
- Competence of management
- Time since last audit
- Liquidity of assets
- Complexity of transactions
- Distance from the main office
- Changes in accounting systems
- Unit size
- Level of employee morale

Additional criteria based on case studies may be found in *Planning for the Internal Audit Function*, by J. E. Boritz, published by the Internal Auditors Research Foundation in 1983.

**Don’t:** base risk factors on auditors’ considerations alone.

**Do:** involve management personnel in identifying risk factors and ranking them according to their relative importance. This will improve communications between the internal audit department and management and help to ensure that the audit coverage plans and staffing requirements that result from the risk assessment process will be more credible and better accepted.

### Case Study: Example, Inc. — Defining Risk Factors

Risk factors are criteria used for setting audit priorities for audit units. The manager in charge of Example Inc. has identified the risk factors listed in Tables 5 and 6 as being an appropriate basis for prioritizing audit activities.

Tables 5 and 6 list the risk models selected for DIV1 and DIV2 respectively. Each figure contains the risk factor category names and their chosen weights indicating the categories’ relative importance to other categories, followed by the categories’ specific risk factors and chosen weights.

**Table 5: Risk Model for Division 1**

Risk Factor Category	Specific Risk Factor	Chosen Weight
Size		7
	Number of Emps	2
	Dollar Size	7
	Dollar Thruput	6
	Transaction Vol	3
Audit Recency		9
	Last Audit Date	7
Management		3
	Competence	7
	Integrity	6
	Turn-over	4
	Employee Morale	2
External		1
	Public Exposure	3
	Regulations	7
	Econ. Cond.	3



Table 6: Risk Model for Division 2

Risk Factor Category	Specific Risk Factor	Chosen Weight
Size		2
	Number of Emps	2
	Dollar Size	7
	Dollar Thruput	6
	Transaction Vol	3
Audit Recency		3
	Last Audit Date	7
Management		8
	Competence	7
	Integrity	6
	Turn-over	4
	Employee Morale	2
Operations		6
	Op. Complexity	4
	Changes	8
	Distribution	3
	Growth	5

Now that the Risk Factors and their Categories are defined, we can evaluate their importance relative to one another. In this case study, we will use the direct assessment approach on the assumption that we have previously determined relative importance scores for the risk factors.

Risk Assessment Methods

After relevant criteria for establishing relative loss riskiness of auditable units have been identified, the next step is to use them in an organized fashion to arrive at a Risk Score for each auditable unit. There are two fundamental ways, not necessarily mutually exclusive, of estimating the riskiness of an auditable unit: 1) Objective assessment methods, and 2) Subjective assessment methods.

Objective Risk Assessment Methods

It is possible to set priority scores objectively by reference only to quantitative attributes of auditable units (e.g., dollars of throughput, value of assets, number of personnel, volume of transactions, the time elapsed since last audit). By making the largest attribute value represent the highest number on a rating scale (e.g., 100 on a 1-100 rating scale), and taking a simple ratio for each unit relative to this value, all units can be easily ranked.

Example

Table 7 illustrates the use of five risk factors: revenues, expenses, assets, transaction volume and time elapsed since the last audit.

Table 7: Risk Assessment Based on Objective Factors

Risk Exposure/Concern Factors												
Auditable Unit	Revenues		Expenses		Assets		Trans Volume		Time since last audit		Total	
	0	5	0	5	0	5	0	5	0	5	0	25
ABC	3		2		2		3		4		14	
ABD	2		2		2		2		2		10	
ABE	4		2		3		3		4		16	
etc.											etc.	

These risk factors are equally weighted; that is, each risk factor is worth the same number of points. Furthermore, they are objectively determinable. A computer program uses the objective values of the revenues, expenses, assets, transaction volumes and time elapsed since the previous audit for each auditable unit and simply assigns them a relative score using a 5-point scale. These scores are then totaled, with the unit with the highest score representing the unit with highest degree of concern. You will notice also that four of the five specific factors can be considered to be subsidiary to an implicit risk factor category we could call **size**.

In this particular organization, overriding importance and prominence is given to measures of audit unit **size**, with only one other factor being used, time since last audit. No subjective factors are used. The internal audit department from which this illustration was obtained wanted a simple and relatively mechanistic risk assessment approach because it was deemed not possible to make meaningful judgmental ratings for its more than 4,000 auditable units.

Subjective Assessment Methods

There are four main ways of making subjective assessments of risk factor importance; i.e., direct assessments, pairwise comparisons, base rate comparisons, and group judgments. These methods are not necessarily mutually exclusive, and can be used in various combinations.

• Direct Assessment Method

Using a subjective method of evaluation, for each risk factor for each auditable unit, a subjective assessment about risk is made using an importance scale (e.g., a scale ranging from 1-10) representing degrees of concern. These ratings may be simply totaled, or first weighted, then totaled, arriving at each unit's priority score.

Example

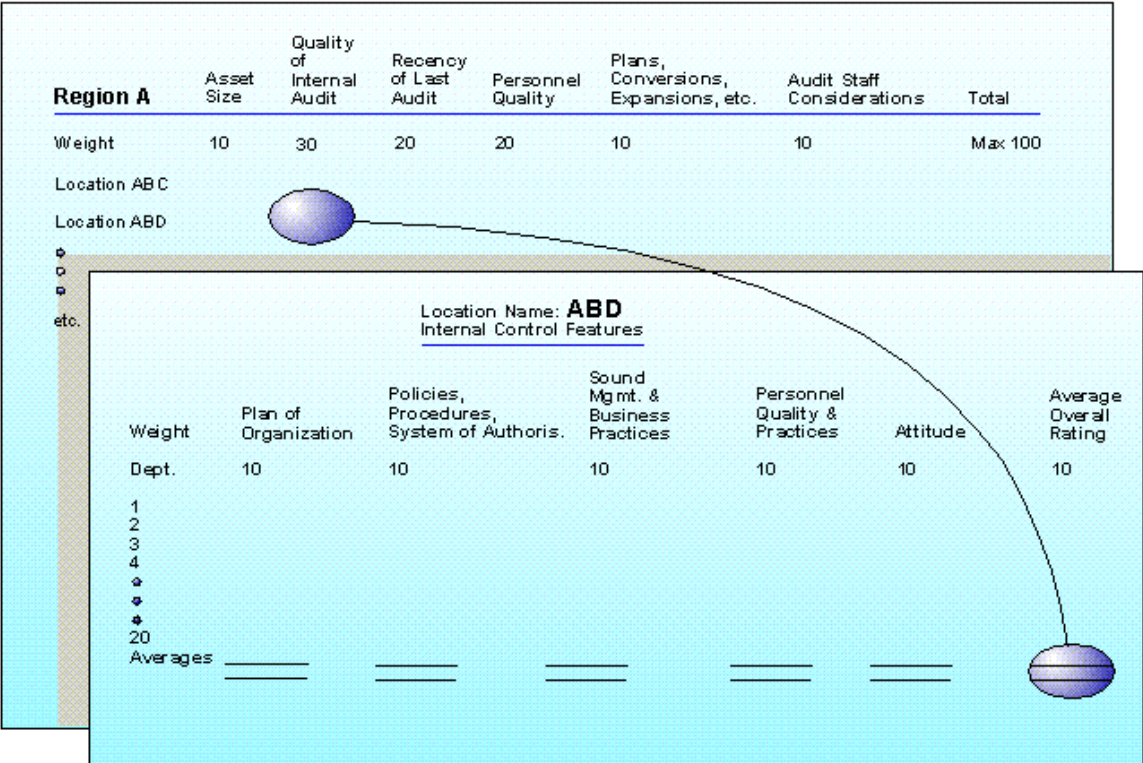
Figure 4 illustrates this approach for a banking organization with several departments at each of about 100 branches.

Across the top are listed the risk factors: asset size, the quality of internal control, the recency of the last audit, personnel quality within a branch, whether there are planned conversions, expansions, etc., and whether there are any overriding audit staff considerations.

These factors provide much more scope for subjective judgment than the previous example. In this case, asset size accounts for only 10 out of a possible 100 points, with another 20 out of 100 points being allocated to another relatively objective measure, recency of last audit. Together, the two objective factors account for 30% out of a possible 100% score, with the other factors being relatively subjective. Another interesting aspect of this example is that the risk factors are themselves constructed in a hierarchy. That is, the quality of internal control score, which is the most important score, having a value of 30 out of 100 points, has a subsidiary set of factors which are evaluated in order to arrive at the quality of internal control rating.

For example, for location ABD, internal control would be rated using 5 sub-factors. In this particular case, all the sub-factors are equally weighted. Each is worth 10 points. For each location, each of the different departments is rated on a scale of 1 to 10 as to the strength of the plan of organization, policies and procedures in force, and so forth. Eventually, the overall grand average of the 5 scores, over all the departments within the location, would be carried forward and converted to a score out of 30; for example, if a rating averaged 4 out of 10 on ABD internal control features, then this would translate into 12 out of 30 on the quality of internal control score. The scores on all of the factors for location ABD would be combined to arrive at a score out of 100, and this score would be compared against similar scores derived for each of the locations in the audit universe.

Figure 4: Risk Assessment Based on Objective and Subjective Factors



We can calculate risk factor evaluations for the calculated risk factors using the financial information recorded for the audit units.

**Table 8: Audit Unit Category Evaluations for DIV1**

	Chosen Weight
Category: Location 1	
Competence	3
Integrity	2
Turn-over	2
Employee Morale	3
Public Exposure	2
Regulations	1
Econ. Cond.	2
Category: Location 2	
Competence	8
Integrity	7
Turn-over	8
Employee Morale	9
Public Exposure	9
Regulations	8
Econ. Cond.	7

**Table 9: Audit Unit Evaluations for DIV1**

	Chosen Weight
Audit Unit: Department 1	
Competence	7
Integrity	8
Turn-over	8
Employee Morale	9
Public Exposure	7
Regulations	8
Econ. Cond.	7
Audit Unit: Department 2	
Competence	3
Integrity	4
Turn-over	2
Employee Morale	3
Public Exposure	2
Regulations	1
Econ. Cond.	3
Audit Unit: Office 1	
Competence	7
Integrity	9
Turn-over	7
Employee Morale	8
Public Exposure	9
Regulations	7
Econ. Cond.	7
Audit Unit: Office 2	
Competence	2
Integrity	4
Turn-over	3
Employee Morale	2
Public Exposure	3
Regulations	3
Econ. Cond.	2

Now that all the evaluations are recorded, we can calculate the Priority Scores.

Table 10: Audit Unit Category Evaluations for DIV2

	Chosen Weight
Category: Plant 1	
Competence	9
Integrity	9
Turn-over	8
Employee Morale	9
Op. Complexity	9
Changes	8
Distribution	8
Growth	7
Category: Plant 2	
Competence	3
Integrity	3
Turn-over	2
Employee Morale	2
Op. Complexity	3
Changes	3
Distribution	2
Growth	1
Category: Administration	
Competence	0
Integrity	0
Turn-over	0
Employee Morale	0
Op. Complexity	0
Changes	0
Distribution	0
Growth	0

Table 11: Audit Unit Evaluations for DIV2

	Chosen Weight
Audit Unit: Operations	
Competence	8
Integrity	8
Turn-over	6
Employee Morale	7
Op. Complexity	8
Changes	7
Distribution	8
Growth	9
Audit Unit: Inventory	
Competence	2
Integrity	4
Turn-over	3
Employee Morale	4
Op. Complexity	3
Changes	4
Distribution	3
Growth	2
Non-Productive	
Competence	0
Integrity	0
Turn-over	0
Employee Morale	0
Op. Complexity	0
Changes	0
Distribution	0
Growth	0

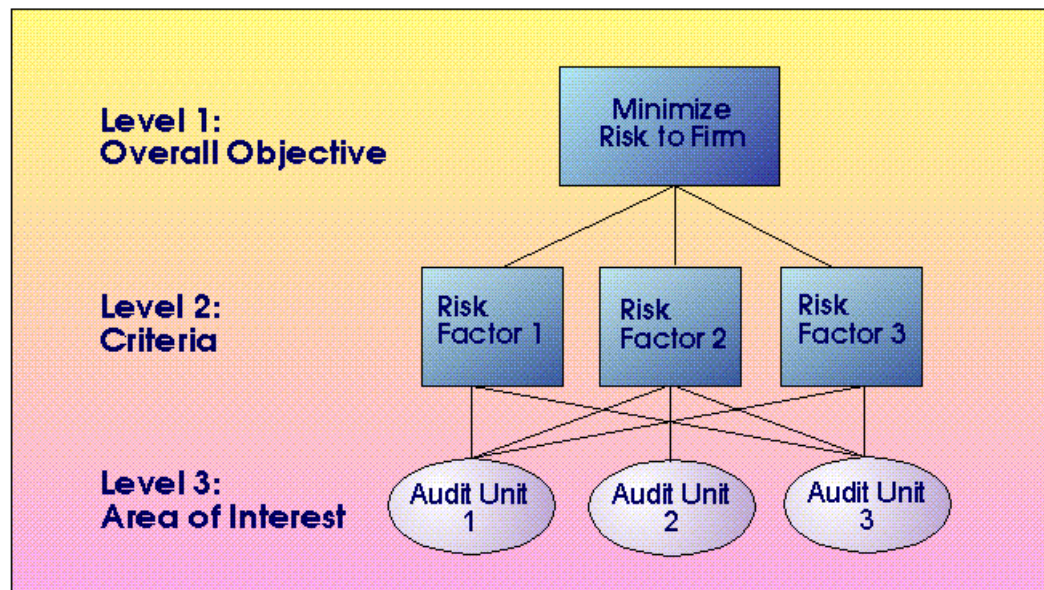


## Pairwise Comparison— The Analytic Hierarchy Process

The Analytic Hierarchy Process (AHP) is a method developed by T. L. Saaty for hierarchically decomposing complex judgments and, via simple comparisons among the components, deriving numerical scores representing their relative importance or value. One of the significant strengths of AHP is that it can measure the degree of inconsistency present in the pairwise judgments, and thereby help ensure that only justifiable rankings are used as the basis for audit plans.

Assume that three risk factors are identified as being appropriate for measuring the degree of risk/concern/exposure associated with audit units. All three risk factors may apply to each and every auditable unit within the organization. So, each audit unit must be evaluated with respect to each risk factor as indicated by the crisscrossing lines in Figure 5.

Figure 5: Analytic Hierarchy Structure of Risk Assessment



### Example

With reference to Figure 5, assume that the objective is to minimize losses, as represented by risk to the firm as a whole. Further, assume that three audit units are being evaluated using three risk factors: Size, Quality of Internal Control and Complexity of Operations.

For each audit unit, this would result in the following three sets of pairwise comparisons:

1. Size vs. Quality of Internal Control
2. Size vs. Complexity of Operations
3. Quality of Internal Control vs. Complexity of Operations

With respect to each audit unit the rater(s) might be asked, "Which risk factor is more important? Risk factor 1 or risk factor 2?" "By how much?" For each audit unit, all pairs of risk factors are compared, one pair at a time, and a number from 1 to 9 is assigned to the one representing greater concern using a rating scale such as the one illustrated in Figure 7 and using a format such as the one illustrated in Figure 6. By making these simple pairwise judgments, it is possible to fill out a table of such comparisons. AHP uses a mathematical technique, eigenvector scaling, for translating these pairwise ratings into numerical scores representing the importance or riskiness of each individual audit unit.

One of the significant strengths of AHP is that it can measure the degree of inconsistency present in the pairwise judgments, and thereby help ensure that only justifiable rankings are used as the basis for audit plans. For example, assuming that Quality of Internal Control was the most important of the three risk factor categories, followed by Size and Complexity of Operations, a consistent set of pairwise comparisons would be as follows:

1. Quality of Internal Control > Size
2. Size > Complexity of Operations
3. Quality of Internal Control > Complexity of Operations

In contrast, an inconsistent set of pairwise comparisons would be as follows:

1. Quality of Internal Control > Size
2. Size > Complexity of Operations
3. Complexity of Operations > Quality of Internal Control

Taking the above example further, numerical scores are assigned to represent the degree to which one risk factor category is more important than another. A consistent set of ratings is:

- 1. Quality of Internal Control > Size by 2
- 2. Size > Complexity of Operations by 2
- 3. Quality of Internal Control > Complexity of Operations by 4

In contrast, an inconsistent set of pairwise comparisons would be:

- 1. Quality of Internal Control > Size by 2
- 2. Size > Complexity of Operations by 2
- 3. Quality of Internal Control > Complexity of Operations by 2

Figure 6: A Format for Recording Pairwise Comparisons

Quality of Internal Control	9 8 7 6 5 4 3 2 1 2 3 4 5 6 7 8 9	Competence of Management
Quality of Internal Control	9 8 7 6 5 4 3 2 1 2 3 4 5 6 7 8 9	Integrity of Management
Quality of Internal Control	9 8 7 6 5 4 3 2 1 2 3 4 5 6 7 8 9	Recent Changes in Systems
Quality of Internal Control	9 8 7 6 5 4 3 2 1 2 3 4 5 6 7 8 9	Size of Unit
Competence of Management	9 8 7 6 5 4 3 2 1 2 3 4 5 6 7 8 9	Integrity of Management
Competence of Management	9 8 7 6 5 4 3 2 1 2 3 4 5 6 7 8 9	Recent Changes in Systems
Competence of Management	9 8 7 6 5 4 3 2 1 2 3 4 5 6 7 8 9	Size of Unit
Integrity of Management	9 8 7 6 5 4 3 2 1 2 3 4 5 6 7 8 9	Recent Changes in Systems
Integrity of Management	9 8 7 6 5 4 3 2 1 2 3 4 5 6 7 8 9	Size of Unit
Recent Changes in Systems	9 8 7 6 5 4 3 2 1 2 3 4 5 6 7 8 9	Size of Unit

Figure 7: AHP Response Scale

Intensity of Importance	Definition	Explanation
1	Equal importance	Two risk factors contribute equally to risk
3	Weak importance of one	Experience and judgment to be slightly more important than another
5	Essential or strong	Experience and judgment indicate one risk factor to be strongly more important than another
7	Very strong or demonstrated importance	A risk factor is very strongly more important than another; its dominance demonstrated in practice
9	Absolute importance	The evidence of the importance of one risk factor over another is of the highest possible order of affirmation
2, 4, 6, 8	Intermediate values between adjacent scale values	When compromise is needed

Base Comparison

The is method is similar to the Pairwise Comparison method except that some factor is chosen to represent a base for comparison and all other factors are evaluated in comparison with this base.

Example

Assuming Size was selected to be the Base for Comparison, for each audit unit, this would result in the following three sets of pairwise comparisons:

Figure 8: A Format for Recording Base Comparison Ratings

Quality of Internal Control	9 8 7 6 5 4 3 2 1	Size of Unit
Competence of Management	9 8 7 6 5 4 3 2 1	Size of Unit
Integrity of Management	9 8 7 6 5 4 3 2 1	Size of Unit
Recent Changes in Systems	9 8 7 6 5 4 3 2 1	Size of Unit

- With respect to each audit unit the rater(s) might be asked, "Assuming that Size of Unit represents a moderate risk score of 5, which risk factor is more important? Risk factor 1 or Size of Unit?" "Please indicate by how much?" For each audit unit, all pairs of risk factors are compared, one pair at a time, and a number from 6 to 9 is assigned to the one representing greater concern while a number from 1 to 4 is assigned to the one representing lower concern, using a format such as the one illustrated in Figure 8.

These pairwise judgments are relatively simple to make; however, the base comparison approach lacks the built-in inconsistency checks of AHP which incorporates safeguards to ensure a reliable set of ratings. On the other hand, AHP’s applicability to very large organizations may be limited because of the need for an excessive number of comparisons, whereas the other methods make a more modest demand on planning.

Group Judgments

Research has shown that groups can often make superior judgments than individuals. Groups can be nominal or interactive, face-to-face, or remote, used to working together or anonymous, and so on. The Analytic Hierarchy Process discussed in the previous section was designed for use by interacting groups.

**Don’t:** choose too many factors, poor scales for rating the factors, inappropriate methods of eliciting factor ratings.

**Do:** choose factors that are applicable, and quantitative scales (e.g., scale of 0-100, 0-9, etc.) that are consistent across various sections of the audit universe. Otherwise, they will yield inconsistent and non-comparable scores.

Usually, subjective judgment about the relative importance of risk factors cannot be avoided, especially when the benefits from auditing are intangible or difficult to predict. Depending on organizational size and characteristics, a combination of methods can be applied.

Regardless of the methods used, it is important to predefine clear guidelines for evaluating risk factors properly. Validate ratings.

Group process should be used to the maximum extent possible; e.g., have a few senior auditors go through the process together or independently correlating their ratings, identifying areas of strong disagreement. Disagreements should be discussed and a consensus reached. Alternatively, collect judgments from individuals then combine them into an overall group assessment. Such mathematically combined groups (i.e., individual judgments mathematically combined into a group score) have been found to be often superior to individual judgments.

Wherever possible, auditee and managerial personnel should be involved in carrying out some or all of the risk assessment, since often they are in the best position to perceive problems as they develop, rather than after the fact. This can be in the form of workshops to identify risk factors, surveys used to capture risk judgments, and feedback sessions designed to evaluate past audit coverage plans. Such co-operation can enhance communication between auditors and auditees, enhance mutual respect, and benefit the entire planning process.

Combining Risk Factor Assessments into an Overall Risk Score

There are many ways of combining judgments, including the mean, median, geometric mean, similar measures adjusted for outliers, and other weighted combinations

Averages

Many of the calculations performed in risk assessment involve some form of averaging.

Weighted Arithmetic Average:

$$\frac{a * M + b * N}{M + N}$$

#### Weighted Geometric Average:

$$\sqrt[M+N]{a^M * b^N}$$

#### Modified Weighted Average:

$$\frac{a * b}{9}$$

The difference between these methods of averaging is most noticeable for low input values. For example, assuming  $M = N = 1$ , the arithmetic average of  $a = 1$  and  $b = 9$  is 5, whereas the geometric average is 3, and the modified weighted average is 1. In some cases, the geometric average produces results which are more “intuitively correct” than the arithmetic average. Similarly, the modified weighted average sometimes produces results that seem most intuitively appealing.

#### Weighted Averages

Values for  $M$  and  $N$  in the above averages enable you to weight input values to reflect their relative importance. The ratio of  $M$  to  $N$  controls how much each input value influences the result.

#### Re-expression

A drawback of averages is that they tend to clump in the middle of the possible range. This clumping becomes even more pronounced if the input data tends to clump as well. Re-expression is the process of redistributing data over a whole range of acceptable values. Keep in mind that when re-expression is used it is possible that the relative riskiness rankings of some units will change.

**Don't:** choose calculations which are susceptible to masking the meaning behind the risk ratings or whose implications you do not understand..Don't go for overly complex formulations, but don't settle on simplistic methods which defeat the purpose behind undertaking the risk assessment in the first place.

**Do:** choose calculations that will yield consistent and comparable scores. Experiment with weighted averages and re-expression.

## Assigning Audit Units to Audit Frequency Categories

Once Risk Scores are developed for all the audit units, they can be sorted into a list according to their order of importance. That list can be subdivided into audit frequency categories to balance the audit intensity and audit frequency so that available resources are not exceeded. Some units will be subjected to a comprehensive audit and others to only a partial audit.



Figure 9: Cyclical Audit Coverage Plan

Priority Category		Audit Phase	Planning Horizon					
			1	2	3	4	5	6
X1		Planning	X	X	X	X	X	X
	Annual	Review and Evaluation	X	X	X	X	X	X
	Full	Testing	X	X	X	X	X	X
		Reporting	X	X	X	X	X	X
X2		Planning	X	X	X	X	X	X
	Annual	Review and Evaluation	X		X		X	
	Partial	Testing		X		X		X
		Reporting	X	X	X	X	X	X
Y1		Planning		X		X		X
	Biennial	Review and Evaluation		X		X		X
	Full	Testing		X		X		X
		Reporting		X		X		X
Y2		Planning		X		X		X
	Biennial	Review and Evaluation		X				X
	Partial	Testing				X		
		Reporting		X		X		X
Z1		Planning			X			X
	Triennial	Review and Evaluation						
	Full	Testing			X			X
		Reporting			X			X
Z2		Planning			X			X
	Triennial	Review and Evaluation			X			
	Partial	Testing						X
		Reporting			X			X

**Don't:** choose fixed cyclic audit patterns assuming that all audits are the same.

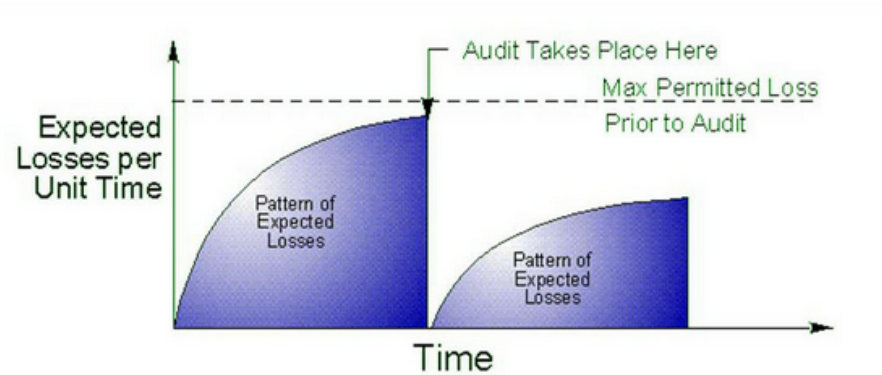
**Do:** set up several audit intensity levels and use them to set audit cost and relate them to other features of audit units besides risk scores

# A Model for Determining Optimal Audit Frequency

This section outlines the key elements which form part of the planning approach incorporated within auditMASTERPLAN®. This approach uses risk ratings, financial measures of loss potential and audit costs to calculate an optimal audit frequency given a planning horizon for the audit universe as a whole.

Figure 10 illustrates a hypothetical pattern in the growth of expected losses over time due to fraud, inefficiency, error, etc. for a given auditable unit or activity.

Figure 10: Pattern of Expected Losses over Time

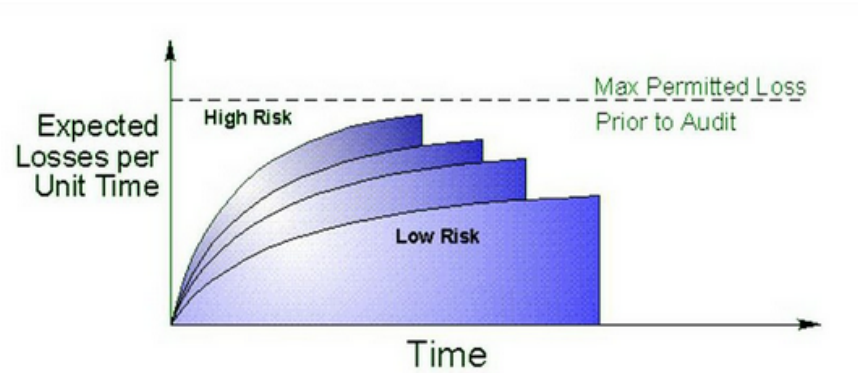


Along the vertical axis are the expected losses (in financial terms per unit of time), and along the horizontal axis is time. Losses accrue in the absence of auditing. The dotted line across the top represents a conceptual maximum. If the losses reach that point, management will automatically call for an audit; for example, if a massive fraud or other loss were to occur within an auditable unit, then, regardless of where in the auditor’s schedule a specific unit was, it would be immediately audited.

The curve represents the pattern of expected losses. The losses rise at a decreasing rate until they hit the maximum, at which point an audit is automatically called. The losses stop growing because the auditor is assumed to be effective at identifying and eliminating the cause of the losses that are occurring within an auditable unit due to fraud, inefficiency, or error. In fact, the rate of loss drops to zero for an instant. However, the auditor leaves, and the losses start growing again.

This model is valuable because it can yield a workable risk analysis approach based on theory. As Figure 10 illustrates, expected losses, in the absence of an audit, rise at some rate and that rate is represented by the steepness of the curve as pictured in Figure 11.

Figure 11: Various Loss Curves



If the curve is very steep, then this indicates that the unit is very risky and the losses accrue at a very high rate. If the curve is fairly shallow, this indicates that the unit is less risky and the losses due to fraud, waste, etc. accrue at a relatively modest rate.

Figure 12: Audit Frequency Patterns over a Planning Period

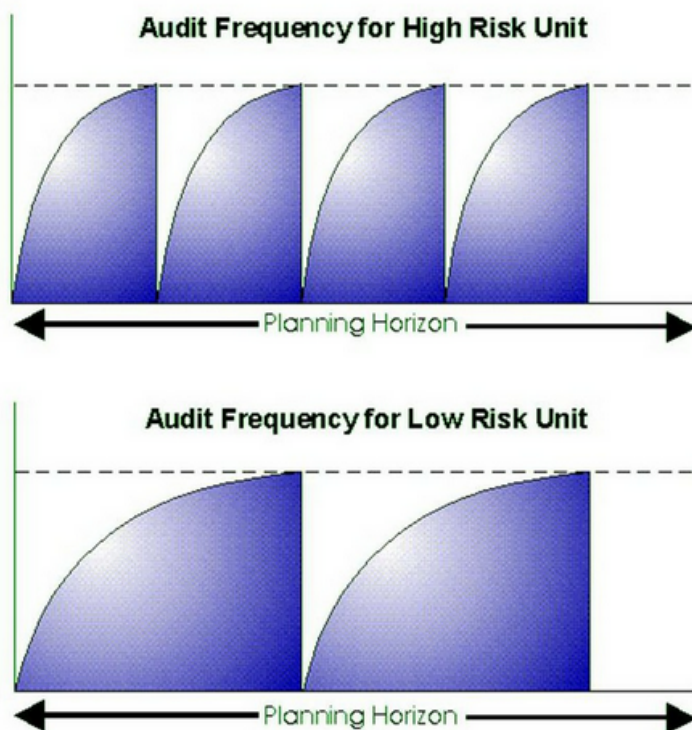
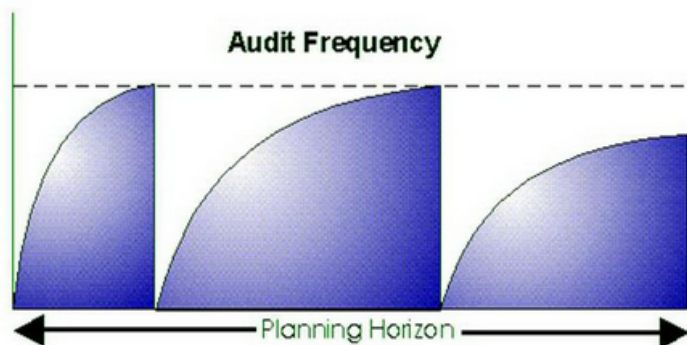


Figure 12 shows a pattern of audits taking place over the planning horizon. As the diagram indicates, if a shallower rate of losses was characteristic of a specific audit unit, then there would be fewer cycles over the planning horizon. In contrast, if the rate of expected losses was steeper, then there would be many more of these cycles within the planning horizon.

Figure 13: Audit Frequency Patterns (cont'd)



A question that sometimes arises from a consideration of these diagrams is, "Why does the auditor apparently not change, for the better, some fundamental risk characteristics of the audit unit permanently?" If he or she did, then the pattern would get progressively shallower as illustrated in Figure 13.

This diagram shows that each audit results in a shallower risk curve (e.g., stemming from worthwhile recommendations, etc.). In fact, this should be the case, otherwise it would be difficult to justify repeated auditing of the same unit.

One way of achieving approximately the same result is by updating the previous risk assessment for an audit unit at the conclusion of each audit, or more appropriately, upon completion of the follow-up visits. This revised assessment would be used to establish the appropriate timing of the subsequent audit. Upon its completion, an updated risk assessment would be used to establish the appropriate timing of the subsequent audit, and so on.

**Don't:** use fixed audit frequencies unrelated to management concerns, risk scores or audit costs. Don't make arbitrary timing choices.

**Do:** use a conditional audit frequency approach based on cost/benefit analysis. Given your audit frequency decisions, make sure that the timing of those audit activities makes sense; i.e., high risk items are front-loaded unless staff availability or other key factors intervene. Relate your audit intensity decisions to your and risk assessments and audit frequency judgments. Update your risk rating and cost data upon completion of each audit.

The next step is to record information about audit personnel, the skills they possess and the Phase-Skill relationships.

Figure 13: Audit Personnel

Name	Status
Supervisor 1	S
Auditor 1	A
Auditor 2	A

Figure 14: Audit Skills

Skill	Code	Cost
Junior	JU	40
Senior	SE	60
EDP	ES	70
Administration	AD	100

Phase-Skill Relationships need to be recorded for both DIV1 and DIV2 since the families have separate Phase files. Using Figure 15 for DIV1 and Figure 16 for DIV2, select the Phase Categories and record the Skill Percentages.

Figure 15: Phase-Skill Relationships for DIV1

DIV1 Phases	% Junior	% Senior	% EDP	% Administration
Planning	0	20	0	80
Field Work	15	75	10	0
Reporting	0	80	0	20

Figure 16: Phase-Skill Relationships for DIV2

DIV2 Phases	% Junior	% Senior	% EDP	% Administration
Planning	0	10	10	80
Field Work	0	60	40	0
Non-Productive				
Training	0	0	0	100
Vacation	0	0	0	100

## Zero-Base Budgeting

Once there is a list of audit units ordered as to their importance, it is possible to use it to help establish the appropriate size of audit department commensurate with the level of risk/coverage deemed acceptable for the organization, as illustrated in Figure 17.

Opposite each auditable unit we can record an estimated number of hours that it takes to carry out that audit. We can then add through the list until we hit the number of hours represented by current staff size. For example, assuming a department size of six employees, we may find that we can carry out eight of the most important audits on the list.

The question then arises, “What would happen if we cut back on one authorized position?” We would now only be able to carry out the first four audits on the list. Similarly, if the audit risk scores indicated that the first 10 audits needed to be incorporated into the audit plan, then it would be clear that an additional auditor would be required.

**Don’t:** use risk scores alone in your analysis; be sure to compare risk-based zero-base analyses with payoff-based analyses.

**Do:** use a zero base budgeting approach to show management and the audit committee the coverage implications of alternative staffing levels.



Figure 17: Zero-Base Budget

Audit Units in Ascending Order of Time Required	Time	Increment 1 (5 Auditors; 7,500 Hours)	Increment 2 (6 Auditors; 9,000 Hours)	Increment 3 (7 Auditors; 10,500 Hours)	Cumulative Time Requirements
Unit 8	100	100	100	100	100
Unit 7	200	200	200	200	300
Unit 6	200	200	200	200	500
Unit 11	500	500	500	500	1000
Unit 10	500	500	500	500	1500
Unit 1	500	500	500	500	2000
Unit 4	1000	1000	1000	1000	3000
Unit 9	1000	1000	1000	1000	4000
Unit 5	1500	1500	1500	1500	5500
		5500			5500
Unit 2	2500		2500	2500	8000
			8000		8500
Unit 3	2500			2500	10500
				10500	

Audit Units in Order of AUPS	Audit Unit Priority Score	Increment 1 (5 Auditors; 7,500 Hours)	Increment 2 (6 Auditors; 9,000 Hours)	Increment 3 (7 Auditors; 10,500 Hours)	Cumulative Time Requirements
Unit 1	11	500	500	500	500
Unit 2	10	2500	2500	2500	3000
Unit 3	9	2500	2500	2500	5500
Unit 4	8	1000	1000	1000	6500
		6500			6500
Unit 5	7		1500	1500	8000
Unit 6	6		200	200	8200
Unit 7	5		200	200	8400
Unit 8	4		100	100	8500
			8500		8500
Unit 9	3			1000	9500
Unit 10	2			500	10000
Unit 11	1			500	10500
				10500	

Audit Units in Order of Time "Priority"	Time	Increment 1 (5 Auditors; 7,500 Hours)	Increment 2 (6 Auditors; 9,000 Hours)	Increment 3 (7 Auditors; 10,500 Hours)	Cumulative Time Requirements
Unit 8	.0400	100	100	100	100
Unit 6	.0300	200	200	200	300
Unit 7	.0250	200	200	200	500
Unit 1	.0220	500	500	500	1000
Unit 4	.0008	1000	1000	1000	2000
Unit 5	.0047	1500	1500	1500	3500
Unit 2	.0040	2500	2500	2500	6000
Unit 10	.0040	500	500	500	6500
		<b>6500</b>			
Unit 3	.0036		2500	2500	9000
			<b>9000</b>		
Unit 9	.0030			1000	10000
Unit 11	.0020			500	10500
				<b>10500</b>	

## Defending Your Risk Assessment Methodology

External auditors are often called upon to review the activities of internal audit departments as part of their justification of their reliance on internal audit work in reducing the scope of their own work in some areas or as part of a special engagement on behalf of management or the board of directors. Long range planning activities and risk assessment methods are often an important focus of such reviews and also of related critical comments by external auditors.

**Don't:** Take shortcuts, fly by the seat of your pants, keep part of your legitimate audit universe outside the process, ignore management and auditee input, make casual, inconsistent or inappropriate judgments, override or short-circuit your formal risk assessment.

**Do:** Follow a systematic approach and document your decisions. Involve management in your risk assessment process. Show the relationship between your audit coverage decisions and your staff availability. Keep the external auditors involved. Educate them but be prepared to back up your approach.