THE INTERNAL AUDITOR COMPASS
N°11 - June 2016

The Institute of Internal Auditors BELGIUM

EVOLUTION OF AUDIT IN A CHANGING WORLD

Diane van Gils,
Auditeur IFACI Certification,
Consultant indépendant

Benoît Harel,
Directeur IFACI Certification

VERS L'AUDIT INTERNE EN DÉBIT 5G !

by Diane van Gils & Benoît Harel

L'innovation puisée dans un programme d'amélioration continue fréquemment jaugé et certifié

En 15 ans, depuis le Cadre de Référence de 2002, les auditeurs internes ont jalonné leur pratique professionnelle de multiples innovations conceptuelles, humaines et technologiques : assurance combinée, lignes de maîtrise, transformation numérique, reporting intégré, pensée critique, développement du capital humain, planification par les objectifs et risques métiers, audit continu, analyse de données, réseau social d'audit, conseiller privilégié et partenaire avec 'voix au chapitre', prise de décision stratégique, gestion de la conformité et de l'éthique...

Ces ruptures créatrices ont permis de donner un nouveau souffle à une activité nécessairement cadrée par les Normes de l'IIA. Accompagnant les révolutions de la maîtrise des risques et activités, un palier élevé de maturité professionnelle a clairement été franchi par l'audit interne !

Au cœur de cette dynamique d'innovations se trouve le programme d'assurance et d'amélioration de la qualité qui distingue notre profession par sa capacité à élever régulièrement la barre de ses exigences et de ses moyens. Aujourd'hui, plutôt rares sont les services d'audit interne performants qui n'ont pas intégré dans leurs gènes un programme d'amélioration continue fréquemment jaugé et certifié.

Même l'évaluation externe indépendante a été accélérée par cette trajectoire : à la classique revue qualité ex-post de périodicité distendue, de méthodologie un peu obsolescente et de conclusions lénifiantes, ont succédé des programmes d'évaluation stimulants, plus fréquents et orientés vers le futur, aux méthodes novatrices, aux préconisations motivantes et aux conclusions plus exigeantes.

Les multiples pratiques innovantes citées n'auraient pu prendre racine sans une solide application des exigences des Normes IIA. De leur coopération étroite, IFACI Certification (Institut Français de l'Audit et du Contrôle Internes, France) et DIIR Dienstleistungen (Deutsches Institut für Interne Revision, Allemagne) ont tiré 12 retours d'expérience. Parce que le progrès passe par le partage, les services d'audit interne souhaitant bénéficier d'un programme de Certification IIA pourront glaner dans cette sélection de 12 sujets incontournables la matière pour amorcer en 2016 leur feuille de route vers un audit interne en débit 5G !

1. UN MODÈLE DE GOUVERNANCE STRUCTURANT LA CHARTE D'AUDIT INTERNE

La charte établit le cadre et les principes d'action : elle omet bien souvent d'indiquer pourquoi et comment le service d'audit interne se concentre sur les domaines à haut risque métier, tant bruts ou nets. L'indication des responsabilités et des interactions du service d'audit interne dans le processus de management des risques est souvent omise ou dépassée dans les faits.

L'application d'un modèle de gouvernance - tel que celui des trois (The IIA) ou quatre (Financial Stability Institute) voire cinq Lignes d'Assurance, ou celui de King-II - permet de mieux structurer le rôle et la contribution de l'audit interne au système de maîtrise des risques, tout en précisant les tenants et aboutissants de l'approche fondée sur les risques métiers déclinée dans l'organisation.

2. UN PLAN DE COMMUNICATION MODULAIRE CONJUGUANT PERTINENCE ET ÉCONOMIE DE MOYENS

Le positionnement de l'audit interne souffre souvent d'une capacité restreinte à satisfaire les différentes parties prenantes, plus particulièrement au niveau des membres du comité de direction dont la diversité des profils, des préoccupations et des besoins de réassurance varie significativement, mais dont l'appui est critique pour assurer un portage efficient des plans d'actions correctives.

Un plan de communication technique vers la direction générale au sens large peut être établi autour de besoins approfondis, priorisés et validés par les dirigeants ; ce plan définit les fréquences, propose une communication modulaire et délimite les demandes spécifiques des métiers en les mettant en cohérence avec les exigences d'assurance et de consultation aux bornes de l'organisation.

3. UNE PLANIFICATION CIBLÉE SUR LES DISPOSITIFS DE MAÎTRISE DES RISQUES MÉTIERS

Le programme d'audit constitue la pierre angulaire de la démarche d'évaluation des systèmes de maîtrise de l'activité. Les méthodes multicritères de sélection des missions sont devenues complexes et consommatrices de ressources, sans que la justification des arbitrages, implicitement ou explicitement impactés par les orientations des dirigeants, en soit substantiellement améliorée. Par ailleurs, les cartographies des risques se perdent souvent dans des problématiques de cotation, alors que l'élément clé est constitué par la délimitation des dispositifs assurant la maîtrise des risques métiers.

En ce sens, l'évolution proposée de la Norme 2010 (qui rejoint la MPA 1110-1 §3) reflète bien les bonnes pratiques observées : la cartographie des risques managériale validée constitue une base de départ, puis son approfondissement impliquant la Direction Générale et le Conseil conduit à une évaluation des dispositifs de maîtrise des risques, répondant mieux aux exigences d'objectivité et d'auditabilité.

4. UNE GARANTIE QUE DES MESURES CORRECTIVES ONT ÉTÉ EFFECTIVEMENT MISES EN ŒUVRE

Le suivi des recommandations constitue souvent une pierre d'achoppement. La mesure de la maîtrise du risque après mise en œuvre du plan d'action prioritaire reste délicate : l'analyse de sa pérennité et de son efficacité est souvent fragile.

Outre le soin apporté au ciblage des causes et à la rédaction pragmatique de la recommandation, un jalon dédié doit rapidement permettre la vérification de fond de l'adéquation du plan d'action et des critères quantifiés de bonne maîtrise du risque. Au moment de la clôture de la recommandation, les preuves et assertions du management ne suffisent pas : la garantie donnée par l'audit interne sur les mesures prioritaires (2500-A1) doit être soutenue par des vérifications minimales d'efficacité et de pérennité complétées par une supervision robuste.

5. UNE MISE EN PERSPECTIVE PLURIANNUELLE DE LA MAÎTRISE DES PRINCIPAUX RISQUES MÉTIERS

Le rapport d'activité à la Direction Générale et au Conseil est généralement un document bien construit sur le fond et la forme. Toutefois, l'agrégation des synthèses des missions individuelles est peu souvent prolongée par une évaluation d'ensemble des systèmes de maîtrise des activités, et à la mise en évidence des problématiques sur lesquelles l'action des dirigeants exécutifs et l'attention des administrateurs est requise.

Une évaluation thématique et systémique de la maîtrise des principaux risques métiers, mise en perspective pluriannuelle, constitue la clé de voûte d'une communication d'audit à forte valeur ajoutée. Cette évaluation doit être anticipée dans son périmètre et alimentée tout au long de l'exercice par un processus continu, cumulatif et itératif.

6. UNE DÉMARCHE DE CONVERGENCE FONCTIONNELLE DES SERVICES DE CONTRÔLE

La coordination entre fonctions de contrôle constitue pour le directeur d'audit interne un levier nécessaire afin de relayer les démarches de maîtrise des activités sur plusieurs niveaux organisationnels, de répartir la charge des travaux d'évaluation et de consultation, et d'alimenter des synthèses cohérentes pour la Direction Générale. Cette coordination s'appuie le plus souvent sur des échanges réguliers, des outils partagés et des comités managériaux ; toutefois, cette coordination se traduit moins souvent par une couverture démontrée des principaux risques métiers, par l'utilisation de référentiels compatibles nécessaire à une assurance combinée, par une confirmation suffisante des compétences, du périmètre, des objectifs et des méthodes des autres fonctions de contrôles.

Dans ce cadre, la réalisation d'une cartographie des fonctions de contrôle au regard des principaux risques métiers peut être complétée par une démarche de convergence des référentiels de contrôle, des échelles d'évaluation et des rapports de synthèse, fondée sur une comitologie plus dense et proactive.

7. UN AVIS STRUCTURÉ ET MOTIVÉ SUR L'ADÉQUATION DE LA GOUVERNANCE DES SYSTÈMES D'INFORMATION

L'audit interne doit évaluer si la gouvernance des systèmes d'information de l'organisation est adéquate afin de soutenir sa stratégie et ses objectifs, dans les domaines managérial, opérationnel et de support. Si des audits de grands projets sont complétés par certains audits de processus informatiques, les conclusions de ces travaux sont moins souvent consolidées pour rendre lisible la pertinence de la gouvernance des systèmes d'information.

Le recours au guide d'audit CIGREF-IFACI-AFAI fondé sur 12 vecteurs ou au référentiel COBIT5 constitue un socle pour reporter un avis structuré et motivé sur l'adéquation de cette gouvernance des systèmes d'information.

8. UN PLAN DE DÉVELOPPEMENT ORGANISÉ AUTOUR DE PÔLES DE COMPÉTENCES

Un ralentissement du rôle de pépinière de talents est observable dans un certain nombre d'organisations ; le taux de rotation moyen des services certifiés IIA-IFACI est par exemple passé sous la barre de 25% en 2015. D'autre part, une sollicitation croissante de développement de pôles de compétence ressort des comités de direction ou d'audit, dans les domaines opérationnels et fonctionnels.

Les services d'audit interne en pointe répondent à ces challenges en établissant un parcours de carrière en forme de mastère interne avec des modules d'expertise clairement identifiables pour l'organisation, des prises de responsabilités croissantes et successives, et surtout le développement de spécialités majeures et mineures, grâce à une combinaison de missions et formations ; une contractualisation de ce parcours avec les Ressources humaines et les Directions métiers contribue à redonner de la fluidité interne, à renforcer l'attractivité du service d'audit et à valoriser les potentiels des auditeurs internes.

9. L'INTRODUCTION DE MÉTHODES D'AUDIT FONDÉES SUR LA RÉINGÉNIERIE DES SYSTÈMES ET PROCESSUS

Les auditeurs internes réalisent les vérifications du plan de travail et classent faits et preuves nécessaires à l'évaluation des activités auditées. Toutefois, la capacité des auditeurs à fonder leurs conclusions et le résultat de leur mission sur des analyses appropriées est souvent appelée à progresser: réaliser une démonstration convaincante, effectuer une revue analytique probante, faire parler indicateurs et échantillons, corroborer une preuve d'audit, conclure sur l'efficacité d'un contrôle... nécessitent souvent de combler quelques lacunes.

Plusieurs services ont choisi de doter leurs auditeurs en méthodes 'lean six sigma' : le recours à ces outils renforce la pensée critique tout en améliorant sensiblement le rendement des tests. Que ce soit dans la définition des objectifs, la mesure des réalisations, l'analyse des déficiences, l'amélioration de la satisfaction des clients, les méthodes ainsi appliquées structurent l'objectivité des évaluations, ainsi que la profondeur et la dimension métier des recommandations.

10. UN LEVIER RÉALISÉ SUR LES CONTRÔLES APPLICATIFS ET LES INDICATEURS MÉTIERS

Une marge de progrès est régulièrement observée en matière d'évaluation des contrôles applicatifs. Le traitement informatisé de données s'est imposé comme le facteur clé de succès de la quasi-totalité des processus, programmes et projets critiques de la plupart des organisations. Dans le même temps, l'évaluation des contrôles applicatifs -tels que les états de contrôle, d'interfaces

et de configuration, les rapports d'anomalies, d'exceptions et de modifications, les traitements de réconciliations et les indicateurs de performance- est plutôt minimisée. Les programmes de tests privilégient en général la comitologie ainsi que les processus et activités opérés directement par les audités.

Les services d'audit interne proactifs établissent en phase d'étude une sélection de contrôles applicatifs inattendus au regard des risques, puis rééquilibrent le programme de tests par des angles inédits d'attaque des données. Ils s'appuient sur des indicateurs métiers renouvelés pour s'extraire des approches habituelles en examinant les données opérationnelles à la marge du domaine audité, que permet seule la capacité d'auditer de bout en bout les informations d'un projet ou d'un processus.

11. UNE SUPERVISION MIEUX ANTICIPÉE, PLUS APPROFONDIE ET ORIENTÉE MÉTIER

La supervision constitue la pierre angulaire de la mission d'audit : elle en organise l'approche, elle en vérifie le déroulement objectif, et assure une communication de haute qualité des résultats et conclusions. Toutefois, l'examen différentiel des livrables jalonnant la mission souligne un apport métier limité de la supervision : note d'orientation générique, revue préliminaire manquant de déclinaison opérationnelle, programme de travail peu retouché, tests non concluants non retoqués, corrections de forme des rapports etc...

Le directeur de missions fournit en entrée de mission à l'équipe une monographie professionnelle et concise du domaine audité, élaborée depuis l'approbation du plan d'audit. La note de cadrage qui en reprend le développement est co-construite avec ce superviseur qui y apporte son expertise fonctionnelle. Le plan d'approche, à la main de l'équipe d'audit, fait l'objet d'un exposé de validation à l'équipe de direction du service. En aval, l'analyse causale et les recommandations sont challengées par le superviseur pour en enrichir la dimension métier et l'opérabilité dans le cadre des orientations stratégiques.

12. UN PLAN DE DÉVELOPPEMENT STRATÉGIQUE DE L'AUDIT INTERNE

Les services d'audit interne disposent maintenant d'une solide cartographie de leurs propres risques et d'un système qualité qui forme l'ossature de leur propre contrôle interne. Toutefois, ils établissent moins souvent une feuille de route mettant en cohérence mission, vision, offre de services, buts et moyens de cette ambition à moyen terme : leur horizon temporel se porte sur le plan d'audit annuel.

S'appuyant sur le Guide Pratique « Développer le plan stratégique de l'audit interne », plusieurs services projettent leurs initiatives innovantes en perspective des objectifs d'apport de valeur pour leur organisation. Sur la base d'un nombre ciblé de piliers stratégiques, ils planifient les investissements, actions critiques et mesures, alliances internes et externes nécessaires à la réingénierie de l'audit interne ; ils mettent en relief les pôles de compétences et d'expertise à développer dans le cadre de l'horizon stratégique ou de transformation de leur organisation.

CONCLUSION : VERS L'AUDIT INTERNE EN DÉBIT 5G

Au travers de cette sélection de 12 points clés, la profession d'audit interne va de l'avant sur la base d'un socle solide de pratiques, pépinière d'innovations éprouvées ou encore balbutiantes, mais sans conteste proactives dans des organisations qui s'appuient sur l'audit interne, partenaire de confiance pour éclairer leurs décisions et réassurer en débit 5G le déploiement des programmes d'optimisation et de transformation de ces organisations. IFACI Certification propose un panel (Encadré n°1) de services permettant d'atteindre une vitesse supérieure, où l'innovation prend racine dans une solide application des Normes IIA. L'Encadré n°2 permet d'illustrer le potentiel d'une Évaluation Maturité de l'Audit interne proposée dans le panel de services IFACI Certification, au regard de l'analyse des niveaux actuels de maturité.

ENCADRÉ n°1 - Les Services d'Évaluation des Directions d'Audit Interne IIA-IFACI

La Certification Qualité conduit à délivrer un label de qualité aux directions d'audit interne qui appliquent les vingt-cinq exigences éprouvées et concrètes du Référentiel Professionnel de l'Audit Interne. Ce Référentiel, issu des Normes Internationales d'Audit Interne, présente les prérequis et forme le tronc commun de notre profession, assurant une pratique exercée dans les règles de l'art.

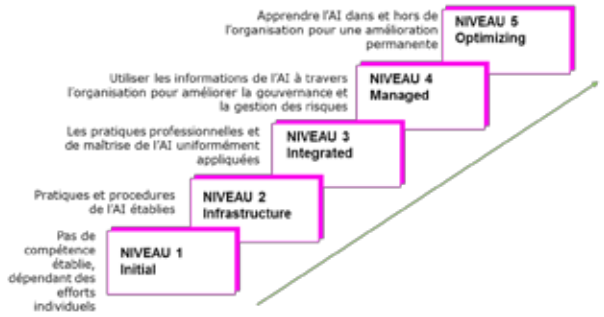
L'Évaluation Maturité transforme l'Audit Interne en acteur d'innovation, en vecteur de concepts précurseurs et de pratiques prospectives, pour une demande de percée organisationnelle, technologique et méthodologique. L'Évaluation Maturité est réalisée avec un modèle intégrant l'essentiel des sujets d'avenir de la profession d'audit, par une approche stimulant la prise de hauteur, l'anticipation et la clarification des besoins.

L'Évaluation Performance permet à l'Audit Interne de conduire un processus de recherche, d'analyse comparative, d'adaptation et d'implantation de pratiques fluides et efficaces. L'Évaluation Performance permet de revenir aux actions essentielles du cycle d'audit, de réduire la récurrence et l'impact des défauts de processus, de maximiser l'impact des interactions avec les parties prenantes et de transformer des contraintes organisationnelles en opportunités de développement.

ENCADRÉ n°2 – Modèle de Maturité de l'Audit interne

L'IIA Research Foundation a développé un modèle de maturité composé de 5 niveaux de maturité.

Ce référentiel est construit sur base de pratiques essentielles permettant aux services d'audit interne de s'élever à un niveau de maturité plus abouti et de le pérenniser au sein de leur organisation.

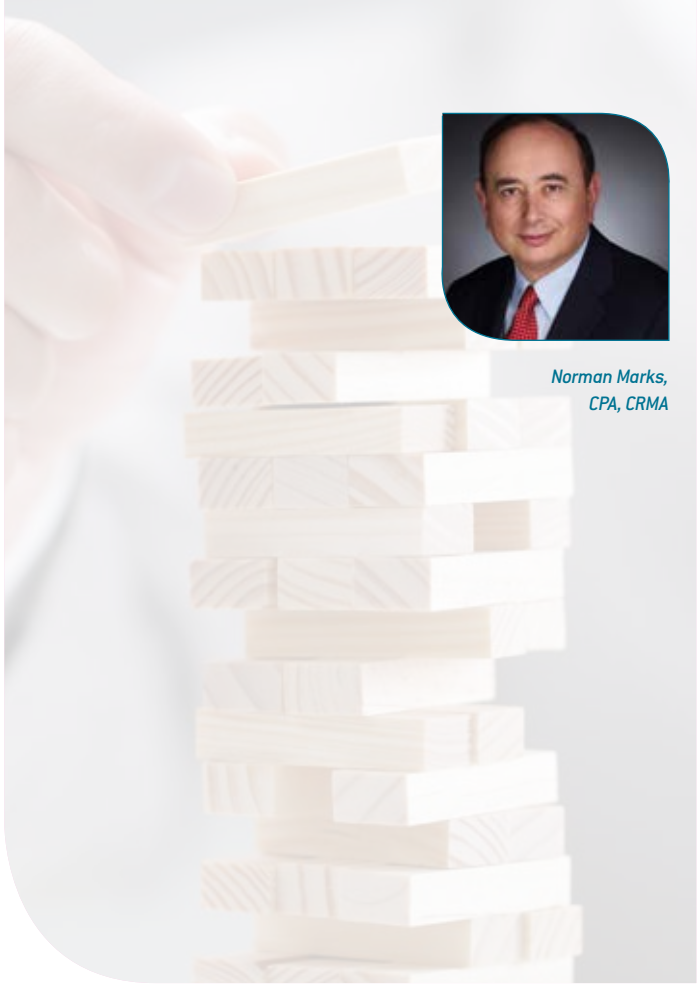


Source : schéma adapté de "Internal Audit Capability Model (IA-CM) for the Public Sector" (Altamonte Springs, FL: The IIA Research Foundation, 2009), p.7

L'approche par ce modèle de maturité permet de prioriser les axes d'amélioration en fonction d'un niveau de maturité souhaité, axes qui ne sont pas limités à la conformité aux normes.

En effet, le diagnostic de maturité constitue une mesure objective des progrès réalisés et un outil d'identification des améliorations nécessaires. L'Évaluation Maturité de l'IFACI conduit à établir une feuille de route vers des pratiques innovantes, ce qui donne un nouveau souffle dans le programme d'amélioration de la performance d'un service d'audit interne.

www.ifaci-certification.com/



Norman Marks, CPA, CRMA

AUDITING THE RISKS THAT MATTER

by Norman Marks

How often does an audit report get the attention of the full board?

Rarely, if ever. Most of the time, the audit committee is the final destination of audit communications; it is very unusual for an audit report to merit a spot on the agenda of the full board.

Should internal auditors, let alone the board and top management, be satisfied with that?

No, they should not be - and that is reflected in the results of some recent surveys.

When KPMG completed its *Global Audit Committee Survey*, they reported that *"Fewer than half of the 1,800 respondents are satisfied that internal audit delivers the value to the company it should (45%), and that the internal audit plan properly focuses on the 'critical risks to the enterprise' (49%)".*

It's not only that these audit committee members were less than satisfied that they were getting full value; about half of them said that internal audit was not addressing the risks that matter to the enterprise as a whole – the critical risks to its success. If internal audit had a contribution to make to the likelihood of the organization achieving its objectives, such as pointing out risks that might derail such achievement or opportunities to enhance results, surely the full board would want to know – and ensure appropriate action is taken by management.

PwC found similar results in its annual report on the State of the Profession. Their comment was that *"expectations have risen, and all internal audit functions need to rise to this new floor: providing assurance on a broader range of critical risks and clearly communicating deeper insights."*

New Zealand is seen by some as quite progressive in its governance and risk management practices. Yet, a member of multiple boards wrote that *"Almost all of IA findings are mundane operational compliance issues".*

What needs to change so that the work of internal audit is valued and seen as addressing the risks that matter?

The traditional process for developing a risk-based audit plan starts with an "audit universe". This is a list of potential auditable entities such as business processes, departments, locations, business units and so on. The auditor then assesses the level of risk associated with each auditable entity, often considering their materiality to the business (perhaps based on revenue or profit); the time since the last audit; whether the last audit identified significant internal control weaknesses; the complexity of accounting; whether there has been a change in management or other key personnel; whether there has been a change in the systems used; the level of management concern; and so on.

The auditor then risk-ranks each auditable entity and those that rank highest are placed on the audit plan.

When it is time to start planning the audit, a second risk assessment is performed. This identifies the more significant risks within the entity that will be audited, and the engagement focuses on controls over those risks.

This traditional approach seemed to work well for many years. The audit committee and senior management can see a logical approach to identifying the risks to audit.

However, it does not always identify the risks that matter to the organization – those that have to be managed if the enterprise is going to achieve its objectives and deliver the desired level of value to its stakeholders.

For example, most internal audit departments audit accounts payable frequently, if not every year. Many also have a regular engagement to identify potential duplicate payments. Yet, when – if ever – has a company failed because of a control weakness in accounts payable, or because it had an excessive level of duplicate payments?

I served as the chief audit executive (CAE) at several companies. At Solectron Corporation, which performed outsourced manufacturing for electronics companies, I inherited a department that had been praised by top management and the audit committee. The former CAE had used the traditional risk-based audit planning approach and my experience there serves as an example of my theme.

When I joined in 2001, the company was the leader in its market with about $19bn in revenue and 60,000 employees. The internal audit department of about 12 people performed 15-20 audit engagements each year, focusing on the largest business locations. They consistently identified serious control issues as well as opportunities, including close to a million dollars in potential duplicate payments.

But were they addressing the risks that were critical to the organization, or only the risks that were critical to the business locations they audited?

One morning, I stopped by the desk of the IT audit manager. It was the week before he and the rest of the team were going to start an audit of a major U.S. site and I expected him to be finalizing his planning and preparation.

I asked him what he was working on and he explained that he was drafting the audit report! How, I wondered, could he be working on the audit report when he hadn't started any of the fieldwork?

He told me that even though each site had different systems and an independent IT organization, he almost always found the same control and security issues. So, he could start drafting the findings as part of his planning work.

He explained the typical control and security issues, and I immediately saw that this was something that needed to be addressed by the corporate CIO and his team. The IT auditor said that a copy of the report always went to the corporate CIO, but the local IT organizations didn't report to him. The corporate CIO had never shown more than a passing interest in the audit reports, even though they surfaced pervasive information security and internal control weaknesses.

I quickly added an audit of the corporate IT and IT security function to the audit plan, focusing on overall IT governance, security policies, and the like. That audit identified serious issues with network-wide security, the inability of the fragmented systems environment to deliver the enterprise-wide information needed by corporate management to run the organization, and more. For example, when the CFO asked how much the company was spending with consulting firms, it took over a month to gather the information!

It was not only the IT organization that was fragmented. The leadership team was also fragmented, with overt competition between geographic regions, business locations, and divisions.

One of our larger factories, in Mexico, told a visiting executive that they had just won a major new contract with a telecom customer. The executive asked about the terms and was shocked when they informed him not only that the gross margin was barely positive but that they had been forced to agree to reduce future sales prices by as much as 20% in each of the future years of the contract! The manager explained that this was necessary because of the tough competition for the sales contract. The visitor asked who was the competition; was it one our leading competitors in the region? No, he was told: it was our factory in China!

I soon became aware of another pervasive issue: as a result of multiple acquisitions, the company had grown to more than 100 manufacturing locations. However, the majority were operating at less than 50% capacity. As a result, operating costs were higher than our competitors and that was putting severe pressure on corporate earnings. Middle management at the corporate headquarters was trying very hard to address the issue; they had produced a plan to reduce the number of factories, but the politics within the senior management ranks and the lack of strong leadership at the top was preventing any constructive change. Instead, at the recommendation of the CFO, the CEO ordered a 10% across the board cut in headcount. This, of course, did not address the real issue of having too much capacity for the sales we were generating.

These were the primary risks to the company, but there were more in a similar vein. For example, every location wrote its own sales contracts. Some global customers, therefore, had different contracts with different terms with 20-30 of our locations. We had lost any and all negotiating power as the customer could negotiate separately with what amounted to 20-30 small companies.
We moved to a different form of risk-based audit planning for 2002 and subsequent years.

Instead of starting with an audit universe, we started with a risk universe. There was no enterprise risk management program at that time; the only enterprise-wide assessment of risk was the one I led, which we used to build the audit plan. The risk universe was a list of the more significant risks facing the company and its ability to achieve its business objectives. We used tools like risk mapping to identify the risks and discuss them with management and then with the audit committee of the board.

We prioritized the risks and identified the audit engagements to address them. While we continued to audit the larger locations, this time it was because they were the more significant sources of the higher risks to the enterprise and its objectives. We also, for the first time, included audits of a number of corporate activities.

For example, one of the greatest risks related to the company's ability to source quality materials for its manufacturing operations that arrived on time and were obtained at a competitive price. If this risk was not managed effectively, it would affect our ability to match or beat our competitors' prices, deliver quality products to our customers on time, and maintain a high level of customer satisfaction. The audit plan included a series of inter-related audits, performed in series by a single team: first, we assessed the controls performed by the office of Senior Vice President at the corporate headquarters over the negotiation of global supply agreements with our major vendors and the monitoring of prices actually paid by each of our factories. (This was necessary as each factory separately negotiated contracts with the same vendors, or their agents, for the same materials.) After this audit of what we would now call "entity-level controls", we performed audits of our four larger locations in Malaysia, China, France, and the U.S.

The results were interesting in a number of ways. Our assessment was that the Penang, Malaysia operation had employed innovative best practices that enabled it to obtain the same quality products from a vendor at lower prices than either the global contract or local negotiators at the other locations. This included taking advantage of local agents with high levels of inventory. Rather than criticize Penang, which the corporate SVP and his people frequently did, we praised them and suggested that the others learn from them. Overall, we felt that the company had not been effective in obtaining quality products at the best price – with the exception of Penang and, to a lesser extent, China (which was managed by staff from Penang). We would not have arrived at this assessment if we had not taken the 'big picture' view of risk and relied instead on individual audits.

Today, I call this approach 'enterprise risk-based' auditing to differentiate it from traditional risk-based auditing.

The change in approach led to our performing more focused audits of the larger locations. Instead of auditing controls over risks that were significant to the location, we audited controls at each location over risks that were significant to the enterprise. We also performed more audits, again focused on enterprise risks, of smaller locations. Finally, we started assessing 'entity-level' controls related to information security, sales contracting, corporate ethics, and more. Assessing controls over enterprise risks required more senior and experienced staff; not only did I change the audit approach, but I helped junior staff rotate out and replaced them with more seasoned individuals. Instead of full-scope audits of major locations by a team of as many as 6-8 people, we performed focused audits, sometimes by just one or two auditors.

By 2004, we had increased the number of audits from 15-20 to over 100.

We identified situations where the risk to corporate objectives and success was higher than the board or top management desired. I made sure that the audit committee was informed and sometimes this required one-on-one private meetings to supplement or even replace audit reports. In some cases, ours was the first objective insight they had received on a critical issue.

At Solectron, I did not have the benefit of a mature risk management program. If such a program had existed, the enterprise-risk based audit plan would have been built this way:

1. Assess management's risk management program. Does it provide a risk assessment that can be relied upon as a basis for the audit plan?
2. If it does not, after ensuring that management and the board are so informed, develop a risk universe and, with management input, prioritize the risks to corporate objectives and success.
3. Identify the audit engagements (which may be several) required to provide assurance that the more significant risks are being managed at desired levels. This may require some internal audit judgment being applied to select the risks to audit. For example, there may be little value in addressing some risks if management already has a major project underway to upgrade the area, or internal audit may decide to increase the level of risk from that assessment by management because of prior audit results, changes in management, or changes in the primary computer systems.

FINAL THOUGHTS

There is a huge difference between the quality and level of assurance and insight obtained by an enterprise-risk based approach and the traditional risk-based planning process. It changes the work that is performed and enables the internal audit activity to provide assurance and identify opportunities that will directly affect the success of the organization.

At Solectron and the companies I joined later, we audited controls over the risks that the executive team and the board discussed. We provided assurance and insight that they relied on as they managed and directed the organization to success – assurance that was relevant to their strategies and objectives.

Many organizations (perhaps a third, based on surveys I have seen) have started the journey to enterprise risk-based auditing. I believe it enables internal audit to be seen as a major contributor to the organization's success, providing insight on the risks that matter to the enterprise and our stakeholders on the board and in the executive suite.