



# AUDITORS MAGAZINE...الأولى في التدقيق

## التدقيق قيادة ابداع تطوير



**ISACA®**  
Tunis Chapter

العدد الأول - جويلية 2018

AUDITORS\_الأولى في التدقيق

E-mail : [auditors.worldwide@gmail.com](mailto:auditors.worldwide@gmail.com)

Website: [www.theauditors.org](http://www.theauditors.org)

Mobile: +21658594540/+201005276821

## كلمة فريق الإعداد

أعزائنا القراء،

مرحبا بكم في العدد الأول من مجلة أوديتورز الأولى في التدقيق....

تتشرف أسرة أوديتورز بإصدار العدد الأول من مجلة أوديتورز الأولى في التدقيق والتي تهدف إلى عرض المستجدات من الموضوعات الحديثة التي يتم تطبيقها عالميا أو ما تم استحدثه بالوطن العربي بمجال التدقيق والحوكمة وإدارة المخاطر.

تضم مجلة أوديتورز مجموعة متنوعة من الموضوعات التي أثرت حديثا في مجال التدقيق والحوكمة وإدارة المخاطر بهدف نشر المعلومات عن كيفية تناولها وتطبيقها عالميا لمواكبة التطورات والمتغيرات العالمية في هذا المجال. وتنفرد المجلة بعرض هذه الموضوعات من خلال منظور وآراء مجموعة من الخبراء وممارسي مهنة التدقيق بأكثر من دولة وبأكثر من لغة وهي العربية والانجليزية والفرنسية بهدف الوصول الى أكبر عدد ممكن من المهتمين والفاعلين في مجال التدقيق والحوكمة وإدارة المخاطر على مستوى العالم.

ومع التطور التكنولوجي الذي تشهده جميع المؤسسات على المستوى العالمي وزيادة الاعتماد على النظم التكنولوجية الحديثة في الأنشطة التشغيلية والانتاجية والتزايد المستمر في الكم الهائل من البيانات التي تعتمد عليها المؤسسات في العمليات التشغيلية، تطورت أنواع المخاطر التي قد تتعرض لها هذه المؤسسات وتنوعت وأصبحت المخاطر التكنولوجية المصاحبة لذلك التطور من أهم أنواع المخاطر التي يجب على المدقق الداخلي التحقق من إدارتها بشكل كفاء. وعلى ضوء هذه المستجدات، تغيرت مهام المدقق الداخلي بتغير مستويات المخاطر وأولوياتها وظهور أنواع جديدة من المخاطر التكنولوجية التي تتغير بشكل متسارع. وقد تناول العدد الأول من المجلة مجموعة من الموضوعات المختلفة التي تطرقت الى كيفية معالجة هذه المتغيرات أهمها: حوكمة تكنولوجيا المعلومات والتدقيق الداخلي، الحوكمة المؤسسية والتدقيق الداخلي، مسؤولية التدقيق الداخلي تجاه عمليات الاحتيال، The 2018 Update of ISO 31.000، Gouvernance des ressources Humaines، Le nouveau cadre du management des risques COSO II، التدقيق الداخلي والمتغيرات التكنولوجية الحديثة... والعديد من الموضوعات الجديدة والتميزة التي انفردت بها المجلة.

كما يضم هذا العدد الأول من مجلة أوديتورز حوارا مع السيد وليد بوزويطة رئيس المعهد التونسي للحوكمة والتدقيق والسلامة المعلوماتية، فرع منظمة ايساكا العالمية المختصة في حوكمة وتدقيق نظم المعلومات بتونس ISACA Tunis Chapter بالإضافة الى التحديثات المتوقعة سنة 2019 في منهج شهادة المدقق الداخلي المعتمد CIA.

أعزائنا القراء،

ان شاء الله نعمل جميعا على مواصلة التعاون المهني المثمر ورسم خطوات النجاح في تقدم وتطوير المهنة والمساهمة في إثراء البحث العلمي في مجال المراجعة/التدقيق بجميع أنواعه والعمل على رفع كفاءة المدقق العربي بالخصوص وتأهيل كوادر جديدة في سوق العمل.

وفي الختام،

تفضلوا باسمنا وباسم كافة أسرة أوديتورز بقبول فائق الشكر والاحترام.

## فريق اعداد المجلة

الدكتورة ميرفت حسين السيد

مدير تدقيق داخلي بقطاع سوق المال  
مصر



مرwan الشرف بنعلي  
مراقب المالية/مدقق حكومي بهيئة الرقابة العامة للمالية  
مهندس كمبيوتر  
وزارة المالية التونسية



## المحتويات

- 5..... أهم المنظومات الالكترونية المستخدمة في مجال التدقيق الداخلي، كتابة: مروان بنعلي
- 12 ..... مسؤوليات التدقيق الداخلي في موضوع الاحتيال، كتابة: زاهر الرمحي
- 14 ..... التدقيق الداخلي والمتغيرات التكنولوجية الحديثة، كتابة: ميرفت حسين السيد
- 21 ..... الوصفة السحرية لتحفيز الأنشطة الرقابية في المؤسسات، كتابة: سامر حمد الله
- LE NOUVEAU CADRE DE MANAGEMENT DES RISQUES "COSO II" de 2017, Auteur : Krimi**
- 24 .....Abdessatar
- 28 .....The 2018 Update of ISO 31.000, Author: Hans Læssøe
- 30 ..... التطور المتسارع في التشريعات الرقابية والمعايير الدولية وأثره على أعمال البنوك، كتابة: إبراهيم الطعاني
- 32.....Rethinking the Three Lines of Defence, Author: Hans Læssøe
- 36.....Gouvernance des ressources Humaines, Auteur: Ben Ali Marwen
- 45..... ISACA Tunis Chapter محادثة مع السيد وليد بوزوينة رئيس المعهد التونسي للحوكمة والتدقيق والسلامة المعلوماتية
- 49 ..... الحوكمة المؤسسية والتدقيق الداخلي، كتابة: مروان بنعلي
- 52 ..... حوكمة تكنولوجيا المعلومات ونشاط المراجعة الداخلية، كتابة: ميرفت حسين السيد
- 60 ..... منظومة التصرف الالكتروني في التقارير الرقابية، كتابة: مروان بنعلي
- 64 ..... لعبة إلكترونية تزيد من نسبة معرفة الموظفين، كتابة: أحمد الملاحي
- 69..... A Practical Approach to Risk Tolerance, Author: Hans Læssøe
- 75..... Sur l'usage des ratios par les auditeurs, Auteur : Jean François Caron
- 78..... CIA Exam: Why, How, and What Is Changing January 2019

# أهم المنظومات الالكترونية المستخدمة

## في مجال التدقيق الداخلي

بقلم السيد مروان بنعلي، مراقب المالية/مدقق حكومي، هيئة الرقابة العامة للمالية التونسية

### مقدمة

وتجدر الإشارة الى ان إدارات التدقيق الداخلي في عديد المؤسسات تواجه عدة صعوبات أهمها ارتفاع تكلفة مهمات التدقيق ومحدودية الموارد البشرية والمالية وغياب كفاءتها في بعض الحالات، مما أثر سلبا على جودة وكفاءة وظيفة التدقيق ودورها في تقديم الإضافة المنشودة منها. في المقابل، يوفر استخدام التكنولوجيا الحديثة في عمليات التدقيق ربحا كبيرا في الوقت والمجهود وهم ما يفرض على المدققين الداخليين العمل بقوة، وبمزيد من الاحترافية، لمواجهة التحديات التي يفرضها التحول الرقمي على قطاع التدقيق الداخلي، وذلك بغية ضمان التدقيق الفعال، ونجاح مؤسساتهم.

في هذا السياق وفي ضل الأهمية الكبرى للتقنيات الحديثة في مجال التدقيق الداخلي، تهدف هذه الدراسة إلى عرض أهم البرامج الالكترونية المشهود لها عالميا في مجال التدقيق الداخلي وإدارة المخاطر والتي تساعد في تحسين كفاءة وفاعلية هذا المجال. وتدرج كافة البرامج التي سنقوم بعرضها ضمن تقنيات الكمبيوتر المساعدة في أعمال التدقيق (البرامج الالكترونية الجاهزة) **Computer-assisted audit techniques (CAATs) or computer-assisted audit tools and techniques (CAATTs)**.



يشهد العالم اليوم تطورا ملحوظا في الدور الذي تلعبه التكنولوجيات الحديثة في كافة مجالات الحياة الاقتصادية والاجتماعية للبلدان. وأصبح مبدأ التركيز على المعلومات والتكنولوجيا كعامل من العوامل الأساسية في التقدم والتنمية من الأمور المسلم بها. حيث مثلت تكنولوجيات المعلومات بالنسبة لكافة الشركات الخاصة والعامة أداة أساسية وفعالة لأداء أنشطتها بطريقة سريعة ودقيقة.

وبما أن التدقيق الداخلي: "نشاط مستقل وموضوعي يقدم تأكيدات وخدمات استشارية بهدف إضافة قيمة للمؤسسة وتحسين عملياتها. ويساعد هذا النشاط في تحقيق أهداف المؤسسة من خلال اتباع أسلوب منهجي منظم لتقييم وتحسين فاعلية عمليات الحوكمة وإدارة المخاطر والرقابة." حسب تعريف معهد المدققين الداخليين Institute of Internal Auditors (IIA)، أصبح استعمال تكنولوجيات المعلومات في هذا المجال حاجة ملحة ومن أساسيات نجاح إدارة التدقيق الداخلي في أداء مهامها بالسرعة والدقة المطلوبتين. حيث يقوم عمل التدقيق الداخلي أساسا على معالجة البيانات خاصة المحاسبية منها بطريقة يدوية دعمت بطريقة الكترونية والتي تتطلب من أي مدقق داخلي أن يتقن استعمال البرامج الإعلامية ونظم المعالجة الإلكترونية المتاحة الان، بالقدر الذي يمكنه من اداء عملية التدقيق بحرفية تامة.

أعمالهم. ولكن ليس من المتوقع أن يكون لدى جميع المدققين الداخليين نفس الخبرة التي يتمتع بها المدقق الداخلي الذي تكون مسؤوليته الأساسية تدقيق نظام المعلومات.

- **1220 ت. 2** - في سياق بذل العناية المهنية اللازمة يجب أن يأخذ المدققون الداخليون في الاعتبار استخدام التدقيق المعتمد على التكنولوجيا وغيرها من تقنيات تحليل البيانات.
- **2110 ت. 2** - يجب على نشاط التدقيق الداخلي تقييم ما إذا كانت حوكمة تكنولوجيا المعلومات في المنشأة تُدعم وتساند استراتيجيات وأهداف المنشأة.

## II. فوائد استخدام المنظومات الالكترونية الحديثة

توفر البرمجيات الحديثة تسهيلات كبيرة لادارة التدقيق الداخلي تمكنها من تحسين أداءها و جودة مخرجاتها. ومن أهم هذه الفوائد نذكر:

- جمع البيانات من الجهة الخاضعة للتدقيق بشكل مستقل وبدون أي مس لبياناتها او برامجه،
- تحليل البيانات المستخرجة تماشيا مع أهداف عملية التدقيق المحددة مسبقا،
- سرعة جمع البيانات ومعالجتها مما يحسن من مردودية أعمال التدقيق عبر التخفيض في مدة انجاز مهمات التدقيق،
- إمكانية التعامل مع حجم كبير من البيانات في نفس الوقت وبطريقة حيوية،
- إمكانية الكشف عن الحالات الاستثنائية غير الاعتيادية في البيانات،

## 1. المعايير الدولية للتدقيق الداخلي واستعمال التكنولوجيات الحديثة

تضمنت المعايير الدولية للممارسة المهنية للتدقيق الداخلي الصادرة عن معهد المدققين الداخليين في نسخته 2017 جملة من التعريفات للمصطلحات الجديدة المرتبطة بالتكنولوجيات الحديثة وهي:

- **تقنيات التدقيق القائمة على التكنولوجيا:** أي أداة من أدوات التدقيق الآلي، مثل برمجيات التدقيق العامة وتلك التي تنتج اختبار البيانات وبرامج التدقيق المُحوسب ووسائل التدقيق المتخصصة وتقنيات التدقيق بمساعدة الحاسوب.
- **ضوابط تكنولوجيا المعلومات:** الضوابط التي تدعم إدارة الأعمال والحوكمة فضلاً عن توفير الضوابط العامة والتقنية في مستوى البنية الأساسية لتكنولوجيا المعلومات مثل التطبيقات، والمعلومات، والبنية الأساسية، والأفراد.
- **حوكمة تكنولوجيا المعلومات:** دائرة أو قسم أو فريق من المستشارين أو غيرهم ممن يقدمون تطمينات وخدمات إستشارية موضوعية ومستقلة بهدف إضافة قيمة للمنشأة وتحسين عملياتها. يساعد هذا النشاط المنشأة على تحقيق أهدافها بإعتماد مقارنة نظامية ومنهجية لتقييم وتحسين فعالية كل من مسار إدارة المخاطر والرقابة الداخلية وحوكمة المؤسسة.

كما تضمنت المعايير جملة من التوصيات الوجوبية للمدققين الداخليين فيما يتعلق باستعمال البرمجيات الالكترونية في مهامهم وهي:

- **1210 ت. 3** - يجب أن يكون لدى المدققين الداخليين معرفة وافية بأهم مخاطر تكنولوجيا المعلوماتية والضوابط الرقابية المتعلقة بها، وكذلك تكون لديهم معرفة بتقنيات التدقيق المعتمدة على التكنولوجيا المتوفرة من أجل إنجاز

والتركيز على الملفات الإلكترونية مما يزيد من كفاءة القيادة في جميع جوانب سير العمل التدقيق الداخلي.

من بداية عملية التدقيق إلى نهايتها، يعتبر TeamMate من أهم المنظومات الإلكترونية التي تمس كافة مراحل عملية التدقيق الداخلي من خلال منظومة شاملة مكونة من خمس برامج مختصة ومندمجة وهي:



#### أ- ادارة المخاطر TeamRisk

كجزء من منظومة تيم مايت، يمثل TeamRisk نظام متقدم لتقييم المخاطر الذي يمكن إدارات التدقيق الداخلي من وضع خطة تدقيق قائمة على المخاطر.

#### ب- برمجة التدقيق TeamSchedule

يمكن TeamSchedule مستعمليه من برمجة مهامهم والوسائل المتوفرة لديهم بطريقة تمكن من توضيح لتوزيع الموظفين و متابعة المهام ضمن برنامج سنوي. ومن اهم المهام المقدمة نذكر:

- جدولة المشاريع بناء على معايير محددة من قبل المستخدم (المخاطر، تاريخ البدء المتوقع، النوع، الموقع)،

- المساعدة على كشف مواقع الضعف والخلل في أنظمة الرقابة الداخلية،
- الاقتصاد في نفقات إدارة التدقيق الداخلي خاصة مصاريف التنقل والهاتف في حالة الشركات التي لها فروع متباعدة جغرافيا،
- الاقتصاد في الموارد البشرية،
- تسجيل كافة مراحل عملية التدقيق من التخطيط الى كتابة التقرير وهو ما يمثل أدلة إثبات موثقة لحماية المدقق الداخلي و إمكانية برمجة تلك المراحل لإعادة تنفيذها آليا في المهام المستقبلية...
- هذا بالإضافة الى مجموعة من الخاصيات والتسهيلات الحصرية التي تمنحها كل منظومة لمستعملها وهو ماسنحاول التركيز عليه في بقية المقالة.

### III. أهم المنظومات الإلكترونية المستخدمة في مجال التدقيق الداخلي

#### 1. منظومة تيم مايت TeamMate: Do More with Less

باعتبارها الرائدة في مجال برمجيات إدارة التدقيق في العالم، أحدثت منظومة TeamMate ثورة في مجال التدقيق وتمكين إدارات التدقيق بجميع أحجامها من قضاء وقت أقل في البرمجة، التوثيق والمراجعة مقابل مزيد من الوقت لتوفير خدمات ذات قيمة مضافة. وهو ما جعل قرابة أكثر من 85 ألف مدقق من أكثر من ألفي منظمة في جميع أنحاء العالم قد اكتشفت بالفعل عرض TeamMate وقامت بتجربته.

من خلال توفير منظومة إلكترونية متكاملة لإدارات التدقيق، يزيل TeamMate الحواجز المرتبطة بالعمل المستندي الكلاسيكي

## 2. منظومة ايديا IDEA للتدقيق وتحليل المعطيات



كأحد أهم البرامج الرائدة في مجال التعامل مع البيانات المالية والتي تصدره شركة CASEWARE في نسخته العاشرة حاليا ، يوفر هذا البرنامج تسهيلات كبيرة في التعامل مع قواعد البيانات وتحليلها ومعالجتها بالدقة والسرعة المطلوبتين تمكن من زيادة كفاءة وجودة عمل إدارة التدقيق الداخلي:

- تسهيل عملية استيراد البيانات Data Import من أي قاعدة بيانات،
- تسهيل عملية تحويل البيانات Data Export بعد معالجتها لأي شكل (.pdf, .xls, .txt...)
- النفوذ الى عديد وظائف التدقيق المشتركة من بينها قانون Benford
- تسجيل كل مراحل التدقيق والتعامل مع البيانات مما يتيح إمكانية استعمالها في مهمات تدقيق لاحقة،
- توفير تسهيلات من اهمها IDEA add-ons، IDEAScript، منتديات Forums، وبنار Webinar ، بوابة الدعم Support Portal ...

لمزيد المعلومات حول المنظومة، يمكن زيارة موقع الويب <https://www.casewareanalytics.com/products/idea-data-analysis>

- تخصيص الموارد (مالية وبشرية) وتوزيعها،
- البحث عن الموارد: أداة متقدمة تسمح برساء مهمات التدقيق من اختيار أعضاء فرقتهم وفق احتياجات المهمة الحالية.

### ج- متابعة التوقيت والنفقات TeamTEC

تمكن TeamTEC كجزء من تيم مايت المتكاملة، تمكن من تحديد الوقت والنفقات المتعلقة بمهمات التدقيق. كما تسمح هذه التطبيقية من متابعة التقدم المحرز في المهام الصادرة عن إدارة التدقيق الداخلي والتكاليف المرتبطة بها واصدار تقارير تلخص نسب التقدم و النفقات المتعلقة بذلك.

### د- نظام وثائق التدقيق TeamEWP (Electronic Working Papers)

كجزء من منظومة تيمات المتكاملة، تمكن هذه التطبيقية من خلال هيكله قواعد البيانات المتناسكة من إيجاد المعطيات اللازمة وزيادة كفاءة عملية التوثيق والتدقيق. كما أن جميع المعلومات الهامة مثل البرامج، الفوارق، الملاحظات، الموافقات وتاريخ التغييرات في قواعد البيانات مسجلة الكترونيا مما يمكن من الرجوع اليها في أي وقت و من أي جهة أخرى.

### هـ- متابعة عملية التدقيق والفوارق TeamCentral

يمثل هذا الجزء قاعدة بيانات قوية ومتناسكة لمتابعة عملية التدقيق والفوارق عبر الواب التي تجمع معطيات على كافة المهمات المسجلة بتطبيق TeamEWP والنتائج التي تم التوصل اليها إضافة الى متابعة تنفيذ التوصيات المقدمة من قبل المصالح المعنية و الإدارة العليا.

لمزيد المعلومات حول المنظومة، يمكن زيارة موقع الويب <http://www.teammatesolutions.com>



### 3. لغة أوامر التدقيق (Audit Command Language) (ACL Language)



## ACL Analytics

كأحد أهم البرامج الأوسع انتشارا عالميا في مجال التعامل مع البيانات المالية والتي تصدره شركة ACL ، يوفر هذا البرنامج تسهيلات كبيرة في التعامل مع قواعد البيانات وتحليلها ومعالجتها بالدقة والسرعة المطلوبتين تمكن من زيادة كفاءة وجودة عمل إدارة التدقيق الداخلي.

من أهم وظائف البرنامج في نسخته الحالية 13 ACL كما تم عرضها في الموقع الرسمي للمنتج نذكر:

- تعميم البيانات وفقا لتاريخها Aging ،
- اكتشاف التكرار في الأرقام Duplication Identification ،
- إمكانية تصدير البيانات من البرنامج إلى برامج أخرى Export ،
- استخراج البيانات ذات الطبيعة الاستثنائية في ملفات Extraction .
- اكتشاف الفجوات في التسلسل الرقمي للبيانات Gap Identification ،
- ضم ودمج البيانات من ملفين منفصلين في ملف واحد Joining & Relation ،

- تصنيف البيانات على طبقات محددة على أساس عامل يتناسب مع أغراض الرقابة Stratification ،
  - سحب العينات Sampling ،
  - تصنيف وفرز البيانات وفقا لأي حقل ضمن الملف Sorting ،
  - تلخيص وتجميع البيانات وفقا لأغراض الرقابة Summarization ،
  - تجميع قيم البيانات الموجودة في الحقول Total file ...
- لمزيد المعلومات حول المنظومة، يمكن زيارة موقع الواب <https://www.acl.com>

### 4. مايكروسوفت إكسيل MS Excel

يعتبر برنامج مايكروسوفت إكسيل أحد أهم البرامج الالكترونية المستعملة من قبل المدققين الداخليين نظرا لسهولة استعماله وتوفر المراجع التفسيرية بأغلب اللغات. إذ يقدم هذا البرنامج عديد الوظائف لمستعمليه نذكر أهمها كما وردت بالموقع الرسمي لشركة مايكروسوفت وحسب النسخة الأخيرة من البرنامج 2016 Excel:

- ترتيب البيانات: من خلال تنظيم البيانات الرقمية أو النصية في جداول بيانات أو مصنفات من شأنها مساعدة المدقق في اتخاذ قرارات أفضل.
- إعادة تنسيق البيانات وترتيبها: أثناء قيام المدقق بإلقاء نظرة على تكوينات مختلفة، فإن تطبيق Excel يميز أسلوب مستعمله ويتعرف عليه، ويتولى إكمال البيانات المتبقية تلقائياً. لا حاجة إلى الصيغ أو وحدات الماكرو. وترشده ميزة البحث «أخبرني المزيد» إلى أوامر الميزة بحيث تعثر على النتائج التي تبحث عنها.

جُمّل SQL القياسية وكذلك البرامج ذات المهام الحرجة، سواء المنتشرة محلياً أو في السحابة....

#### IV. كيفية استعمال المنظومات الالكترونية

كمدقق داخلي، يمكنك وبسهولة كبيرة استعمال أحد هذه المنظومات الالكترونية او بعضها في نفس الوقت لتقوم مهامك بالسرعة والنجاعة المطلوبة.

بعد تثبيت المنظومة الالكترونية التي اخترتها Audit Tool على جهازك، يكفي ان تأخذ نسخة انية من البيانات التي تحتاجها في مهمتك Data Live copy لتبتعد عن مخاطر الاشتغال مباشرة على بيانات الانتاج Operational Data. يمكنك بعد ذلك إدخال النسخة في المنظومة الالكترونية وتشغل عليها وتقوم بالاختبارات التي تريدها.



- إجراء تحليل شخصي للبيانات: يعمل Excel على إجراء التحليلات المعقدة نيابة عن مستعمله، كما يلخص بياناته مع معانيات لخيارات pivot-table ، بحيث يمكن مقارنة وتحديد الخيار الذي يعرض فكرة مستعمله بأفضل طريقة.

#### 5. مايكروسوفت اكسس MS Access

يعتبر برنامج مايكروسوفت اكسس أحد اهم البرامج الالكترونية المستعملة من قبل المدققين الداخليين نظرا لسهولة استعماله وتوفر المراجع التفسيرية بأغلب اللغات. اذ يقدم هذا البرنامج عديد الوظائف لمستعمليه نذكر أهمها كما وردت بالموقع الرسمي لشركة مايكروسوفت وحسب النسخة الأخيرة من البرنامج Access 2016:

- سرعة بدء العمل عند استخدام قوالب قواعد البيانات: يمكنك البدء بسرعة عن طريق إنشاء تطبيق مخصص أو استلهام أفكارك من مجموعة من قوالب التطبيقات الجديدة التي تتميز بتصميماتها الاحترافية. يمكنك أيضاً إنشاء القوالب من التطبيقات التي أنشأتها لإعادة استخدامها أو مشاركتها مع الآخرين.
- تكامل البيانات بين Access وتطبيقات مجموعة الأعمال: توفر مكتبة الموصلات في Access طرقاً عديدة لتكامل البيانات الواردة من التطبيقات ومصادر البيانات المستخدمة في تشغيل شركتك. Ac وتتشي السيناريوهات المتكاملة عبر مصادر البيانات الحديثة مجموعة من المعارف الدقيقة والمرئيات في واجهة Access المألوفة.
- تخزين البيانات في SQL: يمكنك تخزين البيانات في SQL Server و Microsoft Azure SQL لتعزيز الوثوقية والأمان القوي وقابلية التوسع وسهولة الإدارة على المدى الطويل. فتطبيقات Access تساهم في تحسين بناء

## خلاصة

المشكلة الحقيقية ليست في اقتناء البرنامج ، إنما في استخدامه بالشكل الصحيح ، إذ يمكن التعاقد مع منتج برامج تدقيق إلكتروني ولكن الأهم هو التدريب على استخدامه، الشيء الذي يبين الأهمية التي ستقوم بها الدورات التكوينية للمدققين حول استعمال مثل هذه المنظومات التقنية كخطوة ثانية.



ان استعمال المنظومات الالكترونية من قبل المدقق الداخلي يمكنه من سهولة وسرعة جمع المعلومات المطلوبة من خلال إمكانية الدخول إلى قواعد البيانات الخاصة الإدارة الخاضعة لعملية التدقيق بشكل مستقل وآمن لا يؤثر على بياناتها أو برامجها والقيام بتحليل تلك البيانات وفقا لأهداف عملية التدقيق. كما تساعد هذه المنظومات المندمجة على التدقيق في حجم كبير من البيانات وتحليلها وتسجيل كافة عمليات التدقيق التي يقوم المدقق بتنفيذها وكذلك النتائج التي يخلص لها.

كما تساهم التقنيات الحديثة من تحسين جودة عمل ادارات التدقيق الداخلي و مواجهة التحديات التي يفرضها تطور الجهات الخاضعة للتدقيق في مجال استعمال الوسائل الحديثة اضافة الى مساهمتها للحوكمة الالكترونية التي تعمل العديد من الشركات على تكريسها صلب ادارتها بكامل مصالحتها.

للتواصل مع الكاتب: [benali.marwen@gmail.com](mailto:benali.marwen@gmail.com)

## مسؤوليات التدقيق الداخلي في موضوع الاحتيال

بقلم الدكتور زاهر الرمحي، CIA، CICS، مستشار وخبير في التدقيق الداخلي

إن مسؤوليات **التدقيق الداخلي** في موضوع الاحتيال أشارت إليها معايير التدقيق الداخلي الصادرة عن معهد المدققين الداخليين الأمريكيين IIA ضمن المعايير الدولية للممارسة المهنية للتدقيق الداخلي (نسخة 2017) ونستطيع أن نجعلها فيما يلي:

\* أشار **المعيار رقم 1210** إلى ما يلي: (يجب أن يتمتع المدققون الداخليون بالمعرفة الوافية التي تمكنهم من تقييم مخاطر الاحتيال والكيفية التي تدار بها المخاطر من خلال المؤسسة).

يلاحظ أن هذا المعيار ركز على امتلاك المعرفة لدى المدققين التي تمكنهم من التحقق من قيام الوحدات المعنية بتقييم مخاطر الاحتيال ووضع الإجراءات اللازمة لإدارتها وفق أولويات تقييم المخاطر بحيث يتم التركيز على المخاطر المرتفعة، والذي لا يستطيع المدقق الداخلي التحقق منها إذا لم يمتلك المعرفة الخاصة بتقييم مخاطر الاحتيال، وكذلك على المدققين الداخليين امتلاك المعرفة اللازمة بمؤشرات الاحتيال Red Flags كما اشار الارشاد التطبيقي لهذا المعيار وهي عبارة عن بعض الاحداث والتصرفات اذا لاحظها المدقق قد تقود الى وجود احتيال.

\* اشار **المعيار رقم 1220** إلى ما يلي: (يجب على المدققين الداخليين بذل العناية المهنية اللازمة أثناء قيامهم بأعمالهم آخذين بعين الاعتبار العناصر التالية):

- مدى العمل اللازم لتحقيق أهداف المهمة.
- درجة التعقيد أو الأهمية النسبية أو أهمية المسائل التي يتم تطبيق إجراءات التطمين عليها.
- ملائمة وفعالية مسار الحوكمة وإدارة المخاطر والرقابة.
- احتمال حدوث أخطاء جسيمة أو الاحتيال أو عدم الامتثال.
- تكلفة أعمال التطمين مقارنة بالمنافع الكامنة.

يعتبر موضوع **الاحتيال** من المواضيع التي تترك إدارات المؤسسات في كافة القطاعات لما يترتب عليها من آثار سلبية سواء خسائر مالية أو تأثير على السمعة. وقد أشار التقرير الدولي للاحتيال وسوء الاستغلال الوظيفي الصادر عن جمعية مكافحة الاحتيال الدولية ACFE لعام 2016 أن المؤسسات تخسر 5% من إيراداتها سنويا نتيجة عمليات الاحتيال.



وقد يتساءل الكثيرون ما هو دور التدقيق الداخلي في موضوع الاحتيال؟ هل دوره اكتشاف الاحتيال مثلا؟ وهل إذا اكتشف احتيال في أنشطة خضعت للتدقيق سابقا يمكن أن يوجه لوم لإدارة التدقيق الداخلي؟ وهل التدقيق الداخلي معني بالتحقيق في حالات الاحتيال؟ هذه اسئلة عديدة وغيرها من الاسئلة يمكن ان تطرح في هذا الموضوع.



من المعلوم أنه على فريق التدقيق وقبل تنفيذ أي مهمة أن يقوم بوضع خطة للمهمة يتم اعتمادها من قبل مدير إدارة التدقيق الداخلي أو من يفوضه. ومن ضمن مكونات الخطة ضرورة وجود تقييم لمخاطر النشاط أو مركز العمل المستهدف بالتدقيق من خلال اعداد مصفوفة المخاطر والتي من ضمنها تقييم مخاطر احتمالية وجود الاحتيال إضافة إلى المخاطر الأخرى والتي بناء على نتيجة التقييم يتم تحديد اتجاهات تنفيذ مهمة التدقيق.

اما بخصوص التحقيق في الاحتيال، يمكن للتدقيق الداخلي المساعدة في التحقيق المبدي للاحتيال والذي يعني تحديد نقاط الضعف في نظام الرقابة الداخلية التي أدت إلى حدوث حالات الاحتيال وتقييم مؤشرات الاحتيال للحالات التي حدثت والتوصية بأية إجراءات لاحقة.

أما بخصوص اكتشاف الاحتيال، فالمدقق الداخلي غير معني باكتشاف الاحتيال إلا إذا كان ضمن العينة التي تناولها وبشرط ان يكون ضمن عناية الشخص الحريص لأن هناك حالات احتيال حتى لو جاءت ضمن عينة المدقق لا يستطيع اكتشافها لأنها نفذت بطريقة لا يستطيع الشخص الحريص والمتبصر أن يقوم باكتشافها مثال ذلك التواطؤ بين أكثر من موظف أو ما شابه.

- درجة تعقيد المهمة وأهميتها النسبية.
- احتمالية حدوث أخطاء جسيمة او احتيال).

من المعروف وحسب المعيار الرئيسي رقم 1200 الصادر عن معهد المدققين الداخليين بأنه يجب على المدقق الداخلي بذل العناية المهنية اللازمة والتي من قواعدها ضرورة التركيز على الجوانب ذات الأهمية أو الجوانب التي تتضمن مخاطر ملازمة مرتفعة Inherent Risk وكذلك يجب التركيز على الأنشطة التي من المحتمل أن يحدث فيها احتيال. ومثال ذلك إذا توفر لدى المدقق بعض القرائن على وجود احتيال أو إذا لاحظ وجود مؤشر احتيال مثلا أو إذا تكررت حالات احتيال سابقا ضمن النشاط الذي يقوم بالتدقيق على أعماله، فعلى المدقق هنا تطبيق قواعد العناية المهنية اللازمة بزيادة العينات والربط المهني للجوانب المشتركة مع بعضها والتدقيق بعين الفاحص لاحتمالية وجود الاحتيال والسعي لإمكانية التعزيز من أطراف خارجية إذا رأى ذلك مناسبا مثل تعزيز أرصدة حسابات البنوك من خلال البنك أو تعزيز رصيد أحد الموردين من خلال المورد.

\* أشار المعيار 2120 إلى ما يلي: (يجب على نشاط التدقيق الداخلي تقييم احتمال حدوث عمليات احتيال وكيفية إدارة المنشأة لمخاطر الاحتيال).

على الإدارة وضع الاجراءات الرقابية لمواجهة المخاطر التي سبق وإن تم تقييمها ومن ضمنها ضوابط رقابية لمواجهة مخاطر الاحتيال وعلى التدقيق الداخلي أثناء قيامه بتقييم أنظمة الرقابة الداخلية التحقق من وجود هذه الضوابط ومدى تطبيقها للتخفيف من احتمالية حدوث الاحتيال.

\* أشار المعيار 2210 إلى ما يلي: (يجب أن يأخذ المدققون الداخليون في اعتبارهم عند تحديد أهداف مهمة التدقيق احتمال وجود أخطاء هامة أو عمليات احتيال أو حالات عدم نقيده أو مخاطر أخرى).

للتواصل مع الكاتب: z\_ramahi@hotmail.com

# التدقيق الداخلي والمتغيرات التكنولوجية الحديثة

بقلم الدكتورة ميرفت حسين السيد CCO، CIA، مدير تدقيق داخلي بقطاع سوق المال، مصر

## مقدمة

### 2. أهم المتغيرات التكنولوجية الحديثة:



ومن أهم المتغيرات التي انتشرت على نطاق واسع لتصبح متداولة بين أنحاء العالم ما يلي:

#### 1. Fin tech (Financial Technology)

وهي استخدام النظم التكنولوجية الحديثة في مجال الخدمات المالية بسهولة مع ضمان استخدام آمن للمعاملات المالية، وحمايتها من المخاطر الإلكترونية والتي تعتبر بمثابة تهديد للمؤسسات التي تعتمد على تقديم الخدمات المالية التقليدية. حيث تعمل هذه المؤسسات على استخدام التطبيقات التكنولوجية الحديثة لتقديم الخدمات المالية للعملاء مثل تطبيقات الدفع المستخدمة عن طريق الإنترنت البنكي او عن طريق الموبيل Internet Banking & smart Phone، وامكانية استخدام العملات الرقمية والعملات المشفرة من خلال تلك التطبيقات. ومن البنوك التي شاركت في تطوير وتطبيق هذه

يعتبر التقدم التكنولوجي المتسارع الذي يشهده العالم في السنوات الاخيرة تحديا كبيرا أمام مهام التدقيق الداخلي. فقد أدى التطور التكنولوجي والانفتاح العالمي نتيجة استخدام وسائل الاتصال الحديثة عبر شبكة الإنترنت وشبكات التواصل الاجتماعي والتي اتاحت نقل البيانات والمعلومات بين أنحاء دول العالم في شكل لحظي، إلى ظهور العديد من التطبيقات التكنولوجية الحديثة وظهور العديد من المصطلحات التكنولوجية الجديدة التي أصبحت تتناقل بشكل كبير بين المؤسسات باختلاف أنواعها (مالية - تجارية - صناعية-...)، سعيا وراء كسب شريحة جديدة من العملاء أو اكتساب أسواق جديدة للحفاظ على بقاءها وعدم خروجها من دائرة المنافسة، فضلا على تدعيم قدرتها في تلبية احتياجات أصحاب المصالح بالمؤسسة (العملاء -الموردين - المساهمين - الدائنين-...) التي تتأثر بتلك المتغيرات التكنولوجية المتسارعة.

#### 1. التدقيق الداخلي والمتغيرات التكنولوجية الحديثة

أدى التطور التكنولوجي الذي تشهده المؤسسات بكافة أشكالها إلى احداث تغييرات سريعة ومتلاحقة في النظم التشغيلية والادارية المستخدمة في أعمالها اليومية والتي تمكنها من أداء أهدافها وخططها الاستراتيجية، والتي تشكل تحديات هامة لقيام المدقق الداخلي بمهامه ليس فقط في تقدير المخاطر المترتبة على تطبيق النظم الجديدة وانما في التحقق أيضا من توافق هذه المتغيرات مع أهداف واستراتيجيات المؤسسة بشكل فعال، وبما يتوافق مع احتياجات وتوقعات أصحاب المصالح. فهل تتوفر كافة الدوافع التي تبرر هذا التغيير؟ وما هي المخاطر المترتبة على تطبيقه مقارنة بالمخاطر المترتبة عند اتخاذ قرار بعدم التغيير؟

### 3. Crypto Currencies

وهي أحد أشكال العملات الرقمية والتي تم تصميمها بحيث تكون آمنة التداول مع الحفاظ على سرية بيانات المتعاملين وعدم الإفصاح عن معاملاتهم وفي المقابل يتم التداول عليها من خلال نظام Block chain.

ومن أهم العملات المشفرة التي أخذت اهتمام واسع المدى خلال الأعوام القليلة الماضية هي عملة البيتكوين والتي شهدت تداول متزايد بدرجة عالية العام الماضي واستمرت في الارتفاع حتى بداية هذا العام، ثم أخذت في الانخفاض وبطريقة متسارعة وذلك لعدم وجود اعتراف دولي لها وعدم وجود أحد الجهات الضامنة لتسوية المعاملات الخاصة بها مما يجعلها غير مكتملة للشكل القانوني ليتم الاعتراف بها كأحد العملات الرسمية المعترف بها دولياً. حيث أن القائمين عليها هم أشخاص وليس هيئة أو سلطة تنظيمية) أحد البنوك المركزية (تقوم بتنظيم عملية الإصدار والتداول الخاص بها أو وجود غطاء مقابل للإصدارات الخاصة بها .



### 4. Block Chain

هو قاعدة للبيانات الالكترونية التي تستخدم كسجل لبيانات المعاملات التي يتم تنفيذها من خلال الأجهزة المتصلة بنظام Peer to Peer network (P2P) أو شبكة الند للند وكل الأجهزة المتصلة بالشبكة

التدقيق قيادة ابداع تطوير

التطورات والأفكار التكنولوجية بنك HSBC & Credit Suisse من خلال تطوير نظم الدفع والتحويلات البنكية عبر الانترنت أو الموبيل أو التليفون البنكي والمدعمة بنظم الحماية اللازمة التي تضمن أمن وسرية بيانات العملاء .



### 2. Artificial intelligence and robotics technology

ويقصد بمصطلح نظم الذكاء الاصطناعي الجمع بين استخدام الاجهزة التقنية الحديثة ومجموعة من النظم والبرامج المتطورة المدعومة بنظم معالجة للبيانات والتي تساعد في اتخاذ القرار في حالات مختلفة مثل نظم a set of "if-then" rules ، والتي تستخدم لتنفيذ المهام التي تتطلب دقة متناهية أو ذات مخاطر عالية على حياة البشر . وقد تم تطوير هزم النظم بحيث تكون قادرة على التكيف مع معلومات غير مؤكدة أو غير مكتملة.





تحتفظ بنسخة من سجل العمليات الالكترونية والتي يتم تحديثها في وقت واحد لمنع حدوث اخفاق في أحد النقاط المتصلة وهو ما يسمى بـ (SPOF) single point of failure، وتستخدم الآن Block chain network في العديد من العمليات الالكترونية، حيث لم تعد قاصرة على تداول العملات الرقمية أو البيتكوين حيث تعتبر من أحد الطرق الامنة والفعالة في ادارة قاعدة البيانات القائمة على المعاملات الرقمية. وقد تم استخدامها في عدة مجالات بشكل واسع في مجال صناعة التداول على العقارات، Supply chain، الادوية، Smart card payments، التصويت الالكتروني، وغيرها من استخدامات.

#### 6. Cloud Computing Technology

وهو مصطلح يستخدم لتقديم الخدمات المستضافة عبر الانترنت (Cloud computing الحوسبة السحابية) وهذه الخدمة تمكن المؤسسات من استغلال بعض الموارد او الاجهزة الافتراضية (virtual machine (VM)) لاستخدام بعض التطبيقات التكنولوجية أو الوحدات التخزينية للمعلومات والبيانات Server less بدلا من قيام المؤسسة ببناء وصيانة الهياكل أو اقتناء البنية الاساسية الخاصة بها ومستلزماتها من أجهزة ووحدات تكنولوجية حديثة مثال التطبيقات الخاصة بشحن الكهرباء بناء على الاستخدام ، Pay per use وبالتالي الاستفادة من المزايا التكنولوجية الحديثة مع سهولة الاستخدام وتوفير التكاليف والمرونة في الاستخدام وفقا للاحتياجات والمتغيرات الخاصة بالمؤسسة.



#### 5. Cyber security and IT Governance

وحكومة تكنولوجيا المعلومات هي مجموعة من الضوابط والاجراءات والعمليات التكنولوجية المصممة لحماية النظم والشبكات التكنولوجية من المخاطر والهجمات الالكترونية cyber attacks أو الاستغلال الغير مصرح به لنظم المعلومات أو تحقيق منافع خاصة تجاه بعض أصحاب المصالح داخل أو خارج المؤسسة. لذا لا بد وان تعمل كل مؤسسة على وضع الاستراتيجية الفعالة والتي تتوافق مع أهداف المؤسسة ككل التي تعمل على تخفيف وتقليل الهجمات الالكترونية السيبرانية والعمل على امن وحماية نظم المعلومات.







### 9. Bots technology

وهي أحد التطبيقات المساعدة والتي قد تظهر أثناء استخدام الانترنت والتي تقوم على دراسة القوائم المفضلة لدى المستخدم والتي من خلالها يمكن للمستخدم أن يحقق وفر من استخدامه لتلك الأدوات التي تساعده في تحقيق أختياراته او الامور البحثية التي يرغب في اقتناءها كما، يمكن أن يتم استخدام تلك التقنية في حجز رحلات السفر أو الفنادق أو طلب الوجبات وأكثر من هذا بكثير.



### 10. Mobile First

وهي استراتيجية لتطوير مواقع الانترنت بحيث تتناسب مع استخدام الهواتف الذكية وذلك كنتيجة لتزايد أولوية استخدام أجهزة الهواتف من اجهزة الكمبيوتر لدى الكثير من المستخدمين حيث أصبحت الهواتف الذكية قريبة وفي متناول الجميع ويمكن من خلال الهواتف الذكية التواصل مع العملاء بشكل أسرع وامكانية جمع البيانات والمعلومات من خلال بعض التطبيقات المخصصة لذلك مما يسهل التواصل بفعالية مع العملاء المستهدفين ومساعدتهم في اتخاذ قرار الشراء بشكل أكثر فعالية وامكانية التواصل مع قاعدة كبيرة من العملاء.

### 7. Internet of Things (IoT)

وهو امكانية توصيل الاجهزة عن طريق الانترنت مثل أجهزة الكمبيوتر والهواتف الذكية وأجهزة السيارات وأجهزة المؤسسة وحتى الاجهزة المنزلية والتي يمكن أن يتم توصيلها جميعا عبر الانترنت، وبالتالي الحصول على امكانية التحكم في الاجهزة عن طريق الانترنت عن بعد، ودون ضرورة التواجد بمكان تشغيلها. وبالتالي يمكن للشركات والحكومات والمستهلكين الاتصال بأجهزتهم ولوحات المعلومات والشبكات ووحدات التخزين وأمن المعلومات عبر الانترنت لتسهيل امكانية إدارة أعمالهم بعدة أماكن دون التواجد الفعلي بتلك بها.



### 8. Quantum computing

ويطلق عليها حوسبة الكم وهي مجال لتطوير تكنولوجيا الحاسبات والتي تركز على نظرية الكم وسلوك الطاقة الناشئة عن الذرة (atomic and subatomic) وهم ما يشكل قفزة كبيرة في مجال الحاسبات وتزويدها بقدرة أكبر بكثير مما هي عليه الآن، وتحقيق جودة وامكانية عالية بالاداء من خلال القدرة على تنفيذ العديد من المهام في وقت واحد وياكثر من مكان باستخدام كافة التباديل الممكنة. وتشمل المراكز الحالية للبحوث في مجال حوسبة الكم MIT، Oxford University، IBM.

### 3. مميزات وعيوب تطبيق المتغيرات التكنولوجية الحديثة:

أصبحت المتغيرات التكنولوجية الحديثة من أهم الأهداف التي تسعى جميع المؤسسات الى إقتناؤها وسرعة تطبيقها لمواكبة موجة المتغيرات التكنولوجية الحديثة التي تجتاح العالم حفاظا على استمراريتها بسوق العمل ورفع الميزة التنافسية لها بين المؤسسات المماثلة. لذا يجب على المؤسسات دراسة إمكانية تطبيق تلك المتغيرات الحديثة من كافة الجوانب المتعلقة بها قبل اتخاذ قرار تطبيقها وفقا لما يلي:

#### I. أهمية تطبيق المتغيرات التكنولوجية:

التطور التكنولوجي الذي يشهده العالم جعل من الصعب على أي مؤسسة أن تتجنب التطورات التكنولوجية الحديثة وتتركها جانبا دون ان تهتم بالتعرف على تلك التكنولوجيا ومعرفة استخداماتها فالاعتماد على الادوات التكنولوجية أصبح متداخلا في أغلب المتطلبات التشغيلية اليومية بمعظم المؤسسات التي تهدف الى تيسير العمليات التشغيلية والانتاجية والحصول على خدمات متميزة تتناسب مع الاحتياجات المتغيرة للعملاء وتسهيل سرعة التواصل بين كافة الاطراف.

وعلى الرغم من أهمية تطبيق تلك المتغيرات الا أنه ينبغي على المؤسسات القيام بدراسة جدوى الاستقادة من تطبيقها في مجال انشطتها أو كيفية ايجاد البدائل الملائمة لها في حالة تعذر اقتنائها، ودراسة الجوانب السلبية التي يمكن ان تحدث للمؤسسة في حالة تطبيقها.

#### II. المميزات التي يمكن تحقيقها من تطبيق المتغيرات

##### التكنولوجية:

من أهم المميزات التي تسعى المؤسسات الى اكتسابها من خلال المبادرة بتطبيق النظم التكنولوجية الحديثة مايلي:

#### ■ سهولة الوصول الي البيانات

حيث تعتبر البيانات من أهم مصادر القوى التنافسية لاي مؤسسة وخاصة مع التطورات التكنولوجية العالمية، فالمؤسسات التي لديها أكبر قدر من المعلومات يمكنها أن تستغله في اكتساب ميزة تنافسية عن مثيلاتها بإمكانية التأثير على عملاءها من خلال الحملات التسويقية التي تخاطب احتياجاتهم المختلفة وتقديم اختيارات متنوعة تتناسب مع الفئات المختلفة.

#### ■ تحسين وسائل الاتصال:

من أهم المميزات التي أحدثتها الثورة التكنولوجية سهولة وثورة التواصل اللاحظي بين شتى أنحاء العالم، حيث بإمكان اي مؤسسة فتح مجالاتها التسويقية والبيعية على المستوى العالمي من خلال شبكات التواصل الالكتروني Social Media وليس قاصر فقط على الاقليم الذي تعمل به المؤسسة.

#### ■ سهولة التداول الالكتروني:

إمكانية عرض السلع والخدمات التي تقدمها المؤسسات من خلال الصفحات والمواقع التكنولوجية المخصصة لذلك، وإمكانية السداد الالكتروني من خلال نظم السداد المساعدة في ذلك مثل Pay Pal ونظام الـ Block chain والتي تحقق إمكانية السداد على طريق Digital coins والتي ساعدت في تطور نظم المدفوعات على مستوى العالم بسهولة التحركات النقدية بين شتى الدول بدون قيود أو تعليمات إدارية أو عوائق نقدية. مما دعم نشاط سوق تداول العقارات على مستوى العالم وإمكانية إنهاء الإجراءات الخاصة بانتقال الملكية والسداد الكترونيا.

#### ■ سهولة اعداد الدراسات البحثية والاستكشافية والتسويقية:

وفرة وإتاحة كافة البيانات بشتى أنواعها بالمواقع الالكترونية المتخصصة مثل Bloom Burg، اسهم في إمكانية اعداد الدراسات البحثية والتسويقية عن أي مؤسسة أو منظمة باي بلد على مستوى العالم دون اللجوء الى طرق جمع البيانات بالاساليب التقليدية، والذي

المخاطر ينبغي على كل مؤسسة التعرف عليها بشكل جيد ودراسة كيفية إدارة المخاطر الناشئة عنها قبل اخذ القرار بإقتناءها، فعملية إدارة نظم المعلومات لا بد وأن يتم تطبيقها وفقا لقواعد حوكمة نظم المعلومات، والتحقق من توافقها مع أهداف المؤسسة. وفيما يلي بعض العيوب والمخاطر الهامة التي قد تنتج في حالة في اختيار تطبيق النظم التكنولوجية الحديثة:

- ارتفاع التكاليف المتعلقة باقتناء وصيانة النظم التكنولوجية الحديثة
- زيادة تكاسل العاملين، وعدم الاستغلال الكفء لساعات العمل والتي تنتج من الاقدام على اقتناء كل ما هو حديث من النظم التكنولوجية التي تساعد في تسهيل سير العمل بالمؤسسة وتقليل حجم الأعمال.
- زيادة احتمال مخاطر الهجمات أو الاختراقات الأمنية للنظم الالكترونية والتي تأخذ شكل موجات متعددة من الهجمات الالكترونية على المستوى العالمي.
- ارتفاع التكاليف المتعلقة بحماية النظم التكنولوجية الحديثة نتيجة للتطور التكنولوجي وتزايد الاعتماد على النظم الحديثة في ادره نظم المعلومات فان الهجمات الالكترونية تعتبر من المخاطر الهامة على المستوى العالمي والتي تتطور بتطور نظم الحماية مثال:

Wanna Cry, Ransom ware & Remote Access Trojan (RAT) والمعروف Joanap، وهو ما يساعد على ارتفاع تكاليف الحصول على نظم الحماية المتطورة والحديثة التي تمنع حدوث مثل تلك الهجمات.

- زيادة تعرض المنشآت الصغيرة للهجمات الالكترونية أو الاختراقات الأمنية لعدم قدرتها على توفير نظم الحماية الامنة او الحديثة لارتفاع تكاليف الحصول عليها.
- عدم التخطيط الجيد للحصول على النظم التكنولوجية الحديثة قد يؤدي الى مخاطر توقف الانتاج او تعرض البيانات للفقد مما يؤثر على حجم أعمال المؤسسة.

من شأنه ساعد المؤسسات في تحسين ميزات التنافسية وجذب مزيد أكثر من العملاء والتوسع في الاسواق العالمية.

### ■ امكانية تخزين واسترجاع كم هائل من البيانات:

تعتبر المعلومات من المصادر الهامة لاي مؤسسة التي تمكنها من تحسين أداءها أو اتخاذ قرار يتعلق بمجال نشاطها، ومع التقدم التكنولوجي العالمي والنمو الهائل لحجم البيانات Big Data التي تعتمد عليها المؤسسة في تحسين مستوى أداء انتاجها او الخدمات التي تقدمها، والتي تمكنها من التعرف على احتياجات العملاء المختلفة والمتطورة للحفاظ على مستوى رضاء العميل، فقد ظهرت الحاجة الى ضرورة تخزين وتشغيل واسترجاع لكم الهائل من البيانات والذي ينمو بشكل مستمر في ظل ذلك التطور التكنولوجي .

### ■ خفض التكاليف الانتاجية وحجم الأعمال :

ادى التطور التكنولوجي الى خفض التكاليف الانتاجية من خلال اتباع طرق معالجة التشغيل الصحيحة وتقليل نسبة الهالك وتخفيض الوحدات المعيبة من خلال التطبيقات المبنية على الذكاء الاصطناعي Artificial Intelligent التي تساعد في امكانية الادارة عن بعد للمراكز الانتاجية التي تتميز بالمخاطر العالية أو بأماكن بعيدة دون الانتقال اليها، أمكانية التدخل الفوري للقيام ببعض العمليات الحرجة التي تتطلب التدخل السريع من خلال استخدام robots لاجراء العمليات الجراحية الحرجة التي تتطلب التدخل الفوري مع عدم توافر المختصين بذلك.

### III. العيوب والمخاطر التي قد تنتج من تطبيق المتغيرات

#### التكنولوجيا الحديثة:

وعلى الرغم من المزايا العديدة التي يحققها التطور التكنولوجي إلا أن بعض التطورات التكنولوجية قد تعتبر غير مناسبة الاستخدام مع بعض المؤسسات إما لطبيعة أعمالها التي لا تتناسب معها أو لارتفاع تكاليف اقتناء هذه التكنولوجيا بما يؤثر على قدرتها الانتاجية، او انها قد لا تحقق المنافع الكافية للمؤسسة مقارنة بتكلفة اقتناءها . كما أن بعض التقنيات الحديثة قد يصاحب تطبيقها خلق نوعية جديدة من

- http://health.usf.edu/is/blog/2018/02/08/impl .5  
 ementing-new-technology-challenges-  
 advantages-and-goals  
 https://www.information-age.com/modern- .6  
 technology-advantages-disadvantages-  
 123465637/  
 https://www.infosys.com/industries/financial- .7  
 services/white-papers/Documents/fintech-  
 revolution-banking.pdf  
 https://www.itgovernance.co.uk .8  
 http://www.wired.co.uk .9

■ تهدف معظم الاكتشافات التكنولوجية الحديثة الى تقليل الجهد البشري والاعتماد أكثر على الآلات في بعض الوظائف Reboot technology مما يساعد في ارتفاع نسب البطالة والاستغناء عن بعض الوظائف

## المراجع:

- 1 . https://www.iaa.nl/actualiteit/nieuws/rethinking-the-audit  
 2 . https://ic.globaliaa.org/Documents/CS-4-9.pdf  
 3 . https://www2.deloitte.com/content/dam/Deloitte/us/Documents/finance/us-internal-audit-innovation.pdf  
 4 . https://www.pwc.com.au/assurance/assets/innovation-internal-audit-nov09.pdf

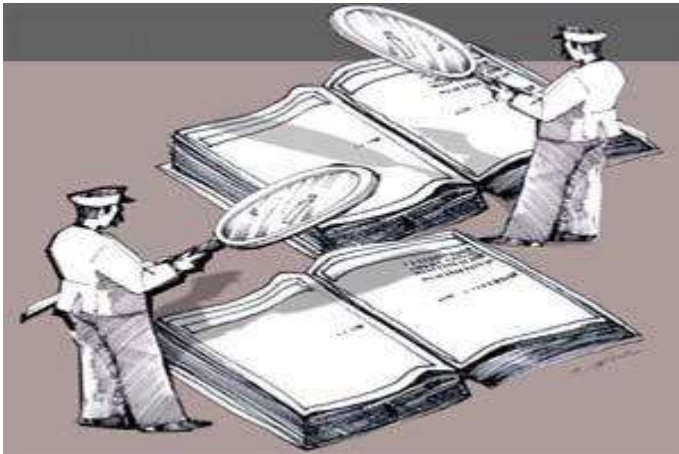
للتواصل مع الكاتب: mervat\_cia@yahoo.com

# الوصفة السحرية

## لتحفيز الأنشطة الرقابية في المؤسسات

بقلم السيد سامر حمد الله CFSA، CIB، CICS، مدير إدارة المخاطر، القطاع المصرفي، الأردن

لكن هل فكرنا في أصل هذه المعضلة! وما أسباب انتشار هذه الانطباعات السلبية عن الأنشطة الرقابية في المؤسسات (في أغلب الأحيان!).



من تجربتي الشخصية، أعزى ذلك لسببين رئيسيين:

**الأول،** سبب تاريخي لانطباع مهني متوارث من الأجيال السابقة جزء منه يعود اللوم فيه علينا نحن -مسؤولي وموظفي الدوائر الرقابية- حيث أن بعضنا استخدم السلطة والقوة الإدارية الممنوحة لنا بشكل سلبي وتعامل بفوقية -أحيانا -مع الزملاء في الدوائر الأخرى مما خلق ذلك النفور لديهم من كل نشاط داخل المؤسسة متعلق بالرقابة والتدقيق الداخلي وفي مراحل لاحقة ضم إدارات المخاطر الى المجموعة "الغير مرغوب فيها"، إذا صح استخدام هذا المصطلح.

إذا كنت أحد العاملين في إدارة التدقيق الداخلي-إدارة المخاطر-إدارة الرقابة الداخلية، فأنت بالتأكيد تعاني. تعاني من ماذا؟ لنطرح بعض التساؤلات التالية ونرى ما هو ردك.

- عند تعاملك مع زملائك في الدوائر الأخرى (دوائر الأعمال- دوائر الدعم)، هل تشعر بأنهم يتفهمون الغاية من وجودك للتدقيق عليهم؟!
  - هل يتعاونون معك بصدق أم بخوف؟
  - هل تلاحظ ايجابية في تقبل ملاحظات التدقيق الداخلي؟
  - هل تلاحظ تفهمهم لدورك كمسؤول لمخاطر التشغيل/الائتمان/السيولة... عند رفع توصية تختلف مع توصياتهم؟
  - هل يقوموا بالتعاون بالإبلاغ عن الحوادث التشغيلية حسب اجراءات المؤسسة؟ هل تشعر بتفهمهم للغاية من ذلك؟
  - هل سمعت زملاءك في الدوائر الأخرى وهم يعيرون عن رأيهم بالدوائر الرقابية على أنها للتنظير فقط!
- الكثير من نمط هذه التساؤلات قد يخطر على بال أي منا -مسؤولي وموظفي الدوائر الرقابية- كل حسب تجاربه والمواقف التي تعرض لها خلال مسيرته العملية. ولكن اعتقد جازما أن ردودنا جميعا على هذه التساؤلات أعلاه ستكون متشابهة بنسبه عالية جدا، وهي للأسف ستكون سلبية!

الحديثة من تلك المفاهيم الخاطئة أو البالية التي يمكن لمدراءهم توريثها لهم من خلال أعمالهم اليومية.

فمثلا: قبل عدة سنوات قامت إحدى المؤسسات باستقطاب 9 من الخريجين الجدد من المتفوقين في تخصصاتهم الجامعية من خلال برنامج اعداد موظفين مميزين ليكونوا في المستقبل القريب قادة كفوئين للمؤسسة. وتم اخضاعهم لبرنامج توعوي وتدريبى خاص. ولحسن الحظ كان التدقيق الداخلي من ضمن البرنامج التوعوي (خلافاً للمؤسسات الاخرى التي غالبا لا تشمل التدقيق الداخلي بأي من هذه البرامج). وعندما جاء أولئك المتفوقين، كل في يوم منفصل، دهشت لعدم معرفة أي منهم بقيمة هذا النشاط في المؤسسات وهم جميعا خريجي تخصصات إدارية مختلفة (إدارة أعمال، محاسبة، تجارة واقتصاد...) بل أن أحدهم لم يستطع أن يعرّف التدقيق الداخلي تعريفا يقارب الصحيح!!

فالحل باعتقادي بات واضحا وليس بحاجة لكثير من الكلام، الحل يكمن في: التوعية والتثقيف. اكررها مرة ومرة وألف مرة. إن من أصعب التغييرات التي يمكن فعلها هو تغيير الثقافة لدى الناس ومشكلتنا الأساسية هي الثقافة المغلوطة التي يحملها الأغلب من زملائنا في الدوائر الأخرى في مؤسساتنا. ولكن، كيف!



التدقيق قيادة ابداع تطوير

والجزء الآخر يعود على زملائنا في الدوائر الأخرى الذين لم يواكبوا تطور فكر هذه الأنشطة الرقابية وورثوا أفكارهم السلبية للأجيال الجديدة من خلال ترهيبهم من أثر الدوائر الرقابية عليهم في تطورهم الوظيفي وتحقيق مستهدفاتهم البيعية/الربحية. حيث أنهم ارتقوا في السلم الوظيفي في المؤسسات لمناصب قيادية نتجت عن تفوقهم في أعمالهم ولكن لم ينظروا لوهله أن الأنشطة الرقابية - وابتداء التدقيق الداخلي- قد تطورت أفكارها وأساليبها بحيث أصبحت "شريك" business partner وليس "خصم".

شخصيا، حدث معي موقف خلال الأشهر الأولى من عامي الأول في الحياة المهنية، حيث كنت أعمل في دوائر العمليات المركزية. في أحد أيام العمل دخل شخص الادارة صباحا (لم أكن أعرفه مسبقا) وختم بطاقة الدوام الورقية التي كان يحملها في حقيبة يده. وإذ برئيس القسم المسؤول عني يهمس لي "أعوذ بالله، هذا الانسان قميء" فاستسرت مستغربا: من هذا؟! فأجاب بنبرة احتقار: " هذا مدقق، وأكد هو قادم ليلقي بلواه على أحد الأقسام" وفرح كثيرا بعد ما علم أن قسمنا ليس القسم المنشود من هذه الزيارة.....!!! هذا بالضبط ما كان يشعرنى به العديد من الزملاء عند زيارتي لهم عندما صرت مدققا بعد هذه الحادثة بعشرة سنوات تقريبا.

أما السبب الثاني، فإن المؤسسات لم تعنى بشكل مؤثر بتثقيف الجيل الجديد الذي ينضم سنويا إلى كوادرها بتوعيتهم وتثقيفهم بمفاهيم الرقابة الداخلية وإدارة المخاطر والحوكمة وأثرها الإيجابي على أعمالهم وعلى تطور الفكر المؤسسي عموما وفي جميع الدول بشكل نسبي. إضافة الى أنه وللأسف حتى الجامعات لم تطور مناهجها بحيث تتضمن شروحات وافية لمفاهيم الرقابة وإدارة المخاطر والحوكمة بحيث يتم إعداد الطلاب الذين هم نواة القادة لتلك المؤسسات مستقبلا بحيث تجعل أولئك القادمين الجدد يميزون المفاهيم الصحيحة أو

مع المسؤولين عن التعليم العالي للحث على تطوير المناهج الجامعية بحيث تواكب الأفكار والأساليب الحديثة للأنشطة الرقابية مما يساعد على تزويد سوق العمل بخريجين يتمتعون بالوعي والتعليم السليم الذي تستطيع المؤسسات البناء عليه بشكل أسهل عند انضمام هؤلاء الخريجين للمؤسسات. فأولئك هم الذين سيتبوأوا المناصب الإدارية والقيادية بعد زمن ليس ببعيد من السنين وبالتالي سيكونوا هم من سيطالب بأن تكون المؤسسات التي يملكونها أو يقودونها تتمتع بأنشطة رقابية كفؤة وفعالة وتعمق المفاهيم السليمة للرقابة الداخلية والمخاطر والحوكمة وغيرها مما قد يتطور من أنشطة رقابية مستقبلا.



للتواصل مع الكاتب: samrallah@gmail.com

بقناتي هنالك طريقان أحدهما أسهل من الآخر وبالعكس!!

**الأول** نتائجه أسرع ولكن تحقيقه ليس سهلا... كلنا يعلم المقولة المهنية التي نكرها دائما في جميع المحاضرات والمؤتمرات... **Tone at the Top**... إذا صلح الرأس صلح كامل الجسد. على مجالس الإدارة والإدارات التنفيذية العليا العمل بشكل فعال لضمان نشر الوعي والثقافة اللازمة لدى جميع العاملين في المؤسسة. لو فكرنا قليلا سنجد أن مجالس الإدارة تبذل الكثير من الوقت والأموال في اللجان والاجتماعات ولكن فقط لإرضاء المتطلبات التشريعية وليس بشكل أساسي لإيمانهم بأن هذه اللجان والاجتماعات هي وسيلة مهمة لإيصال الرسائل لكل العاملين في المؤسسة وعلى رأسهم الإدارة التنفيذية العليا بجدية اهتمام المجلس بإدارات التدقيق الداخلي والمخاطر وماتانة نظام الرقابة الداخلية. فلو تم بذل نفس الجهد والوقت والمال ولكن بتغيير الهدف بحيث يكون التأثير إيجابا على فعالية الأنشطة الرقابية لكانت النتائج أعظم من حيث تطوير البيئة الرقابية وتقليل المخاطر أو ادارتها بشكل أكثر فاعلية مما سينتج أرباحا أفضل على المدى البعيد. ففي حقيقة الأمر هذه الأنشطة الرقابية تابعة لمالكي المؤسسة ووجدت لحمايتهم فمن الأجدر العناية بهم بطريقة أفضل.

أما **الثاني** فيحتاج لوقت أطول ولكن تحقيقه أسهل. إن التركيز على الجيل الجديد من خلال التدريب والتوعية المستمرة بالقيمة التي تضيفها الأنشطة الرقابية في المؤسسة لأعمالهم ولتطورهم الإداري. هذا الجيل الذي إذا صلح سيصلح مستقبل البيئة الرقابية للمؤسسات وسيورثون الأجيال التي ستأتي من بعدهم إرثا سليما غير الإرث الموجود حاليا. أيضا أو من أنه يجب التواصل بطريقة أو بأخرى

# LE NOUVEAU CADRE DE MANAGEMENT DES RISQUES "COSO II" de 2017: CONSIDERATION DU RISQUE DANS LE PROCESSUS D'ETABLISSEMENT DE LA STRATEGIE ET DE LA CONDUITE DE LA PERFORMANCE

Par M. KRIMI Abdessatar, CIA, CRMA, DPAI, IRCA, PECB, IFC, DSRM, Tunisie

## COSO



### I. À propos de COSO

Créée à l'origine en 1985, COSO (Committee of sponsoring organizations of the treadway commission) est une organisation volontaire relevant du secteur privé, présidée par James C. Treadway, qui s'emploie à améliorer les performances organisationnelles et la gouvernance grâce à un contrôle interne efficace, à la gestion des risques de l'entreprise et à la dissuasion de la fraude. COSO est parrainé conjointement par l'American Accounting Association (AAA), l'American Institute of Certified Public Accountants (AICPA), Financial Executives International (FEI), l'Institute of Management Accountants (IMA) et The Institute of Internal Auditors (IIA).

### II. Genèse du cadre de référence COSO II

L'"Entreprise Risk Management- Integrated Framework" présenté sous l'acronyme COSO II publié en 2004 est le prolongement de l'"internal control- integrated framework" (COSO I) publié aux Etats Unis en 1992.

Le cadre original rédigé par PwC (Price waterhouse coopers) en 2004 est un référentiel largement accepté et utilisé par les entreprises pour améliorer leur capacité à gérer l'incertitude et à déterminer le risque à accepter car il vise à accroître la valeur des parties prenantes.



Faut-il remarquer que PwC a eu une relation de longue date avec COSO et, par conséquent, a été engagé le 21 octobre 2014 par le conseil d'administration de ce dernier ainsi que les organisations parrainantes en tant qu'auteur principal de la mise à jour. Le projet a généré des intérêts globaux et interprofessionnels dans les secteurs public et privé.

Le nouveau Cadre, maintenant intitulé Enterprise Risk Management - Intégrant la Stratégie et la Performance, conserve et s'appuie sur les points forts de la publication originale de 2004 tout en clarifiant et élargissant les orientations où il a été jugé utile de le faire.

### III. Pourquoi cette mise à jour de COSO II ?

Développé à l'origine en 2004 par PwC sous la direction du Conseil de COSO, le cadre intégré "COSO ERM" est l'un des cadres de gestion des risques les plus largement reconnus dans le monde.

La mise à jour du cadre, qui s'appuie sur son prédécesseur, vise à améliorer son contenu et sa pertinence afin que les organisations du monde entier puissent tirer le meilleur parti de leurs programmes de gestion des risques d'entreprise.

Cette mise à jour souligne l'importance de la gestion des risques de l'entreprise dans la planification stratégique. Il met également l'accent sur l'intégration de l'ERM dans toute l'organisation, car le risque influence la stratégie et les performances dans l'ensemble de l'organisation.

Au cours de la dernière décennie, la complexité du risque a changé et de nouveaux risques sont apparus. Un appel des parties prenantes pour une plus grande transparence et responsabilisation ainsi que l'importance des discussions sur les risques au niveau du conseil d'administration ou de surveillance et des dirigeants ont suscité un examen et un rafraîchissement du Cadre pour aborder l'évolution de la gestion des risques de l'entreprise et la nécessité pour les organisations d'améliorer leur approche de gestion des risques .

### IV. Contenu du nouveau cadre de management des risques "COSO II"

Le nouveau cadre décrit comment les dirigeants peuvent avoir une plus grande confiance en face à de nombreux défis d'affaires stratégiques du 21ème siècle, car ils naviguent dans l'évolution des marchés, l'innovation rapide et un arsenal réglementaire renforcé.

Le Cadre est conçu pour transformer un monologue de risque préventif et basé sur des processus en une conversation proactive axée sur les opportunités pour découvrir comment la gestion des risques peut créer, préserver et réaliser la qualité et la valeur pour l'entité.

Le Cadre traite de l'évolution de l'ERM, des avantages qui peuvent être obtenus et de la nécessité pour les organisations d'améliorer leur approche de la gestion des risques.

La première partie de cette publication, mise à jour, offre une perspective sur les concepts et les applications actuels et évolutifs de la gestion des risques de l'entreprise.

La deuxième partie de ce Cadre, est organisée en cinq composantes faciles à comprendre qui tiennent compte des différents points de vue et des structures d'exploitation, et améliorent les stratégies et la prise de décision.

Ces 5 composantes sont interdépendantes et divisées en 20 principes différents

Les principes sont gérables en taille, et ils décrivent des pratiques qui peuvent être appliquées de différentes façons pour différentes organisations indépendamment de la taille, du type ou du secteur. L'adhésion à ces principes peut fournir à la direction et au conseil une attente raisonnable que l'organisation comprend et s'efforce de gérer les risques liés à sa stratégie et à ses objectifs.

Le cadre est axé sur l'avenir et traite de plusieurs tendances auxquelles les entités sont susceptibles de faire face et auront un effet sur la gestion des risques de l'entreprise, telles que :

- Faire face à la prolifération des données
- Tirer parti de l'intelligence artificielle et de l'automatisation
- Gérer le coût de la gestion des risques
- Construire une organisation plus forte

#### V. Les avantages de la mise à jour de COSO II

La mise à jour se concentre sur les défis et l'évolution des attentes en matière de gestion des risques d'entreprise auxquels sont confrontés les

leaders et les conseils dans le paysage actuel, y compris les changements dans les marchés économiques, l'évolution des technologies et l'évolution de la démographie dans le but de soutenir la prise de décision.

Cette mise à jour répond à l'appel pour un accent plus important sur la façon dont la gestion des risques d'entreprise intègre la stratégie et sa mise en œuvre ainsi qu'aux performances. Il ne fait aucun doute que les organisations continueront à faire face à un avenir plein de volatilité, de complexité et d'ambiguïté.

La gestion des risques de l'entreprise sera une partie importante de la manière dont une organisation gère et prospère à travers ces temps. De nombreux risques deviennent de nature plus globale et plus interconnectés.

#### Les avantages à tirer de cette mise à jour du COSO II sont les suivants :

- fournit une meilleure compréhension de la valeur de la gestion des risques de l'entreprise lors de l'établissement et de la mise en œuvre d'une stratégie.
  - améliore l'alignement entre la performance et la gestion des risques de l'entreprise afin d'améliorer l'établissement des objectifs de performance et la compréhension de l'impact du risque sur les performances.
  - répond aux attentes en matière de gouvernance et de surveillance.
  - reconnaît la mondialisation des marchés et des opérations et la nécessité d'appliquer une approche commune, quoique adaptée, à travers les régions

géographiques.

- présente de nouvelles façons de voir le risque pour établir et atteindre des objectifs dans le contexte d'une plus grande complexité commerciale.

- développe le reporting (les rapports) pour répondre aux attentes en faveur d'une plus grande transparence des parties prenantes.

- contient l'évolution des technologies et la prolifération des données et des analyses pour soutenir la prise de décision.

#### VI. A qui profitera cette mise à jour du COSO II

- Président Directeur Général
- Conseil d'Administration
- Contrôleurs
- Managers

#### CONCLUSION :

Le cadre de référence COSO II, mis à jour, vise à aider les organisations à être plus résilientes et mieux positionnées pour capturer à temps la hausse des paysages à risques changeants. Cela explique les interconnexions entre les risques, la gouvernance et le contrôle interne.

Les attentes quant à l'efficacité et à la valeur de la gestion des risques ont évolué de manière significative et couvrent tous les niveaux d'une organisation, de son conseil d'administration et de sa direction à des gestionnaires fonctionnels. La mise à jour de COSO II publiée en 2017 s'appuie sur les concepts développés dans le cadre original de 2004, reflète l'évolution de la pensée et des pratiques de gestion des risques d'entreprise et tient compte de l'émergence de mégatendances globales et de l'évolution des attentes des parties prenantes.

En dernière analyse, l'objectif global de cette mise à jour étant de continuer à encourager une culture consciente des risques.

Pour plus d'informations, n'hésitez pas à contacter l'auteur : [abkrimi@yahoo.com](mailto:abkrimi@yahoo.com)

# The 2018 Update of ISO 31.000

Written by : Mr. Hans Læssøe, AKTUS (www.aktus.dk), Denmark



Somewhat later than planned, the ISO 31,000 risk management standard update was released in February 2018. When addressing this, there are two findings, which stands out :

- The 2018 edition is better than the former 2009 edition
- It is an update – it is not a complete change of the approach to risk management. Hence if you are already in line with the ISO 31,000 standard, there may not be any need to change your overall approach

This leaves the ISO 31,000/2018 (ISO) well ahead of the updated COSO standard despite the almost quantum leap the 2017 update has been given since the 2004 edition.

ISO is based on a reduced set of nine core principles which is a strong and effective approach to standardising risk management. Recognising that all companies and organisations are unique in one way or another, one principle (# 3) states that risk management must be tailored to the individual organisation. As such, there is no “one size fits all”, and hence any attempt to create a standard based

on standardized processes and governance structures is ineffective.

These nine principles constitute the foundation of ISO risk management – and if/when an organisation builds its risk management approach, systems, processes and structures around these – they will be highly likely to have an effective and efficient risk management which truly add value and competitive advantage vis a vis lagging competitors. Importantly, one principle includes a push for continuous improvement.

The standard emphasizes that risk management must be an integral part of decision making. This was also stated in the 2009 edition but appears to have been largely ignored by risk managers and executives/boards across the globe. Common risk management practices are still reactive safety measures on already made decisions rather than an element of proactive decision support.

In the 2018 this “integrated in decision making” is stated repeatedly and is hence very hard to continuously ignore. To me, this is a fabulous lever for risk professionals, which they can use in

their discussions with top management and boards as to how to develop and improve the handling of risks – be it positive or negative risks of the company.

I can only encourage risk professional who are not involved in decision making to vigorously use the updated ISO as leverage to get involved in strategic planning, sales & operation planning, resource allocation, budgeting – and other business processes, which make decisions under uncertainty ... as all decision processes do.

This means that risk managers should look at any decision process, and address how that includes uncertainties (if at all) – and how can the risk profession add value to that approach. This will enable risks to be taken deliberately, intelligently and on an informed basis.

In any organisation there are multiple categories of risks taken, and here ISO in my perspective fall somewhat short in recognizing these. I agree, that by the end of the day, it all comes down to some element of decision making – but the systematic and often highly efficient approach many companies have to standard risks such as currency volatility, credit risk, employee safety, natural disasters, IT operational safety, manufacturing errors, etc. is not tangibly handled in ISO – which appears to focus on the risks taken by business decisions from strategy to day-to-day management.

However, this somewhat falls in line with the fact that the ISO 9000 standard, which over years is gradually moving into becoming a Total Quality Management (TQM) approach now explicitly requires risks and opportunity management being embedded in processes.

Hence – the two ISO standards may appear to “collaborate” where operations and standard risks are being embedded in the company TQM

approach, and risk management is focused on decisions.

This may very well be a deliberate and good development – especially as multiple business analyses indicate that 80% of all major risks hampering companies are driven by (bad) decisions or poor strategizing. Despite this – too many companies and organisations – do not have explicit processes and tools to systematically identify and address the uncertainties and risks taken by decisions. Furthermore, it appears that the higher the level of management involved (and the higher potential impact), the less systematic is the risk management.

As stated – the update is an update. Yet, to many companies, the full application of this will lead to a significant improvement of the value risk management provides for the company.

Such an increase is highly needed for organisations if they are to persevere in the world ahead. Changes happens today more often and with bigger impact than ever before. Extrapolating this means that changes today happen less frequently and with less impact than ever in the future that lies ahead. To survive and prosper – organisations must mentally leave the concept of risk management as they know it and implement a culture and approach of intelligent risk taking. Such an approach is fully in line with the updated ISO 31,000/2018 standard.

## ISO 31000:2018 published



For further information, contact the author :  
hl@aktus.dk

# التطور المتسارع في التشريعات الرقابية والمعايير الدولية

## وأثره على أعمال البنوك

بقلم السيد إبراهيم الطعاني، رئيس وحدة التدقيق الداخلي بالبنك الأردني الكويتي

### 1. مقدمة

تخضع البنوك لعدة جهات رقابية وتشريعية محلية ودولية متعددة كذلك فهي ملزمة بتطبيق المعايير الدولية المتعلقة بالمحاسبة والتدقيق الداخلي والخارجي، حيث يصدر العديد من التعليمات والأنظمة والقوانين منها ما هو جديد يطبق لأول مرة ومنها ما هو تعديل وتحديث للقائم، ولابد من الإشارة هنا إلى تطور الوسائل التكنولوجية المستخدمة في التعاملات المصرفية بشكل كبير وهذا يسبب الزيادة في المخاطر المحتملة وخاصة مخاطر الاحتيال الإلكتروني. ونكون جازمين بالقول بأن البنوك هي من أكثر القطاعات الاقتصادية الخاضعة للرقابة من عدة جهات ويعود ذلك إلى عدة أسباب أهمها أن تعثر أحد البنوك لا يسمح الله لن يكون تأثيره محدود على ملاك (مساهمين) البنك بل سيؤدي ذلك إلى ضياع حقوق المودعين والتأثير السلبي على المقترضين وقد يمتد تأثيره على البنوك الأخرى والقطاع الاقتصادي في البلاد.

### 2. التحديات التي تواجه البنوك للاستمرار بالنشاط المصرفي:

معظم البنوك غير راضية عن كثرة القوانين والأنظمة والتعليمات الصادرة عن عدة جهات سواء كانت محلية أو خارجية ومن وجهة نظر البنوك فإن تلك التشريعات والأنظمة تعيق العمل وتزيد الكلفة على البنوك بشكل كبير سواء من حيث الحاجة إلى المزيد من الموارد البشرية أو الأنظمة الآلية المتعددة لتطبيق تلك التشريعات إضافة إلى أن تطبيق بعض معايير المحاسبة الدولية (IAS) ومعايير التقارير المالية الدولية (IFRS) سيكون له أثر سلبي على نتائج أعمال البنوك ولا تكاد تخلو استراتيجية أي بنك من مثل هذه التحديات والتي يمكن

تبويبها من حيث الجهات الرقابية التي تخضع لها البنوك ومن حيث التشريعات والنظم الرقابية التي يجب تطبيقها للاستمرار في النشاط .

#### 1.2. الجهات الرقابية التي تخضع لها البنوك:

من أهم الجهات الرقابية التي تخضع لها البنوك ما يلي:

\***البنوك المركزية المحلية والإقليمية (إن وجدت)** وكذلك البنوك المركزية في الدول المضيفة في حال وجود تفرع خارجي للبنك سواء كان هذا التفرع على شكل فروع خارجية أو شركات تابعة. وتهدف البنوك المركزية بالدرجة الأولى إلى حماية المودعين وحماية الاقتصاد من أية تبعات ناتجة عن تعثر البنوك.

\***هيئات سوق المال المحلية وفي الدول المضيفة** وذلك في حال وجود انتشار خارجي للبنك على شكل شركات تابعة وذلك بحكم أن البنوك عبارة عن شركات مساهمة، حيث يصدر عن تلك الهيئات العديد من التشريعات والتي تهدف بالدرجة الأولى إلى حماية المساهمين الحاليين والمستثمرين المحتملين مستقبلاً.

\***وحدات مكافحة غسل الأموال** فيما يخص عمليات مكافحة غسل الأموال وتمويل الإرهاب، وكما هو معلوم فإن تلك الوحدات تحرص على قيام البنوك بتطبيق ما يصدر عن المنظمات الدولية بهذا الخصوص مثل مجموعة العمل المالي (FATF)، مجموعة العمل المالي لمنطقة الشرق الأوسط وشمال افريقيا (MENAFATF)، مجموعة (EJMONT) لوحدات الاستخبارات المالية... الخ.

#### 2.2. التشريعات والنظم الرقابية التي يجب تطبيقها:

وبالعودة إلى أهم الأنظمة والتعليمات الحديثة والمعدلة الصادرة عن البنوك المركزية نجد ما يلي:

نظر البنوك حيث أن تلك التشريعات والتعليمات لها جوانب ايجابية متعددة وذلك من عدة نواحي أهمها:

1. الفصل في المهام والفصل بين المساهمين ومجلس الإدارة والإدارة التنفيذية،
2. تعزيز أنظمة الضبط والرقابة الداخلية وخطوط الدفاع الثلاثة والحد من حالات الاحتيال وحالات غسل الأموال وتمويل الإرهاب وارتكاب الأخطاء،
3. حماية معلومات العملاء ومعلومات البنك وتجنب العقوبات الدولية.

وبالإضافة لذلك فإنه على البنوك أن لا تنظر إلى مصالحها الفردية وجانب الربحية فقط فهي لا تعمل في بيئة معزولة عن القطاعات الأخرى والبلدان الأخرى وأن أية مخاطر يتعرض لها البنك سيكون لها آثار سلبية على البنوك الأخرى والقطاعات الأخرى، وإن ترك الخيار للبنوك لتطبيق ما تريد لن يحقق العدالة بين البنوك بل على العكس سيكون بمثابة عقاب للبنوك الملتزمة.

وفي النهاية يفترض في البنوك أن تكون على وعي ودراية بأنها تعمل في بيئة رقابية متغيرة ومتطورة وعليها أن تكون مستعدة لتلك التغييرات سواء من حيث الاستثمار في الموارد البشرية أو الأنظمة الآلية.



➤ الحوكمة وحوكمة تكنولوجيا المعلومات والأمن السيبراني والحوسبة السحابية وحماية المعلومات والشفافية وحماية المستهلك المالي ومكافحة غسل الأموال وتمويل الإرهاب وقانون فاتكا... الخ، حيث أن الالتزام بتلك التشريعات والتعليمات يتطلب من البنوك المزيد من المصاريف والكلف للاستثمار في الموارد البشرية والأنظمة الآلية، إضافة إلى أن عملية التطبيق لها أثر سلبي على رضا العملاء وبالتالي مواجهة المزيد من المصاعب في جذب عملاء جدد والمحافظة على العملاء الحاليين.

➤ معايير المحاسبة الدولية ومعايير التقارير المالية الدولية وخاصة معيار (IFRS9) والذي بدأ تطبيقه من بداية هذا العام (2018)، فبالإضافة إلى الكلف اللازمة للاستثمار في الموارد البشرية والأنظمة الآلية لتطبيق المعيار فإن تطبيقه من وجهة نظر البنوك له نتائج سلبية على نتائج أعمال البنوك وذلك كون تطبيقه يتطلب البدء بإعداد مخصصات ديون للعملاء من تاريخ المنح وليس من تاريخ التعثر كما هو معمول به سابقاً، وبالتالي التأثير سلباً على أرباح البنوك.

➤ إرشادات بازل وخاصة ما يتعلق منها بكفاية رأس المال ففي الوقت الذي بدأت عملية التطبيق ببازل (I) نتحدث الآن عن بازل (IV) وهذا أدى ويؤدي إلى وجود ضغوط على عملية احتساب كفاية رأس المال وتضمنين معظم المخاطر في عملية الاحتساب وبالتالي البحث عن موجودات ذات مخاطر منخفضة على حساب الربحية للاحتفاظ بالنسب المطلوبة، إضافة إلى الحاجة إلى المزيد من التدريب والاستثمار في الموارد البشرية.

**الإيجابيات التي تتحقق من الالتزام بالتشريعات والنظم الرقابية على البنوك:**

بالرغم من التحديات المذكورة أعلاه ومن الكلف الإضافية التي قد تتكبدها البنوك إلا أن الجهات الرقابية والتشريعية لا تتفق مع وجهة

للتواصل مع الكاتب: [ibtaani@yahoo.com](mailto:ibtaani@yahoo.com)

# Rethinking the Three Lines of Defence

Written by : Mr. Hans Læssøe, AKTUS (www.aktus.dk), Denmark

Traditionally, companies have used a concept known as “Three Lines of Defence” (**3LoD**) to ensure actions and decisions were compliant with defined rules and regulations. The approach is still widely used and based on validation of compliance.

1. The line manager responsible for the decision/action is the first line of defence and responsible for operating within the frames provided.
2. An (semi)independent controlling function is responsible for validating the decisions and actions to ensure these are compliant with company rules and legislation.
3. An (often external) independent audit is responsible for making a last validation of compliance.

This approach works well in many cases, and hence the statistical likelihood that actions/decisions are non-compliant is vastly reduced.

That said – deliberate fraud and collaboration between a line manager and his/her controller can hide inappropriate actions to the extent the spot checks made by auditors will not lead to disclosure. When subsequently discovered, this leads to the scandals of ENRON, VW and many many others, where even high-level executives were proven to be fully aware of and thereby tolerated wrongful behaviour. The 3LoD is not effectively ensuring good decisions.

Furthermore, the process is inherently slow, reactive, laborious and is not adding value to the company when imposed on the many

decisions/actions which are fully compliant with company frames and legislation.

Today, and in the business environment of tomorrow, this is no longer viable for a number of reasons :

- With the ever-increasing speed of change there will not be time to have a separate process that validates decisions and actions. Bear in mind that the world will never in future change as slowly as it is today.
- In an ever-increasing competition companies will not be able to afford spending resources on validating decisions/actions that should be within some set of rules and frames – it is a process consumers and customers will not pay for.
- With an ever-increasing globalization companies operate in and serve multiple countries and cultures – and validating decisions/actions becomes complicated to the extent it will be next to unbearable.

I am not suggesting that we eliminate validation and aspects of what is essential quality control on decisions and actions. Leveraging and building on the developments of the 4<sup>th</sup> Industrial Revolution, I am suggesting that enhanced data capture systems and artificial intelligence (AI) will replace human processing and be able to turn on warning lights when decisions are borderline or outside defined frames and legislation.



Today, we see Google, Facebook and probably an abundance of others capture, look into and scrutinise social media data, and whatever else they can get hold of – to direct advertisement as well as sell the data to whoever wishes to buy them, for whatever purpose they may have, political or otherwise. Cambridge Analytics and alleged Russian influence on US elections are the latest cases in point. Something similar can be done by companies to ensure that decisions and actions are compliant – which opposed to secret data capture, is not unethical – and can be done in real-time and is hence not prolonging a decision process or an action. In fact, a real-time AI based frame and legal validation can serve as a decision support for the active manager as it may help direct the decision or action.

### The Preplacement – Three Levers of Decision

Managers on all levels still need support when making decisions in a complex and changing world, but this has to be value adding, proactive, simple, and seamlessly embedded into the decision process to allow adequate dynamics and speed.

Based on this, I suggest the 3LoD are replaced by three levers of decision– formulated in terms of questions the manager can ask himself whilst making a decision or taking an action:

1. How does this support the company mission ?
2. Is this ethically/morally sound ?
3. How certain is it, that this will be value adding to the company ?

Below, I will elaborate further on each of these.

#### 1. Supporting Company Mission

In short, actions and decisions have to be focused to drive the company fast enough to sustain its competitiveness in the world of the future. Hence, there are no time, nor money or resources to bother with anything else.

Warren Buffet work with this as his 5/25 rule. He asks people to define the 25 most important things to do. Then to rank/prioritize these in groups of five based on importance. Then simply discard all those, which are not in the highest priority group to ensure attention to and execution of these top five priorities – before attending to anything else.

In this context, it is important to note, that very few companies (and none that I have seen), have the mission of enhancing shareholder wealth. To list a few randomly selected :

**Google** To organize the world's information and make it universally accessible and useful.

**Nestlé** "Good Food, Good Life" is to provide consumers with the best tasting, most nutritious choices in a wide range of food and beverage categories and eating occasions, from morning to night.

**Amazon** To be Earth's most customer-centric company, where customers can find and discover anything they might want to buy online, and endeavours to offer its customers the lowest possible prices.

**Volvo** Driving prosperity through transport solutions.

**LEGO** Group Inspire and develop the builders of tomorrow.

All of these mission statements communicate that the company wishes to do something positive for their customers and consumers. Creating and enhancing shareholder wealth is not mentioned in the mission statement. Even mission statements of financial institutions focus on their service/value to their customers rather than executives and shareholders.

So ... how does your current decision or action support the mission of your company. If you cannot explain that in simple terms, you probably should direct your attention to something that does support your company mission.

## 2. Ethically/Morally Sound

With the expansion of social media and real-time global communication, transparency is unavoidable and uncontrollable. Abraham Lincoln is famed for stating that “You can fool all the people some of the time and some of the people all the time, but you cannot fool all the people all the time”. The quote may in fact not have been his and is suggested to stem from 17<sup>th</sup> century France.

Nevertheless, the days where companies or governments could control the flow of information are long gone, and where bad news formerly may be revealed “eventually”, they will now be revealed fast and uncontrollably – in some cases exacerbated by untrue “facts”.

As consumers and organisations are becoming increasingly aware of this, the risk of losing business due to a bad reputation – driven by disclosure of some bad behaviour – has increased significantly both in terms of likelihood, speed and impact.

The scandals surrounding British Petroleum and the Deep-Water Horizon accident, Union Carbide and the Bhopal accident, Volkswagen and the emission fraud and many others show, that unacceptable behaviour is, well, unacceptable – and will lead to substantial reduction of company/share value and hence deplete the value for shareholders. Bad behaviour is simply bad business.

When I entered corporate life decades ago, I was taught by an executive, that ethical decision making was not all that complex. “If you would hate to see a journalist write about your decision in tomorrow’s newspaper, you probably shouldn’t make it”. There are numerous other editions of this around – the essence is the same – if you are not willing to be transparent – you are possibly on a wrong track. Now, I am not relating ethics/morals to legislation for two reasons :

- The links between legislation and sound ethics are often somewhat opaque and defies logic. Furthermore, following the (letter of the) law may not be good enough to be morally justifiable in the eyes of your partners, consumers and the general public.
- Deliberately and knowingly breaking the law is not presumed to be a viable and acceptable business solution.

So ... is the decision/action I am about to make ethically sound ? If not, I probably need to find another way of meeting whatever target I have set.

## 3. Adding/Creating Business Value

The last lever of decisions is related to value creation. This may/need not be fiscal value but may be improving on any performance metric defined by the company such as injury rate, employee retention, environmental impact, brand value, customer satisfaction ... the list is endless and differs from company to company.

There are two important elements of this.

\* One is related to company value added. Over the years, I have seen many decisions and actions, which are aimed at promoting the individual deciding manager and/or his/her domain, irrespective of whether this adds value to the company. Such private “hobby horses” mis-directs attention and resources, which fewer and fewer companies can afford in a competitive world.

To remedy this, managers should be required to explain and justify added value to the company when making a decision.

\* The other element deals with the uncertainties inherently embedded in any decision made and action taken. The question becomes “What is the certainty/likelihood this will add the targeted value to the company”.

This means that a planned/expected/targeted value of the decision/action is defined.

I have seen multiple decisions made and actions taken, where there was not even an attempt to define what success looked like. When this is not defined, those involved cannot see, nor celebrate a success or be blamed for failing, and will be demotivated.

The latter also requires, that the decision includes intelligent risk taking, and hence that the risks and opportunities pertaining to the decision/action are identified, assessed and modelled in the business case, which is no longer a simple "income – cost = profit" statement, but includes e.g. Monte Carlo simulation of relevant uncertainties and hence shows that there is an e.g. a 60% likelihood this decision will deliver on or above target, and a 5% likelihood the outcome will impact the company negatively.

Based on which the risk taking can be managed and decided.

This drive risk professionals being involved in decision and business case preparation. In my experience, this involvement often also leads to identifying additional opportunities to pursue in a project, and an actual performance above target.

It is important to remember that risk management is not about implementing risk aversity – but about intelligent risk taking. Being safe, when the boat is rocking is not enough to remain competitive – we have to be able to rock the boat ourselves from time to time.

So ... how certain am I that this decision/action will add value to the company (and how do I know). If I cannot answer these questions, I still have some "homework" to do before the decision can be made intelligently.

### Closing Comments

The concept of using three lines of defence to ensure that decisions and actions are compliant with a defined framework of company rules and legislation is becoming increasingly cumbersome, slow and obsolete.

In a future, where speed of change, competition and globalization is ever-increasing, a more active and effective approach is needed.

I suggest that the meaning of the 3LoD abbreviation is changed to be the "Three Levers of Decision" as an active and integrated decision process element where deciding managers address the "quality" of their decision by asking the three questions mentioned.

Clear positive responses to all three questions will provide a reasonable certainty the decision/action is "good", whereas opacity and vagueness on one or more indicates a "bad" decision.

These elements can, as well as compliance issues, be validated, but in the world of the 4<sup>th</sup> Industrial Revolution, I suggest we leave it to AI based systems to do the validation as we do not have the time, nor wish to spend the money to have human beings serve as reactive decision validators.

---

For further information, Contact the author : [hl@aktus.dk](mailto:hl@aktus.dk)

# Gouvernance des ressources Humaines

Ecrit par : M. Ben Ali Marwen, Contrôleur des Finances CGF, Tunisie

## Introduction

Les Normes internationales pour la pratique professionnelle de l'audit interne de l'IIA (IPPF), dans sa version pour l'année 2017, définissent la Gouvernance comme « **Le dispositif comprenant les processus et les structures mis en place par le Conseil d'informer, de diriger, de gérer et de piloter les activités de l'organisation en vue de réaliser ses objectifs.** »

Partie intégrante du processus de Gouvernance de l'entreprise, la gouvernance des ressources humaines ou tout court gouvernance RH est un processus visant à garantir que l'élément humain de toute institution est soumis à l'éthique et aux compétences requises dans le travail. Il vise à développer tous les moyens nécessaires pour mettre en place des procédures de gestion des ressources humaines pour le système d'éthique et de compétence, notamment la sélection du personnel, la rémunération, l'engagement comportemental, la gestion de la performance et d'autres fonctions de gestion des ressources humaines.

Et vu l'importance de ce concept, L'Organisation Internationale de Normalization ISO a publié sa norme ISO 30408:2016 "Management des ressources humaines -- Lignes directrices sur la gouvernance humaine". Cette dernière fournit des lignes directrices et propose de mettre en place des outils, processus et pratiques destinés à favoriser le développement et l'amélioration continue d'une gouvernance humaine efficace au sein d'une

organisation. Elle s'applique aux organisations de toutes tailles et de tous secteurs, qu'elles soient publiques ou privées, à but lucratif ou sans but lucratif.

Dans ce même cadre et via cet article, nous allons mettre l'accent sur l'audit de la fonction RH comme pilier fondamental dans l'instauration d'une gouvernance RH dans l'entreprise. Des expériences tirées de l'administration tunisienne vont appuyer notre étude.



### I. Implication de la direction, facteur clé de la réussite de la Gouvernance RH

L'investissement est l'élément humain de l'un des éléments les plus importants de la réussite dans les institutions. A notre époque actuelle, les ressources humaines et la gestion des talents et la formation sont plus d'intérêt à la haute direction de l'institution et cela se reflète dans la conviction

croissante parmi les décideurs de l'importance du rôle joué par cette administration, qui conduit finalement à renforcer la position concurrentielle de l'institution.

Ces dernières années, les chercheurs se sont intéressés de plus en plus aux sciences de gestion, à la gestion des ressources humaines, au talent et à la formation, notamment sur les concepts modernes qui affecteront certainement les banques dans les décennies à venir. (Mondialisation), genre et générations Une nouvelle culture en ressources humaines a été mise en place qui croit en ces concepts et travaille à leur meilleure mise en œuvre.

En effet, toute direction d'une entreprise cherche à construire un modèle distinctif et pionnier dans la gestion, le développement et la gouvernance des ressources humaines. Elle vise aussi à élaborer et à mettre en œuvre une stratégie intégrée pour les ressources humaines de l'entreprise, à élaborer des cadres de gouvernance et à moderniser les systèmes et les pratiques en matière de ressources humaines des organismes gouvernementaux.

La direction soutient les efforts de modernisation des ressources humaines de l'entreprise, et la réalisation du lien entre les programmes et les initiatives des ressources humaines, ainsi que les objectifs et les priorités stratégiques de l'entreprise. Elle comprend la gestion et le soutien à la transformation des ressources humaines au niveau stratégique par la structure juridique et organisationnelle de l'entreprise et développement des ressources humaines et des applications pratiques et la mise à jour des ressources humaines, le leadership et les processus de planification de renforcement des capacités.

**Bref**, sans l'implication des dirigeants et des décideurs de n'importe quelle entreprise dans le processus de Gouvernance RH, ce dernier ne peut plus réussir voire même voir le jour.

## II. La culture d'entreprise, facteur primordial de la réussite de la gouvernance RH



Chaque entreprise possède sa propre culture, qui la distingue des autres. Cette culture inclut un ensemble de connaissances, de concepts, de valeurs et de rituels permettant de :

- Différencier l'entreprise des autres entreprises travaillant dans le même domaine
- Conduire l'engagement et la culture de l'intérêt collectif plus que l'attention personnelle de l'individu.
- Connecter l'entreprise à son personnel travaillant d'une part, et de s'adapter à l'environnement dans lequel elle est située....

L'audit interne est une carrière continue, non seulement en raison de l'évolution des milieux de travail, mais aussi en raison des changements dans les priorités des intervenants. Ces dernières années ont vécu l'émergence de l'audit de la culture en tant que nouveau domaine émergent sur lequel les dirigeants doivent se concentrer, en réponse à une prise de conscience croissante du fait que l'audit « visuel » ne suffit pas à lui seule. Un audit invisible ou «doux» issue de la culture de l'entreprise est indispensable à sa bonne gouvernance.

La culture d'entreprise ne se limite pas aux valeurs adoptées par l'entreprise, mais aussi à la façon dont l'entreprise transforme ces valeurs en réalité. Toute entreprise doit déployer, consolider et surveiller les valeurs souhaitées. Il est essentiel de savoir dans quelle mesure ces valeurs sont appliquées par le biais des rapports d'audit interne, en dépit des défis liés à l'application de cette méthodologie.

Les lignes directrices publiées par l'Association des auditeurs internes IIA du Royaume-Uni et d'Irlande ont récemment reconnu que "l'audit des indicateurs culturels est complexe .... Et reconnaît la nécessité pour les auditeurs internes d'être satisfaits de leur compréhension de la culture de leurs entreprises et de la culture du risque. "

Par conséquent, l'activité d'audit interne doit répondre à la question suivante : **Peut-on vraiment donner une confirmation et une assurance suffisante quant à l'efficacité des contrôles et de la politique de gouvernance de son entreprise pour faire face à des risques en cas d'absence d'intérêt à la culture d'entreprise et à la culture du risque ?**

Si vous avez des doutes quant à l'importance d'évaluer l'application de ces valeurs, vous pouvez se souvenir du modèle d'Enron et ses valeurs déclarées qui sont centrées sur la communauté, le respect, l'intégration.... Mais, où sont-elles maintenant ? Et de nombreux autres exemples provenant de différents endroits dans le monde (Lehman Brothers et American Global Group et Nortel) qui indiquent une forte corrélation entre la faiblesse de la culture et la performance de l'organisation, et son échec éventuel.

D'un autre côté, une bonne performance semble être soutenue par une bonne culture. Le succès des marques mondiales telles qu'Apple et Google est en partie attribuable à leurs cultures fortes, qui entretiennent des relations solides entre tous les entreprises, et établissent une solide approche de la performance.

Les auditeurs internes sont appelés à comprendre l'environnement réglementaire dans leurs installations conformément aux normes du Comité Treadway (COSO), mis à jour en 2017. Cependant, l'environnement réglementaire doit également être compris dans le contexte de l'audit visuel et de l'audit invisible. Le défi pour les auditeurs internes réside dans la différence complète entre l'évaluation de l'efficacité des audits invisibles et l'évaluation de l'efficacité des audits visuels. Il peut être démarré en regardant la signification des audits invisibles, qui incluent :

- Engagement envers l'éthique et l'intégrité.
- Comportement à risque.
- La surveillance du rendement et du contrôle internes par le conseil.
- Responsabilités, responsabilités et structures organisationnelles.
- Système de dépendance administrative et chemin de rapport.

- Pratiques de recrutement - Engagement à tirer des personnes qualifiées à la lumière des objectifs et des valeurs de l'établissement...

Bien gouverner son entreprise, c'est en fait bien gouverner sa culture d'entreprise. La gouvernance RH devient tributaire de la culture du personnel de chaque organisation.

Vu le rôle de l'audit dans la gouvernance RH, nous citons ces recommandations pour l'audit de la culture :

1. Étudier la forme de culture adoptée par l'entreprise et comment elle est évaluée à travers différents processus. Par exemple, l'entreprise adopte-t-elle des valeurs déclarées ? Quel type d'indicateurs existe-t-il pour évaluer dans quelle mesure le personnel applique ces valeurs ? Votre organisation mène-t-elle des enquêtes auprès des employés pour comprendre les opinions et les comportements des employés ? L'équipe de la haute direction écoute-t-elle le personnel et prend-elle des mesures appropriées au besoin ? Ont-ils une politique de communication avec les employés ou non ?

2. Veiller à ce que la culture d'entreprise soit prise en compte dans le cadre de gestion des risques de l'entreprise. Mais qui est responsable ? Par exemple, comment la politique de gestion des risques de votre entreprise gère-t-elle une culture de prise de risque ? Quel type de culture du risque est promu par l'entreprise ? Comment peut-il être comparé à la réalité ? Les activités à risque de l'entreprise sont-elles conformes à la tolérance au risque et aux politiques énoncées ?

3. En ce qui concerne le réglage de la stratégie d'audit interne et les plans annuels recommandent que vous êtes d'accord avec le conseil d'administration et l'équipe de direction de votre entreprise sur le sens de la culture pour l'entreprise et que la formule pour arriver à se mettre d'accord des rapports sur les questions intangibles pour maintenir la confidentialité et la sensibilité. S'assurer que le monde de l'audit inclut la culture de l'audit en tant que sujet d'audit clé, ou l'un des aspects couverts par toutes les fonctions d'audit. S'assurer que les plans de vérification interne sont conçus de manière à fournir des preuves de conformité aux contrôles invisibles tels que le leadership, l'éthique et les valeurs. Cela nécessitera un jugement bien informé. L'Institute of Internal Auditors IIA aborde l'utilisation du «courage inné» pour former une opinion.

4. Le cadre du Committee of Sponsoring Organizations de la Treadway Commission (COSO) fournit une bonne base pour évaluer l'environnement de gouvernance d'entreprise et garantir le type de culture réglementaire en place. Par exemple, les décisions sont-elles centralisées ou décentralisées. Quelle approche le Conseil d'administration a-t-il développé? La relation entre le conseil ET l'équipe de direction est-elle bonne? Quel genre de récompenses et d'incitations l'entreprise offre-t-elle aux employés et offre de les garder?

Changer sa culture d'entreprise à travers des audits RH bien ciblés passe par un audit de la culture de l'entreprise pour bien comprendre et réussir sa mission d'audit.

Nous incitons sur l'importance des audits RH et le changement de la culture de son personnel pour bien aboutir à une gouvernance efficace de son entreprise.

### III. Rôle de l'audit interne dans la gouvernance RH

Partie intégrante du processus de gouvernance d'entreprise, l'audit interne joue un rôle important dans l'évaluation du processus de gouvernance RH comme indiqué dans les NORMES INTERNATIONALES POUR LA PRATIQUE PROFESSIONNELLE DE L'AUDIT INTERNE (LES NORMES) IPPF, version 2017:

#### 2110 – Gouvernance

L'audit interne doit évaluer et formuler des recommandations appropriées en vue d'améliorer les processus de gouvernance de l'organisation pour :

1. Les prises de décisions stratégiques et opérationnelles ;
2. La surveillance des processus de management des risques et de contrôle ;
3. La promotion des règles d'éthique et des valeurs appropriées au sein de l'organisation ;
4. Une gestion efficace des performances de l'organisation, assortie d'une obligation de rendre compte ;
5. La communication aux services concernés des informations relatives aux risques et aux contrôles ;
6. La coordination des activités et la communication des informations entre le Conseil, les auditeurs externes, les auditeurs internes, les autres prestataires d'assurance, et le management.

**2110. A1** – L'audit interne doit évaluer la conception, la mise en œuvre et l'efficacité des objectifs, des programmes et des activités de l'organisation liés à l'éthique.

**2110. A2** – L'audit interne doit évaluer si la gouvernance des systèmes d'information de l'organisation soutient la stratégie et les objectifs de l'organisation

### IV. Conduite d'une mission d'audit RH, cas d'une entreprise publique tunisienne

L'audit des ressources humaines constitue un processus complet de vérification objective et systématique des pratiques, de la documentation, des politiques et des procédures en vigueur dans le système des ressources humaines de l'entreprise.

Un audit RH efficace aide à comprendre la nécessité de développer et d'élargir la fonction des ressources humaines. Il guide également le système pour maintenir la conformité aux règles et règlements en constante évolution. Contribuant ainsi à analyser l'écart entre "quelle est la fonction des ressources humaines existantes ?" et "ce qui devrait être mieux pour la fonction des ressources humaines de l'organisation".

Pour bien mener une mission d'audit RH, il est essentiel tout d'abord que la haute direction établisse clairement les modalités et la portée de l'audit avant que la cellule d'audit interne ou le cabinet d'audit externe commence son boulot.

Une mission d'audit interne se déroule en trois phases : Préparation, Evaluation ou terrain, restitution. Le suivi du plan d'action complète l'ensemble.

Chaque mission d'audit fait l'objet d'une planification, qui prévoit la durée de chaque grande phase et les principales échéances à respecter (réunion d'ouverture, réunion de clôture, rédaction du rapport provisoire, phase contradictoire, rapport définitif...).



Les trois premières étapes comprennent une vaste gamme de quantité, ainsi que des informations qualitatives. La méthode de collecte d'informations dépend de la taille du public cible, de la disponibilité du temps et du type de données à collecter.



## Préparation

La première phase, la phase de collecte d'informations avant l'audit, comprend l'examen des politiques de l'Organisation, des manuels des ressources humaines, des manuels des employés,

des rapports et autres, qui constituent la base du travail de l'organisation.

Dans ce cadre, le personnel des entreprises publiques en Tunisie est réglementé par la loi n° 85-78 du 5 août 1985, portant statut général des offices, des établissements publics à caractère industriel et commercial et des sociétés dont le capital appartient directement et entièrement à l'Etat ou aux collectivités publiques locales, telle que modifiée et complétée par la loi n° 99-28 du 3 avril 1999 et la loi n° 2003-21 du 17 mars 2003 et la loi n° 2006-58 du 28 juillet 2006 et la loi n° 2007-69 du 27 décembre 2007, relative à l'initiative économique. Les dispositions spécifiques à chaque entreprise publique sont réglementées par un statut particulier approuvé par un décret. C'est à base de ce statut particulier que nous avons tracé ces tableaux, très utiles pour collecter des données statistiques concernant la gestion RH au sein d'une entreprise publique.

### Données générales

Nombre total du personnel	N-5	...	N	N+1
<b>Nombre du personnel selon le type de recrutement</b>				
Concours				
Recrutement direct				
Détachement				
Intégration				
<b>Nombre du personnel par Situation juridique</b>				
Titulaire				
Stagiaire				
Contractuel				
<b>Nombre de personnel par Situation Administrative</b>				
Actif				
Détaché				
Inactif				
Sous les drapeaux				
<b>Nombre de personnel par Fonction</b>				

Directeur général				
Directeur				
Sous-directeur				
Chef de service				
<b>Nombre de personnel par Filière</b>				
Personnel d'exécution (Catégories 1-6)				
Personnel de direction (Catégorie 7-13)				
Les cadres (Catégories 14-16)				
<b>Nombre de personnel par Catégorie</b>				
1				
2....				
16				
<b>Nombre de personnel par Echelon</b>				
1				
2....				
25				

- **Recrutement**

\* Par les concours, règle général à adopter

Concours	N°	Date d'ouverture des candidatures	Type de concours		Date de clôture	Nombre des candidats	Candidats retenus
			Ecrit (+/-) Oral	Dossiers			

\* Par Recrutement direct, cas spécifiques

Employé	Matricule	Poste occupé	Date de recrutement

- **Situations administratives**

\* **Détachement**

- D'un établissement public vers l'entreprise

Employé	Matricule	Poste occupé	Date de Détachement	Date de fin de détachement	Corps d'origine

- De l'entreprise vers un autre établissement public

Employé	Matricule	Poste occupé	Date de Détachement	Date de fin de détachement	Corps De détachement

\*Contrat

Employé	Matricule	Poste occupé	Date de Début contrat	Durée de contrat

▪ Prêts

Employé	Matricule	Montant Prêt	Type Prêt	Durée de contrat	Code Prêt	Date de début	Date de fin

▪ Missions à l'étranger

Employé	Matricule	Objet de la Mission	Date de Mission	Nombre de participant	Durée de la Mission

### La phase d'évaluation ou phase « terrain »

La deuxième étape est la présentation sur le site et comprend des questionnaires, des entrevues, des observations, des discussions informelles et des sondages ou un lien entre ces méthodes pour obtenir les contributions nécessaires des membres de l'organisation.

### Restitution des résultats

La phase d'examen nécessite une enquête détaillée sur les dossiers RH existants, les dossiers du personnel, l'absence des employés, le renouvellement des statistiques, les notifications, les demandes d'indemnisation et l'évaluation des performances.

## Conclusion

Le baromètre 2016 de la gouvernance RH dans les grandes entreprises françaises, menée conjointement par les cabinets Deloitte et Misceo, revient sur les grandes thématiques liées à la gouvernance des ressources humaines. A travers des données chiffrées, des analyses, des points de vue et les témoignages de DRH de grands groupes français, cette édition dresse un panorama complet de la gouvernance RH en 2016 et propose des pistes d'amélioration pour une gouvernance plus efficace. Parmi les principales observations de ce baromètre, on cite:

Les conseils d'administration positionnent la gestion des talents et le développement du leadership aux deux premiers rangs de leurs priorités.

Dans la grande majorité des entreprises participantes, le Comex est une instance où l'on parle régulièrement et avec beaucoup d'intérêt des thématiques RH.

Pour 59% des entreprises participantes, la fonction RH est organisée par métier plutôt que par zone géographique.

Les politiques en matière de hauts potentiels, de talent et leadership sont couramment harmonisées et appliquées à l'identique dans tous les pays d'implantation.

La part des organisations qui intègrent la performance RH dans leur tableau de bord peine à augmenter depuis 2010.

Partenaire officiel dans le processus de gouvernance de son entreprise, l'audit interne joue un rôle de catalyseur dans la conduite des changements dans l'entreprise à travers un audit RH efficace, soutenu par le conseil et la Haute direction.

### Référence :

Guide d'audit des ressources humaines, Comité d'harmonisation de l'audit interne, France, 2015

Le contrôle interne et la gestion des risques pour renforcer la gouvernance en Tunisie, OCDE, 2016

---

Pour plus d'information, n'hésitez pas à contacter l'auteur : [benali.marwen@gmail.com](mailto:benali.marwen@gmail.com)

## محادثة مع السيد:



وليد بوزويته

CISA, COBIT5, ITIL, ISO31000

رئيس المعهد التونسي للحوكمة والتدقيق والسلامة المعلوماتية

ISACA Tunis Chapter

الموقع الإلكتروني: [www.isaca-tunisie.org](http://www.isaca-tunisie.org)



ما هي الشهادات التي تقدمها ISACA Tunis Chapter؟ وما هي

نسب الاقبال عليها؟

إيساكا منظمة عالمية رائدة في مجال توفير المعرفة والشهادات والمجتمع والدفاع والتتقيف في مجال ضمان وتأمين نظم المعلومات وضمان الأمن وحوكمة تكنولوجيا المعلومات والمخاطر وقضايا الامتثال الخاصة بها.

ISACA Tunis Chapter لا تقدم شهادات بطريقة مباشرة بل هي

تساعد على الحصول عليها، إيساكا العالمية ISACA

International تشرف على إصدار وإدارة شهادات :

أولا، مرحبا بك سيدي الكريم بيننا

لو تعطينا فكرة عامة عن المعهد التونسي للحوكمة و التدقيق

والسلامة المعلوماتية (تاريخ التأسيس، عدد المنخرطين،...)

قمنا خلال سنة 2007 بمحاولة أولى لإحضار إيساكا إلى تونس،

المحاولة لم تكل بالنجاح و لكن بالمثابرة و العمل الجاد توصلنا

لتأسيس المعهد التونسي للحوكمة و التدقيق و السلامة المعلوماتية في

نهاية سنة 2013 إثر الحصول على الموافقة من جمعية إيساكا

العالمية و هكذا صارت جمعيتنا ISACA Tunis Chapter ممثل

إيساكا في تونس.

2002، حصل أكثر من 30 ألف من المهنيين في جميع أنحاء العالم على CISM الرائدة في الصناعة لتأكيد كلاً من المستوى العالي من الكفاءة الفنية والمؤهلات لأدوار القيادة والإدارة العليا من العيار الثقيل.

**CRISC: Certified in Risk and Information Systems**

**Control** الهامدة الخاصة بالتحكم في المخاطر ونظم المعلومات

شهادة CRISC تمكن من التحقق من صحة المهارات والخبرات في السيطرة على المخاطر ونظم المعلومات. إنها تثبت القدرة على فهم مخاطر العمل وتوضيحها وتنفيذ ضوابط مناسبة ووضع خطط فعالة للتخفيف من المخاطر.

**COBIT5**

COBIT5 هو إطار العمل الوحيد للحوكمة وإدارة تكنولوجيا المعلومات خاصة و المعلومات عامة.

يتضمن برنامج COBIT 5 أحدث الأفكار في تقنيات إدارة الشركات والحوكمة، ويوفر المبادئ والممارسات والأدوات التحليلية والنماذج المقبولة عالمياً للمساعدة في زيادة الثقة في أنظمة المعلومات وقيمتها.

يدمج برنامج COBIT 5 أطر و معايير و موارد رئيسية، بما في ذلك

تقنية المعلومات والاتصالات (Val IT) ومخاطر تكنولوجيا

المعلومات، ومكتبة البنية التحتية لتكنولوجيا المعلومات (ITIL®)

و PMP، TOGAF، PRINCE2، والمعايير ذات الصلة من المنظمة

الدولية للتوحيد القياسي (ISO) .

**CISA : Certified Information Systems Auditor** مدقق نظم

**معلومات معتمد:** هي شهادة مهنية للمتخصصين في تدقيق نظم المعلومات. وهي المعيار العالمي للمتخصصين في تدقيق ومراقبة وتأمين نظم المعلومات منذ سنة 1978. CISA معتمدة من المعهد الأمريكي الوطني للمعايير ANSI. CISA رمزاً عالمياً للإنجاز، الكفاءة، الاحترافية والمعرفة في مجال تدقيق وضبط نظم المعلومات و هي معيار متعارف عليه بين أهل المهنة على مستوى العالم.

**CGEIT: Certified in Governance of Enterprise IT**

**معتمد في حوكمة نظم المعلومات في المؤسسات:** تضمن شهادة CGEIT التي تركز على الإدارة أن الحائزين قادرين على جلب حوكمة تقنية المعلومات إلى مؤسسة، ويمكنهم فهم الموضوع المعقد بشكل شامل، وتعزيز القيمة التي تحصل عليها الشركة من تقنية المعلومات. منذ إنشائها في عام 2007، اكتسب الآلاف من المهنيين في جميع أنحاء العالم تسمية CGEIT الرائدة في الصناعة كوسيلة لتأكيد أن لديهم معرفة واسعة وخبرة واسعة النطاق اللازمة لدعم وتعزيز حوكمة تقنية المعلومات للمؤسسة وضمان تتوافق أنظمة تكنولوجيا المعلومات والأعمال الخاصة بها مع الفعالية والكفاءة المثلى.

**CISM : Cerified Information Security Manager** مدير

**أمن معلومات معتمد** شهادة فريدة تركز على الإدارة وتعزز ممارسات الأمان الدولية وتعترف بالفرد الذي يدير ويصمم ويشرف على أمان معلومات المؤسسة.

شهادة CISM هي معيار الإنجاز المقبولة عالمياً في هذا المجال. تضمن شهادة CISM للحائزين فهم الأعمال التجارية، ومعرفة كيفية إدارة وتكييف التكنولوجيا لمؤسساتهم وصناعاتهم. منذ إنشائه في عام

**CSX: Cyber Security Nexus**

تساعد الشهادة الأفراد على إظهار مهاراتهم وإثبات معرفتهم لمعايير الأمن السيبراني الحالية، وتوفر لأرباب العمل الثقة بأن موظفيهم يحققون المهام المطلوبة وهي تنقسم إلى مستويين:

Cybersecurity Fundamental : يوفر البرنامج، باعتباره نقطة

الدخول إلى برنامج الأمن السيبراني، شهادة قائمة على المعرفة في المفاهيم التمهيديّة التي تحدد وتعرض المعايير والمبادئ التوجيهية والممارسات في المهنة.

CSX Practitioner : شهادة معتمدة للعاملين في مجال الأمن

السيبراني. تسمح لك هذه الشهادة بالعمل بشكل احترافي كمستجيب أول يكون خبيراً في اتباع الإجراءات المعمول بها، باستخدام عمليات محددة، والعمل في الغالب بمشاكل معروفة في نظام واحد.

هل توجد احصائية بعدد الحاصلين على شهادة مدقق نظم المعلومات

المعتمد **CISA** على المستوى العالمي وعلى مستوى تونس؟

على المستوى العالمي يوجد 78640 حاصل علي اعتماد CISA

في تونس يوجد حاليا 23 مقيم حاصل على الاعتماد. والسبب الأساسي لهذا العدد الضئيل هو مغادرة الحاصلين على CISA إلى أوروبا خلال السنتين التي تتلو الحصول على الاعتماد وحصولهم

على عروض عمل مغرية من شركات التدقيق العالمية.

هل توجد احصائية بنسب النجاح بشهادة CISA في تونس وفي

العالم خلال آخر 5 سنوات؟

معدل النجاح في امتحانات في السنوات الأخيرة في العالم يقارب نسبة 52 % وهو نفس معدل النجاح بتونس.

هل لديكم احصائية بتطور عدد المتقدمين للحصول على الشهادات

نتيجة التطور التكنولوجي الذي يشهده العالم؟

نسبة الإقبال على شهادات إساكا في ارتفاع وخاصة منها كوبيت 5

COBIT5 ويعود ذلك إلى وعي المهنيين بأن تحقيق الأهداف

المؤسسية صار صعب المثل في غياب إطار حوكمة ملائم يربط

الحوكمة بالإدارة ويضبط كيفية التبادلات بينهما.

ماهي وضعية مجال تدقيق وحوكمة نظم المعلومات في تونس؟

بالنسبة للتدقيق في النظم المعلوماتية منظومته في تونس تقادمت

ويستوجب الإسراع في إصلاحها، قانون فيفري 2004 مرّت عليه

حوالي 14 سنة وهو لم يعد يفي بالغرض، وكثيرا من الشركات التي

تقوم بهذا التدقيق القانوني يقع التدقيق في شبكة الكمبيوتر أكثر هو

من التدقيق في النظم المعلوماتية والسيبرانية، أما لعدم توفر الموارد

الماليّة بسبب اللجوء إلى العرض الأرخص أو لانعدام الكفاءات.

أما الحوكمة بجميع أنواعها فهي شبه غائبة في المشهد الاقتصادي

والسياسي الحاليين وهو أمر يدعو حقا للتحوف، إذ لا يمكن الحديث

ماهي وجهة نظركم حول مستقبل مجال تدقيق وحوكمة نظم المعلومات في تونس؟

في الوقت الذي تتوجه فيه المؤسسات إلى مستقبل يعتمد بشكل متزايد على التكنولوجيا، وموجها نحو الابتكار، ومحذوف بالمخاطر، ومستقبل مزعج، أين هو التدقيق الداخلي؟ في كثير من الأحيان، على الرغم من الجهود الجارية لتلبية قائمة الاحتياجات المتزايدة لدى أصحاب المصلحة، يجب التحدث على الجيل القادم من التدقيق الداخلي، وهي وظيفة متناغمة مع تحديات المخاطر الناشئة، والتقنيات، والابتكار، والاضطراب الذي تعاني منه المنظمة نفسها؛ ووظيفة قادرة تماما على المساعدة في خلق طرق جديدة للإمداد القيمة. على التدقيق الداخلي تبني أدوات وتقنيات جديدة وتطوير القدرات للاستجابة لتحديات اليوم. من المهم بنفس القدر أن يقوم التدقيق الداخلي بتطوير رؤية متماسكة لكل من المهنة والوظيفة. هذه الرؤية ضرورية من أجل دفع التغييرات اللازمة وترتيب أولويات المبادرات للوظيفة وللمؤسسة ككل.

في الختام شكرا لكم سيدي على رجابة صدركم.

على استراتيجيات ومبادئ وقيم وأهداف وسياسات ومقاييس وتحسن مستمر بدون إطار حوكمة ينظم كل هذا.

هل المؤسسات التونسية حكومية كانت أو خاصة جاهزة للتوافق مع متطلبات حوكمة المعلومات ومتطلبات COBIT5؟

جميع المؤسسات سواء كانت حكومية أو خاصة هي في حاجة إلى إصلاحات عميقة وإطار COBIT5 يمكن مساعدة هذه المؤسسات لإيجاد حلول لمشاكلها. COBIT5 يحتوي على 37 سلسلة عمليات 5 منها تخص أجهزة الحوكمة و 32 تخص أجهزة الإدارة و هو يغطي كامل المؤسسة و ليس النظم المعلوماتية فحسب.

COBIT5 يأتي بحلول لمشاكل المؤسسات التي هي تقوم باعتماده وتكيفه حسب حاجياتها.

ماهي أهم الصعوبات التي تواجه المدقق في نظم المعلومات في تونس؟

تقريبا هي نفسها التي يواجهها المدقق الداخلي. غياب السياسات المكتوبة، العدد الكبير من الاستثناءات و بطئ تنفيذ التوصيات.



## الحوكمة المؤسسية والتدقيق الداخلي

بقلم السيد مروان بنعلي، مراقب المالية/مدقق حكومي، هيئة الرقابة العامة للمالية التونسية

مثل مفهوم الحوكمة المؤسسية **Corporate Governance** إحدى أهم النظريات التي استحوذت على اهتمام الأكاديميين والممارسين والمنظمات المهنية والشركات حكومية كانت أو خاصة.

أتناول في هذا المقال ثلاث محاور مهمة حسب رأيي ستساعد القراء على فهم نظرية الحوكمة المؤسسية وأهدافها وعلاقتها بالتدقيق الداخلي:

### 1. ماذا يقصد بالحوكمة المؤسسية؟



تعددت تعريفات الحوكمة المؤسسية ومن أهمها نذكر:

- "النظام الذي يتم من خلاله توجيه الشركات والرقابة عليها"، تقرير كادبوري (CADBURY) "الأبعاد المالية لحوكمة المؤسسات THE FINANCIAL ASPECTS OF CORPORATE GOVERNANCE"، 1992.
- "نظام يتم بواسطته توجيه منظمات الأعمال والرقابة عليها، حيث تحدد هيكل وإطار توزيع الواجبات والمسؤوليات بين

المشاركين في الشركة المساهمة، مثل مجلس الإدارة، والمديرين، وغيرهم من ذوي المصالح. وتضع القواعد والأحكام لاتخاذ القرارات المتعلقة بشؤون الشركة المساهمة، تقرير "مبادئ حوكمة المؤسسات PRINCIPLE OF COOPERATE GOVERNANCE"، منظمة التعاون الاقتصادي والتنمية (OECD)، 1999.

- "مزيج من المسارات والهيكل التي يضعها مجلس الإدارة لإعلام وتوجيه وإدارة ومراقبة أنشطة المنشأة بغية تحقيق أهدافها"، المعايير الدولية للممارسة المهنية للتدقيق الداخلي، معهد المدققين الداخليين العالمي (IIA)، 2017.

ومع تعدد التعريفات، تبرز جليا الأهمية المتزايدة للحوكمة المؤسسية لدى كافة الشركات الخاصة والحكومية كأحد أهم أسس تطويرها والمحافظة على قيمتها بتضافر جهود كافة الجهات الفاعلة في المؤسسة من مجلس إدارة ولجنة تدقيق وإدارة عليا كل من موقعه وذلك من خلال:

- وضع أهداف استراتيجية ومجموعة قيم ومبادئ تكون معلومة لدى كل العاملين بالشركة،
- وضع وتنفيذ سياسات واضحة،
- إرساء نظام رقابة داخلي قوي ومتناسك،
- إدارة وتقييم المخاطر،
- ضمان دور مهم للتدقيق الداخلي والخارجي....

هذا وقد شملت مبادئ الحوكمة المؤسسية كما وردت بتقرير منظمة التعاون الاقتصادي والتنمية (OECD) بالتعاون مع مجموعة العشرين G20 الصادر سنة 2015 بعنوان "المبادئ

ويساعد هذا النشاط في تحقيق أهداف المؤسسة من خلال اتباع أسلوب منهجي منظم لتقييم وتحسين فاعلية عمليات الحوكمة وإدارة المخاطر والرقابة. " هذا الدور الذي يلعبه التدقيق الداخلي في عملية تقييم نظام الحوكمة تم التنصيص عليه صراحة في المعيار 2110 من المعايير الدولية للممارسة المهنية للتدقيق الداخلي الصادرة عن معهد المدققين الداخليين العالمي IIA (نسخة 2017):

### المعيار 2110 - الحوكمة

يجب على نشاط التدقيق الداخلي تقييم مسار الحوكمة في المؤسسة وتقديم التوصيات المناسبة لتحسين أساليب الحوكمة في المنشأة عبر:

- أخذ قرارات استراتيجية وعملية.
  - الإشراف على عمليات إدارة المخاطر والرقابة.
  - تعزيز الأخلاقيات والقيم المناسبة في المنشأة.
  - ضمان فاعلية إدارة الأداء والمساءلة داخل المنشأة.
  - إبلاغ المعلومات حول المخاطر والرقابة الى الجهات المناسبة داخل المنشأة.
  - تنسيق الأنشطة وتبادل المعلومات بين المجلس والمدققين الخارجيين ومقدمي خدمات التأكيد الآخرين والإدارة.
- كما أكدت المعايير الدولية للممارسة المهنية للتدقيق الداخلي (نسخة 2017) على ضرورة استخدام المدققين الداخليين لمعارفهم وخبراتهم وميزاتهم الأخرى، مثل الاستقلالية والموضوعية، في تقييم فعالية الضوابط الأساسية في المؤسسة وذلك بغرض مساعدة الشركة على تحقيق أهدافها:

**المعيار 1220.ت.1** - يجب على المدققين الداخليين أن يبذلوا العناية اللازمة في أعمالهم وذلك بالأخذ بعين الاعتبار العناصر التالية:

- مدى العمل اللازم لتحقيق أهداف المهمة.
- درجة التعقيد أو الأهمية النسبية أو أهمية المسائل التي يتم تطبيق إجراءات التظمين عليها.

الجديدة الخاصة بحوكمة الشركات G20-OECD Corporate Governance Principles " خمسة مجالات وهي:

- ضمان وجود إطار عام وفعال لحوكمة الشركات.
- الحقوق والمعاملة المتكافئة للمساهمين.
- المؤسسات الاستثمارية وأسواق الأسهم وغيرهم من المؤسسات المالية الوسيطة.
- دور أصحاب المصالح في حوكمة الشركات.
- الإفصاح والشفافية.

### 2. أهميتها والنسبة للشركاء؟

من أهم فوائد تطبيق قواعد الحوكمة المؤسسية بالنسبة للشركات نذكر:

- رفع الكفاءة الاقتصادية للشركة وتعزيز أدائها من خلال الاستخدام الأمثل للموارد وتخفيض التكاليف ووضع الإطار التنظيمي الذي يمكن من خلاله تحديد أهداف الشركة وسبل تحقيقها.
- كسب ثقة المتعاملين مع الشركة من مستثمرين وبنوك تمويلية،
- تعميق الثقة في الاقتصاد والشركات،
- تخفيض المخاطر والحد من الفساد في الشركات من خلال وجود قواعد حسن الإدارة والمحاسبة والإفصاح والشفافية وتعزيز الرقابة والإدارة فيها...

(المصدر: حوكمة الشركات المدرجة في الأسواق المالية العربية، اتحاد هيئات الأوراق المالية العربية، دبي، جويلية 2017).

### 3. العلاقة بين التدقيق الداخلي والحوكمة المؤسسية

تبرز العلاقة بين التدقيق الداخلي والحوكمة المؤسسية وثيقة وقوية من البداية في تعريف التدقيق الداخلي الصادر عن معهد المدققين الداخليين العالمي (IIA): "نشاط مستقل وموضوعي يقدم تأكيدات وخدمات استشارية بهدف إضافة قيمة للمؤسسة وتحسين عملياتها.

**في الختام**، لابد من التأكيد على أهمية التدقيق الداخلي في توعية كافة الأطراف من مجلس إدارة ولجنة تدقيق وإدارة عليا بالدور المحوري للحوكمة في تحقيق أهداف الشركة والمحافظة على ديمومتها وكسب ثقة كافة منظورها من خلال تقديم النصح والإرشاد بالمواضيع ذات العلاقة عن طريق المهام الاستشارية التي يقدمها أو عقد اجتماعات توعوية دورية أو تقديم دورات تدريبية للأعوان في مجال الحوكمة.

- ملاءمة وفعالية مسار الحوكمة وإدارة المخاطر والرقابة.
- احتمال حدوث أخطاء جسيمة أو الاحتيال أو عدم الامتثال.

- تكلفة أعمال التطمين مقارنة بالمنافع الكامنة.

إلا أن هذا التقييم لا يكون فعالا وعمليا والا إذا تم دعمه من نظام حوكمة قوي من أهم قواعده إرساء بيئة رقابية سليمة، ولجنة مستقلة للتدقيق منبثقة عن مجلس الإدارة وتدقيق داخلي أكثر موضوعية واستقلالية مرتبط هيكليا وإداريا بالإدارة العليا وعمليا بمجلس الإدارة ولجنة التدقيق. فكلما كان نظام الحوكمة بالمؤسسة قويا وفعالاً كلما كان التدقيق الداخلي فعالاً وذا قيمة مضافة للشركة. ويبدو دور الحوكمة في تعزيز دور التدقيق الداخلي منطقيا ومشروعا حيث أن عملية البناء في أي شركة تنطلق من وضع الرؤى المستقبلية والخطط الاستراتيجية للمؤسسة لتصل الى إرساء الهياكل التي ستقوم بتنفيذ هذه التوجهات.



للتواصل مع الكاتب: [benali.marwen@gmail.com](mailto:benali.marwen@gmail.com)

## حوكمة تكنولوجيا المعلومات ونشاط المراجعة الداخلية

بقلم الدكتورة ميرفت حسين السيد CCO، CIA، مدير تدقيق داخلي بقطاع سوق المال، مصر

### مقدمة

فقد أصبحت تكنولوجيا المعلومات أحد الركائز الأساسية اللازمة لتطور واستمرارية أعمال المؤسسات بمختلف أنواعها وأنشطتها (خدمية أو مالية أو صناعية)، وسواء أكانت تعمل بالقطاع خاصة أو في القطاع العام، من خلال البيانات والمعلومات التي تنتجها هذه النظم والتي تعتبر ضرورية لتنفيذ الأنشطة أو الخدمات التي تقدمها هذه المؤسسات، بغض النظر عن موقع أو حجم أو طبيعة هذا النشاط. لذا فإن أي تلف أو فقد لأمن البيانات يمكن أن يكون له تأثير مدمر على تلك المؤسسات بالمقارنة من الفوائد التي تنتجها هذه النظم التقنية.

في حين نجد ان هذه النظم التكنولوجية والتقنية قد أظهرت أنواع جديدة من المخاطر التي ينبغي أن يتم إدارتها على نحو كاف لتحقيق الأهداف المرجوة منها.

لذا فقد قدمت المنظمات والمعاهد الدولية لإدارة المخاطر والحوكمة مجموعة من القواعد والتوصيات والضوابط الرقابية التي تهدف لحوكمة تكنولوجيا المعلومات التقنية والوقاية من التهديدات الأمنية المتعلقة بهذه التقنيات والتي يجب أن تلتزم بها المؤسسات حتى تضمن إدارة المخاطر المتعلقة بها، وبما يضمن حماية أصول وموارد المؤسسة والعمل على تحقيق الأهداف الاستراتيجية التي تسعى إليها.

في ظل التطور التكنولوجي العالمي والتزايد المستمر لغالبية المؤسسات المالية في الاعتماد على تشغيل كم هائل من البيانات والمعلومات في عملياتها التشغيلية سواء أكانت مؤسسات مالية أو خدمية أو إنتاجية، بما أدى إلى تحول هذه المؤسسات إلى تطبيق النظم الإلكترونية والتقنية في عملياتها التشغيلية لما تمتاز به هذه النظم عن النظم التقليدية في قدرتها على استقبال وتشغيل ومعالجة الكم الهائل من البيانات في أوقات قياسية، وإمكانية تخزينها وإعادة تشغيلها بصور مختلفة للحصول على نتائج وبدائل تختلف باختلاف الكيفية والهدف المعد من أجلها.

لذا يعمل أعضاء مجالس الإدارات والمديرون التنفيذيون بالمؤسسات المالية على تشغيل وتحليل المعلومات التكنولوجية والحفاظ على دقة وسلامة استخدام هذه المعلومات من بدء تشغيلها وحتى التخلص منها بشكل آمن، ليس فقط لتحقيق قيمة مضافة للمؤسسة وإنما في تحقيق العديد من الأهداف ومنها:

- الحصول على معلومات دقيقة وجودة عالية تساعدهم في دعم اتخاذ القرارات.
- توجيه وتوظيف الاستثمارات التكنولوجية في تحقيق التميز في فعالية استخدام المعلومات التقنية وبما يعمل على تحقيق الأهداف الاستراتيجية للمؤسسة.
- الحفاظ على إدارة المخاطر المتعلقة بتقنية المعلومات بشكل جيد وعند مستوى مقبول للمخاطر.
- العمل على تحقيق التوافق والامتثال مع التشريعات والقوانين والاتفاقيات التعاقدية الخاضعة لها المؤسسة.



## 1. حوكمة تكنولوجيا المعلومات IT Governance



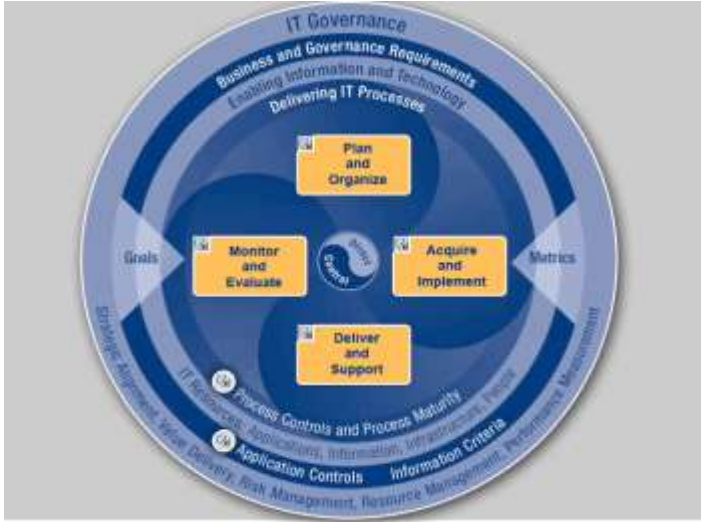
حوكمة تكنولوجيا المعلومات ITG هي جزء لا يتجزء من حوكمة الشركات، والتي تتضمن مجموعة من المسؤوليات والعمليات التي يمارسها مجلس الإدارة والإدارة التنفيذية بهدف حماية أصول وموارد المؤسسة والتحقق من كفاءة استخدامها، من خلال وضع مجموعة من الضوابط الرقابية التي تعمل على إدارة المخاطر الناتجة من استخدام تكنولوجيا المعلومات لضمان أمن وحماية هذه المعلومات، والعمل على تحقيق الأهداف الاستراتيجية للمؤسسة والحفاظ على استمراريته والعمل على التوسع في نطاق أعمالها.

بدأ الاهتمام العالمي باصدار قوانين لحماية البيانات وإدارة المخاطر بعد الانتهاكات والمخالفات المالية التي قامت بها بعض الشركات العالمية (Enron, WorldCom, Tyco, and other corporations) خلال الفترة من 2001 وحتى 2003 والاختراقات الامنية في عام 2004، ومن هذه القوانين قانون ساربانيس-أوكسلي (SOX)، وقوانين حماية البيانات الدولية، وقانون باتريوت بالولايات المتحدة الأمريكية (USAPA)، فقد أحدثت هذه القوانين والقواعد الجديدة تغيرات بمفهوم إدارة المخاطر، ومجال مراجعة تكنولوجيا المعلومات وتحولها من متطلبات ثانوية إلى متطلبات أساسية يتم الالتزام بها في إدارة مخاطر المؤسسة وحماية البيانات والمعلومات والوثائق الصادرة عنها للتأكيد على صحة وموثوقية البيانات

والمعلومات المالية وغير المالية الصادرة من المؤسسة. وقد خصص قانون ساربانيس-أوكسلي (SOX) قسم خاص لمراجعة نظم المعلومات التكنولوجية وأمن وموثوقية المعلومات الصادرة عن تلك النظم وقد تم الانتهاء من هذا الجزء يونيو 2003. وقام معهد المراجعين الداخليين في مايو 2004 بمناقشة دورالمراجعة الداخلية في أمن وحماية تكنولوجيا المعلومات تقصليا وفقا لقانون ساربانيس-أوكسلي (SOX)، وقدمت أيضا لجنة COSO تعديلات على الإطار العام للضوابط الداخلية للمؤسسات المالية للتوافق مع التعديلات والمتطلبات القانونية الجديدة التي وردت بقانون ساربانيس-أوكسلي (SOX)، بهدف تحسين التقارير المالية وتأمين وحماية نظم تكنولوجيا المعلومات وقواعد البيانات ومنع الغش والفساد. كما قدمت جمعية ضبط وتدقيق نظم المعلومات ISACA اطار عمل متكامل لحوكمة تكنولوجيا المعلومات المؤسسية COBIT والذي تم اصداره في ديسمبر 2005، وتم تعديله في مايو 2007 وفقا لاصدار COBIT 4, 4.1، وقد تصميمه بهدف تحديد وثوثيق وتقييم نظم الرقابة على تكنولوجيا المعلومات اللازمة للامتثال مع قانون ساربانيس-أوكسلي (SOX) بالاضافة الى تغطية الجوانب تقصليا التي لم تغطيها اطار الضوابط الداخلية الذي أصدرتها لجنة COSO.

## 2. الأهداف الرقابية على تكنولوجيا المعلومات COBIT

وتعتبر الأهداف الرقابية على تكنولوجيا المعلومات COBIT بمثابة ترجمة للضوابط الرقابية التي أصدرتها لجنة COSO ولكن من الناحية التقنية لنظم المعلومات والوسائل التكنولوجية المرتبطة بها والتي أصدرها معهد ادارة تكنولوجيا المعلومات (ITGI). في تقرير "الأهداف الرقابية لتكنولوجيا المعلومات وفقا لقانون ساربانيس-أوكسلي (SOX)" بهدف التأكيد على وجود ضوابط رقابية فعالة على التقارير والبيانات المالية التي تصدرها المؤسسة.



### الأطر الرقابية لنموذج COBIT4.1

وتتضمن الاطر الرقابية لنموذج COBIT4.1 المكونات التالية:

1. إطار عمل: لتنظيم الأهداف الرقابية لحوكمة تكنولوجيا المعلومات وتقديم أفضل الممارسات في مجال العمليات التكنولوجية بما يتلاءم مع متطلبات العمل.
2. وصف العمليات التكنولوجية: ويعتبر بمثابة نموذج مرجعي يتم اعداده بلغة مشتركة واضحة تتناسب مع جميع أفراد المنظمة، والتي تتضمن وصف شامل للعمليات التكنولوجية داخل المؤسسة وتشمل (التخطيط- وبناء دورات تكنولوجيا المعلومات- التشغيل - وكيفية الرقابة على هذه العمليات).
3. الأهداف الرقابية: وتشمل قائمة بكافة المتطلبات التي حددتها الادارة للرقابة الفعالة على تكنولوجيا المعلومات.
4. نماذج النضج **Maturity Models**: وتشمل القدرة على الوصول داخل كل عملية عند معالجة الفجوات الناتجة أثناء تشغيل العمليات.

وقد تم تصميم الضوابط الرقابية لإطار عمل COBIT لدعم ثلاث مستويات ادارية:

1. الادارة التنفيذية ومجلس الادارة
2. الادارة التنفيذية وتكنولوجيا المعلومات.
3. مسؤولي الحوكمة والتأكيد والرقابة والأمن

واهتم اطار COBIT 4.1 بالربط بين أهداف المؤسسة والبنية التحتية لتكنولوجيا المعلومات من خلال تقديم مجموعة من النماذج المختلفة maturity models and metrics والتي تقيس مستوى الانجاز في تحقيق أهداف المؤسسة من خلال تحديد المسؤوليات المرتبطة بعمليات تكنولوجيا المعلومات، وتنقسم هذه النماذج الى أربعة مجالات محددة هي:

1. التخطيط والتنظيم Planning & Organization
  2. التسليم والدعم لتكنولوجيا المعلومات Delivering and Support
  3. أقتناء وتشغيل النظم التكنولوجية النظم & Acquiring Implementation
  4. المتابعة والتقييم Monitoring & Evaluate
- ويعتبر إطار كوبيت COBIT4.1 من أهم الأطر الرقابية التي تسعى المؤسسات لتطبيقها، وقد تم الاعتراف بها من المعايير الدولية المختلفة بما في ذلك CMMI، ITIL ، TOGAF ، PMBOK، TOGAF، PRINCE2، COSO و ISO 2700.

ويعمل إطار COBIT على دمج جميع الضوابط الرقابية لتكنولوجيا المعلومات تحت مظلة واحدة.

# COBIT®

## AN ISACA® FRAMEWORK

### المبادئ الرئيسية الرقابية لنموذج كوبيت 5 COBIT

ويقدم نموذج كوبيت 5 إطارا شاملا لحوكمة تقنية المعلومات من خلال الاستفادة من الإصدارات السابقة لإطار COBIT مع دمج النماذج الرقابية السابقة بالإصدار الرقابي الجديد وقد تم بناء نموذج COBIT على خمس مبادئ أساسية هي:

1. تلبية احتياجات أصحاب المصلحة Meeting Stakeholder needs
2. تغطية المؤسسة من بدايتها لنهايتها Covering the enterprise end to end
3. تطبيق إطار عمل واحد متكامل Applying a single integrated framework
4. تمكين أسلوب شمولي Enabling a Holistic Approach
5. فصل الحوكمة عن الإدارة Separating Governance from management



وفي إبريل 2012 تم إصدار أحدث إصدار من إصدارات الأطر الرقابية COBIT 5، والذي عزز مبادئ COBIT 4.1 وادماجها مع أطر مخاطر تكنولوجيا المعلومات وأطر قيمة تكنولوجيا المعلومات. والذي قد تم أعداده وفقا لكل من إطار ضمان تكنولوجيا المعلومات (ITAF)، (ISACA). وذلك بهدف إيجاد نموذج لأمن المعلومات التكنولوجية للمؤسسة.



### الإطار الرقابي COBIT 5:

يقدم نموذج COBIT 5 إطارا رقابيا شاملا يساعد المؤسسة في تحقيق أقصى استفادة من نظم تكنولوجيا المعلومات مع الحفاظ على التوازن بين تحقيق الفوائد وتحسين مستوى المخاطر والاستخدام الأمثل للموارد المتاحة لنظم المعلومات، من خلال دعم نظام شامل لحوكمة تكنولوجيا المعلومات على مستوى المؤسسة بأكملها ومع الأخذ في الاعتبار كافة المستخدمين للنظم المعلوماتية للمؤسسة داخليا وخارجيا.

ويعتمد نموذج COBIT 5 على الإصدارات السابقة للنظم الرقابية COBIT 4.1, Val IT, Risk IT والتي تتضمن وضع وتعزيز نظام لحوكمة المؤسسة

الدور الذي تقوم به ادارة المراجعة الداخلية في أمن وحماية تكنولوجيا المعلومات وفقا لقانون ساريانيس-أوكسلي (SOX)، والتعديلات على الاطار العام للضوابط الداخلية للمؤسسات المالية التي أدرتها لجنة COSO للتوافق مع التعديلات والمتطلبات القانونية الجديدة ، قام معهد المراجعين الداخليين (IIA) في مايو 2004 بمناقشة هذه التعديلات بهدف تحسين التقارير المالية وتأمين وحماية نظم تكنولوجيا المعلومات وقواعد البيانات ومنع الغش والفساد.


وفي مارس 2005 قام معهد المراجعين الداخليين (IIA) بتقديم أول دليل للمراجعة الداخلية على تكنولوجيا المعلومات GTAG I، بهدف تقديم دليل ارشادي لادارة التدقيق يمكنها من تفهم المتطلبات الرقابية العامة للقيام بمراجعة تكنولوجيا المعلومات، ومواكبة التطورات والتحديات العالمية التي تتم بتكنولوجيا المعلومات والنظم المتعلقة بها، وبالإضافة الى ذلك قام معهد المراجعين الداخليين (IIA) بتقديم عدة اصدارات تالية لتتناسب مع تلك التطورات التكنولوجية والتي تهدف في مجملها كيفية مساعدة المدقق الداخلي في تحقيقه أهدافه الرقابية على الجوانب التكنولوجية المختلفة التي تواجهه بالمؤسسة سواء تم تطبيقها فعلا أو سيتم العمل بها وفقا للخطط الاستراتيجية للمؤسسة، وبما يتواءم مع التطورات التكنولوجية العالمية .

### 3. الدليل العالمي للمراجعة التكنولوجية Global technology Audit Guide (GTAG)



بزيادة الاهتمام العالمي بتكنولوجيا المعلومات والتغيرات بمفهوم ادارة المخاطر، وتحولها إلى متطلبات أساسية يتم الالتزام بها لادارة مخاطر المؤسسة وحماية البيانات والمعلومات والوثائق الصادرة عنها، وزيادة

ويوضح الجدول التالي الأدلة المختلفة GTAG التي تم اصدارها حتى الآن، والأهداف الرقابية التي يحققها كل منهم حتى يتسنى للمدقق الداخلي الاسترشاد باي منها وفقا للهدف الرقابي الذي يهدف لتحقيقه:

<p>الضوابط الرقابية لتكنولوجيا المعلومات IT</p> 	<p>GTAG-1: IT Controls (Published in Mar 2005) 2<sup>nd</sup> EDITION MARCH</p> <p>وتهدف الى فهم المخاطر والضوابط الرقابية المتعلقة بتكنولوجيا المعلومات وتحديد الأدوار والمسئوليات التنظيمية المتعلقة بالرقابة على تكنولوجيا المعلومات ومتابعة وتقييم المخاطر المتعلقة بها</p>
<p>التغيير وادارة الدفعات</p> 	<p>GTAG-2: Change and Patch Management (Published in June 2005) 2<sup>nd</sup> EDITION MARCH 2012</p> <p>وتهدف إلى ادارة تغيير تكنولوجيا المعلومات والتعرف على أسباب التغيير والتحقق من مدى كفاية الضوابط الرقابية المتعلقة بعملية التغيير والأثر المحتمل على أهداف العمل لضمان التغيير الآمن لتكنولوجيا المعلومات وضمان صحة المعلومات الصادرة عنها حتى اتمام التغيير وتحقيق الأهداف المرجوة من عملية التغيير.</p>



<p>المراجعة المستمرة</p> 	<p>GTAG-3: Continuous Auditing (Published in Oct 2005) 2<sup>nd</sup> EDITION January 2013 وتهدف الى قيام ادارة التدقيق بمهمة التدقيق المستمر لبعض العمليات ذات الطبيعة الخاصة والتي تتطلب القيام باجراءات تدقيق مستمرة لبعض البيانات او العمليات الهامة للتحقق من ادارة المخاطر المتعلقة بها بشكل جيد بما الاختيار يضمن تنفيذها بشكل صحيح.</p>
<p>ادارة التدقيق على نظم المعلومات</p> 	<p>GTAG-4: Management of IT Auditing (Published in Mar 2006) 2<sup>nd</sup> EDITION January 2013 ) يهدف إلى تقديم دليل يساعد ادارة التدقيق الداخلي في القيام بمهام مراجعة نظم المعلومات، وبما يساعد الرئيس التنفيذي للتدقيق في تقديم مهمة التدقيق المتعلقة بنظم المعلومات من خلال التركيز على ثلاث اجزاء رئيسية هي: 1. تقييم الاحتياج لتكنولوجيا المعلومات 2. تقييم المخاطر المرتبطة بتكنولوجيا المعلومات بدقة 3. تنفيذ عملية مراجعة تكنولوجيا المعلومات بفاعلية.</p>
<p>مراجعة المخاطر الخاصة</p> 	<p>GTAG-5: Auditing Privacy Risks (Published in June 2006) 2<sup>nd</sup> EDITION July 2012 الهدف منه هو كيفية التعامل مع المخاطر المتعلقة بأمن وسرية البيانات الخاصة بالمعاملين مع المؤسسة من عملاء ومواردين وعاملين بالشركة وشركاء الأعمال، وكيفية الحفاظ على المعلومات والبيانات الشخصية المتعلقة بتلك الاطراف مع الالتزام بالتعامل على هذه المعلومات بموجب الاتفاقيات التعاقدية؛ والامتثال لقوانين الخصوصية واللوائح وأمن البيانات المعمول بها. وتعتبر الخصوصية قضية عالمية. وقد اعتمدت بلدان عديدة تشريعات الخصوصية التي تنظم استخدام المعلومات الشخصية، فضلا عن تصدير هذه المعلومات عبر الحدود. للشركات للعمل بفعالية في هذه البيئة، مع ظل وجود فهم كافي بكيفية التعامل على هذه البيانات ، مع الامتثال لقوانين الخصوصية.</p>
<p>مراجعة وادارة الهجمات الالكترونية</p> 	<p>GTAG-6: Managing and Auditing IT Vulnerabilities (Published in Oct 2006) deleted January 2013 الهدف من التحقق من فعالية وكفاءة الاجراءات المتبعة في ادارة وتدعيم أمن تكنولوجيا المعلومات وتقييم الاجراءات المتبعة في التعامل مع الاختراقات الغير الامنة لتكنولوجيا المعلومات قد تم الغاء هذا الدليل في عام 2013 مع بعض ادراج المصطلحات المتعلقة به بالاصدار الثاني ل GTAG 4 المصدر في عام 2013</p>
<p>الاستعانة بمصادر خارجية لتكنولوجيا المعلومات</p> 	<p>GTAG-7: Information Technology Outsourcing (Published in Mar 2007) 2<sup>nd</sup> EDITION July 2012 يقدم دليل لكل من الرئيس التنفيذي للمراجعة والادارة في كيفية التعامل مع المعلومات المختلفة التي يمكن الحصول عليها في حالة الاستعانة بمصادر خارجية لتكنولوجيا المعلومات وكل ما يتعلق بالخدمات التي تقدمها هذه الجهة الخارجية من (فترة الانتهاء من الخدمة- كيفية ادارة وتنفيذ العمليات المقدمة من تلك الجهات وفقا لخطط واضحة تتفق مع الاطار العام للالتزام والحوكمة والنظم الرقابية والمخاطر العامة و التي تتعرض لها المؤسسة .</p>
<p>مراجعة النظم الرقابية على التطبيقات</p> 	<p>GTAG-8: Auditing Application Controls (Published in July 2007) يقدم الدليل معلومات عن الضوابط الرقابية المستخدمة في حماية التطبيقات والفوائد المرجوة من تطبيقها وتحديد نطاق تطبيقها وكيفية تقييم المخاطر المتعلقة بها والنظم الرقابية المستخدمة في الرقابة على هذه التطبيقات وكيفية اختبارها وفحصها للتحقق من دقة البيانات المستخدمة بدءا من ادخالها وكيفية تشغيلها واستخراجها وتخزينها بشكل دقيق والتوقيت المناسب.</p>
<p>ادارة تحديد سماحية الوصول للبيانات</p> 	<p>GTAG-9: Identity and Access Management (Published in July 2007) يهدف هذا الدليل الى تقديم مساعدة لمدير التدقيق الداخلي في التعرف على كيفية التحقق من فعالية وكفاءة النظم الرقابية المتبعة في الادارة وتطبيق سياسة تحديد من له الحق في الوصول للبيانات (IAM) وحدود السماحية في استخدام تلك البيانات والفترة الزمنية المسموحة بها في الاطلاع عليها .</p>
<p>ادارة خطة استمرارية النشاط</p> 	<p>GTAG-10: Business Continuity Management (Published in July 2008) (Updated August 2014) يعتبر احد المراجع الهامة التي توضح كيفية التعرف على العناصر الرئيسية بخطة استمرارية النشاط بعد حدوث الكوارث والتي تشير الى ضرورة تحديد العناصر الحرجة بنظم المعلومات التي ينبغي ان تأخذ بالحسبان ، وكذلك الدور الذي يلعبه المدقق الداخلي قبل واثناء حدوث الأزمة والدور الذي يقدمه بعد حدوثها.</p>
<p>اعداد خطة مراجعة نظم المعلومات</p> 	<p>GTAG-11: Developing the IT Audit Plan (Published in July 2008) يهدف هذا الدليل لمساعدة الرئيس التنفيذي للتدقيق الداخلي في فهم بيئة نظم المعلومات داخل المؤسسة والتعرف على كافة أنظمة المعلومات الخاضعة للتدقيق الداخلي وتقييم المخاطر المتعلقة بها ، و التعرف على كيفية اعداد الخطة السنوية لمراجعة نظم المعلومات بالمؤسسة</p>

<p>مراجعة المشروعات التقنية واستلامها</p> 	<p><b>GTAG-12: Auditing IT Projects (Published in March 2009)</b> يساعد CAE's في كيفية متابعة المشروعات والتقنية المتعلقة بتكنولوجيا المعلومات وتقييم المخاطر المتعلقة بها وكيفية فحصها ومتابعتها حتى الانتهاء من تنفيذها وتسليمها</p>
<p>منع واكتشاف الغش بمن خلال لنظم الآلية</p> 	<p><b>GTAG-13: Fraud Detection and Prevention in an Automated World (Published in December 2009)</b> يقدم هذا الدليل كيفية استخدام النظم التكنولوجية في تقديم مجموعة من الأساليب التحليلية التي يمكن استخدامها كأحد أساليب منع او اكتشاف عمليات الغش التي يمكن أن تحدث داخل المؤسسة من خلال تحليل البيانات المتاحة بالشركة ودعمها بمجموعة من البرامج التحليلية التي تسهل تحليل البيانات وتحديد مؤشرات الغش التي يمكن ان تحدث بتلك البيانات</p>
<p>التدقيق على مستخدم التطبيقات</p> 	<p><b>GTAG-14: Auditing User Developed Applications (Published in June 2010)</b> التدقيق على تطوير تطبيقات المستخدم وكيفية التدقيق على الاعمال التي قاموا بتطويرها، والرقابة على التغيرات التي تطرأ عليها، والتحقق من استمرارية وكفاية النظم الرقابية المتعلقة بها قبل وبعد احداث التطويرات عليها وما اذا كانت التطويرات على هذه التطبيقات تتم بموجب النظم الرقابية اللازمة، والتحقق من استمرارية النظم الرقابية على هذه التطبيقات حتى التغيرات العديدة التي قد تطرأ على التطبيقات الاصلية.</p>
<p>حوكمة أمن المعلومات</p> 	<p><b>GTAG-15: Information Security Governance (Published in July 2010)</b> يهدف هذا الدليل لمساعدة CAE's في كيفية ادارة عملية حوكمة أمن المعلومات ضمن خطة التدقيق على أنشطة المؤسسة للتحقق مما اذا كانت المؤسسة تقوم باتباع وتطبيق الممارسات الصحيحة في الحفاظ على أمن البيانات</p>
<p>تكنولوجيا تحليل البيانات</p> 	<p><b>GTAG-16: Data Analysis Technologies (Published in August 2011)</b> يستهدف هذا الدليل مساعدة في CAE's في قيام المؤسسة بعملية تحليل البيانات باستخدام النظم التقنية الحديثة لتحليل البيانات للوصول الى تحليلات افضل ونتائج اكثر فعالية باستخدام النظم التكنولوجية، وذلك لأهمية البيانات للمؤسسة وأهمية الوصول الى التحليلات اللازمة في وقت أسرع نظرا للتزايد الهائل في البيانات المستخدمة بالمؤسسة، وذلك مع الأخذ في الاعتبار المخاطر والتحديات التي قد تواجه المؤسسة عند استخدام تلك التقنيات.</p>
<p>التدقيق على حوكمة نظم المعلومات</p> 	<p><b>GTAG-17: Auditing IT Governance (Published in July 2012 and updated in January 2018)</b> يستهدف هذا الدليل مساعدة ادارة التدقيق في التحقق مما اذا كانت حوكمة تكنولوجيا المعلومات تتوافق مع أهداف واستراتيجيات المؤسسة وتقديم التوصيات اللازمة في حالة عدم توافقها مع هذه الاستراتيجيات والأهداف، وتتولى ادارة التدقيق الداخلي مهمة التحقق من القيام باتباع وتطبيق الممارسات الرشيدة لحكومة تكنولوجيا المعلومات والتحقق من مدى توافر تأكيد عن فعالية نظم الحوكمة المطبقة في تقديم تأكيدات عن نشاط المؤسسة لأصحاب المصالح وأنها تعمل وفقا للأهداف المخططة لها، وقد تم تعديل هذا الدليل خلال عام 2017 حتى يتماشى مع الإطار الدولي والممارسات المهنية للمدقق الداخلي بشكل مباشر.</p>
<p>التدقيق على النظم الذكية</p> 	<p><b>GTAG-18: GTAG 18 - AUDITING SMART DEVICES (Published in August 2016)</b> مع انتشار الأجهزة الذكية ظهرت ضرورة تحديد كيفية ادارة المخاطر المرتبطة باستخدام هذه الأجهزة الذكية أصبح بالغ الأهمية. حيث يمثل أحد التحديات الهامة لـ CAE's في التعرف على احتمالية المخاطر التي قد تتعرض لها المؤسسة من استخدام تلك الأجهزة، وقد تم تقديم هذا الدليل لمساعدة المدققين الداخليين في فهم أفضل لتكنولوجيا الأجهزة الذكية وتحقيق من الحصول على المنافع المرجوة منها عند مستوى أدنى للمخاطر، من خلال فهم هذه الأجهزة والمخاطر المرتبطة بها، والتحقق من ان النظم الرقابية وسياسات الحوكمة المطبقة تعمل بدقة على تخفيف المخاطر المرتبطة بها الى المستوى المطلوب.</p>
<p>تقييم مخاطر الأمن السيبراني</p> 	<p><b>GTAG-19: Assessing Cyber security Risk (Published in September 2016)</b> اصبحت المؤسسات باختلاف انواعها اكثر عرضة لتهديدات الانترنت كنتيجة للتزايد المستمر في الاعتماد على الأجهزة والشبكات التقنية والبرامج والتطبيقات والوسائط الاجتماعية، ونتيجة لهذه المخاطر المتزايدة فيواجه CAE's تحديات كبيرة في ضرورة تطبيق نظم رقابية فعالة تساعده في منع واكتشاف هذه المخاطر، ويقدم هذا الدليل تقييم لمخاطر الأمن السيبراني: الادوار المختلفة لثلاثة خطوط الدفاع بالمؤسسة، مساعدة المدقق الداخلي في توفير القدرة على تقديم تأكيدات عن مخاطر الأمن السيبراني والمخاطر الناشئة عن التهديدات التي تواجه المؤسسة من التواجد في البيئة الالكترونية والاتصال بشبكة الانترنت، كما يناقش الدليل أيضا الدور الذي يقوم به المدقق الداخلي للتعامل مع المخاطر الناشئة من تلك التهديدات وعرض لاسلوب تقييم تلك المخاطر وكيفية الرقابة عليها.</p>
<p>فهم ومراجعة البيانات الكبيرة</p> 	<p><b>GTAG-20: UNDERSTANDING AND AUDITING BIG DATA – FONTE (Published in April 2017)</b> ويقدم هذا الدليل لمحة عامة عن مفاهيم البيانات الكبيرة، لمساعدة المدقق الداخلي في تحديد المكونات المختلفة للبرامج الخاصة بالبيانات الكبيرة بما في ذلك الأهداف الاستراتيجية للمؤسسة، ومعايير النجاح، وعمليات الحوكمة والعمليات التشغيلية والتكنولوجية، كما يقدم الدليل وصف للدور الذي يقوم به المدقق الداخلي تجاه برامج البيانات الكبيرة المستخدمة بالمؤسسة، كما يشمل الدليل اطار المخاطر الرئيسية والتحديات التي تواجه المؤسسة في ذلك المجال، وأمثلة للضوابط الرقابية التي يجب أخذها في الاعتبار عند التخطيط لمراجعة البيانات الكبيرة المستخدمة بالمؤسسة.</p>

أهم المصادر المستخدمة:

<http://isacala.org/doc/ISACALADec2004Issue.pdf>

<https://na.theiia.org/standards-guidance/recommended-guidance/practice-guides/Pages/Practice-Guides.asp>

<https://www.linkedin.com/pulse/governance-importance-auditor-kris-seeburn/>

<http://www.aiiaweb.it/pubblicazione>

[https://www.isaca.org/chapters2/Norway/members/Documents/IIA\\_presentasjon\\_ISACA.pdf](https://www.isaca.org/chapters2/Norway/members/Documents/IIA_presentasjon_ISACA.pdf)

---

للتواصل مع الكاتب: mervat\_cia@yahoo.com

## منظومة التصرف الإلكتروني في التقارير الرقابية

بقلم السيد مروان بنعلي، مراقب المالية/مدقق حكومي، هيئة الرقابة العامة للمالية التونسية

### مقدمة

تتولى هيئة الرقابة العامة للمالية التونسية تحت السلطة المباشرة للوزير المكلف بالمالية إجراء مهمات تفقد ومراقبة مشروعية وجدوى تصرف وحسابات المصالح والهيكل العمومية التالية:

- مختلف المصالح العمومية المركزية والجهوية
- الجماعات المحلية (البلديات والمجالس الجهوية)
- المؤسسات العمومية ذات الصبغة الإدارية والمؤسسات العمومية المماثلة لها
- المؤسسات العمومية غير الإدارية والمنشآت العمومية أو ذات المساهمة العمومية
- الجمعيات
- المجمعات المهنية والتعاضديات والتعاونيات
- الهياكل الأخرى التي تنتفع بصفة مباشرة أو غير مباشرة بمساعدة أو دعم من الدولة أو الجماعات الجهوية أو المحلية كما يمكن تكليف الهيئة بإنجاز مهمات تقويم لنشاط وأداء المصالح والهيكل المذكورة أعلاه وبرامجها ونتائجها المسجلة ومردودها وذلك قصد تحسين طرق تنظيمها وسيرها.

كما تتولى هيئة الرقابة العامة للمالية بصفة حصرية إجراء مهمات تدقيق حسابات المشاريع الممولة بموارد خارجية، لفائدة جل الجهات الممولة (البنك الدولي للإنشاء والتعمير، البنك الإفريقي للتنمية، البنك الياباني للتعاون الدولي، الاتحاد الأوروبي، الصندوق العربي للتنمية الاقتصادية والاجتماعية، صندوق الدول المصدرة للنفط، الصندوق الدولي للتنمية الفلاحية...).

ويتم برمجة مهمات المراقبة بالتنسيق مع الهيئة العليا للرقابة الإدارية والمالية المحدثة منذ سنة 1993 والتابعة لهيكل رئاسة

الجمهورية. كما تتولى الهيئة المذكورة متابعة التوصيات والمقترحات المضمنة صلب التقارير النهائية لمختلف عمليات المراقبة والتفقد التي تحال إليها بصفة آلية.

### I. لماذا وضع تطوير المنظومة الإلكترونية؟

مع التزايد المستمر في حجم تقارير الرقابة الصادرة عن الهيئة إضافة إلى ما تحتوي عليه من مستندات ووثائق كثيرة في شتى المجالات، ورغبة كافة أعضاء الهيئة من مراقبين وإطار إداري في تنظيم البيانات بطريقة آلية، ارتأت إدارة هيئة الرقابة العامة للمالية تطوير منظومة الكترونية داخلية للتصرف في الوثائق والأرشيف تمكن خاصة من تخزين التقارير الرقابية السابقة وتسهيل عملية اطلاع كافة مراقبي الهيئة عليها بكل سهولة وسرعة.

ولتحقيق هذه الأهداف، تم تكليفي ضمن فريق عمل داخلي بتطوير منظومة الكترونية للتصرف في الوثائق والأرشيف تهدف أساسا إلى:

- سهولة تصنيف وترتيب التقارير الرقابية،
- سرعة عمليات البحث،
- سهولة نشر وتوزيع التقارير بين كافة أعضاء الهيئة،
- ضمان حماية التقارير من الاتلاف والضياع والسرقة،
- ربح فضاءات حفظ وتخزين التقارير الرقابية خاصة مع ضيق مساحة مقر الهيئة...

وقد تم استعمال هذه المنظومة في عديد الدول وعديد المنظمات المعروفة دوليا مثل:

- Airbus
- American Stock Exchange
- Federal Aviation Association (FAA)
- Harvard University
- Massachusetts Institute of Technology (MIT)
- UK Defence Academy

### III. مراحل تطوير المنظومة الالكترونية

سيتم تطوير المنظومة على مرحلتين:

- **مرحلة أولى:** تم خلالها تطوير الجزء المخصص لتخزين التقارير الرقابية التي تتم رقمتها في شكل PDF.
- **مرحلة ثانية:** سيتم تطوير الجزء المخصص لمسيرات عمل (Workflow) الخاصة بمكتب ضبط الهيئة (الوارد والصادر) باعتماد عدة معطيات (الرقم، درجة السرية، نوع المراسلة....).

مع العلم فان المنظومة تم تطويرها باللغتين العربية والفرنسية.



وقد تم توسيع الوثائق المخزنة في المنظومة لتشمل كافة أوراق العمل الخاصة بعمليات التدقيق والرقابة ومن أهمها:

- اذن بمهمة
- النصوص القانونية المهمة خاصة المتعلقة بالمشاريع العمومية والمعاهدات مع البنوك الأجنبية
- تعليمات رئيس الهيئة....

### II. الجانب التقني للمنظومة الالكترونية

تم تطوير المنظومة الالكترونية اعتمادا على البرمجية مفتوحة المصدر ألفرسكو ALFRESCO (<https://www.alfresco.com>) المعترف بها عالميا في مجال التصرف الالكتروني في الوثائق. وقد تم الاختيار نظرا لما توفره هذه النظم من امتيازات ومرونة لمستعملها على خلاف البرمجيات الأخرى التي يسميها البعض بالبرمجيات الاحتكارية لشركات معينة:

- مجانية البرمجية،
- إمكانية تحميل وتعديل الكود الأصلي Source code of the program،
- حرية إعادة توزيع البرنامج.
- حرية إنتاج برمجيات مشتقة أو معدلة من البرنامج الأصلي،
- حرية توزيعها تحت نفس الترخيص للبرمجيات الأصلي.
- عدم وجود أي تمييز في البرامج لأي مجموعة أو أشخاص.
- عدم وجود أي تحديد لمجالات استخدام البرنامج...



#### IV. دور المنظومة الإلكترونية في تحسين أداء هيئة الرقابة العامة للمالية

عند استكمال تفعيل المنظومة الإلكترونية، سيكون لهيئة الرقابة العامة للمالية ومراقبيها امكانية:

- تخزين عدد كبير من التقارير الرقابية وأوراق العمل بدون أي صعوبات،
- تخزين جميع صيغ المستندات ( .PDF, .docx, .xls, .pptx,... و الصور والفيديو والFLASH،
- تحويل المستندات إلى أنواع مختلفة مثل تحويل ملف .docx إلى .PDF.

- امكانية حفظ نسخ معدلة من الملفات (Record Management) بمعنى عند تعديل إي ملف فإن البرنامج يحتفظ بالنسخ القديمة وكذلك من قام بالتعديل،
- سرعة البحث عن الملفات ومحتواها بكل سهولة باعتماد تقنية التصفية Filter والترتيب Order حسب عدة معايير مثل سنة التقرير، اسم المراقب، الهيكل التي تمت رقابته.
- إمكانية تخصيص مسيرات عمل (Workflow) وربطها بالمستندات،
- إمكانية فتح الملفات من برامج أوفيس مباشرة بدون استخدام ...Alfresco.

ويبين الرسم التالي تنوع الوظائف التي تقدمها منظومة التصرف الإلكتروني في التقارير الرقابية لهيئة الرقابة العامة للمالية:



كل هذه الإيجابيات تمكن من تحسين أداء المراقبين من خلال تمكينهم من:

- الاستعانة بالتقارير السابقة والنصوص القانونية في أسرع وقت،
- تقليص المدة الزمنية المخصصة لتنفيذ المهمات الرقابية،
- البناء على نتائج المهمات السابقة،
- كسب الخبرة من مقررات رقابية ذات مواضيع متنوعة،
- تبادل التجارب بين المراقبين...الخ

## V. المخاطر المرتبطة بالمنظومة الإلكترونية

## خلاصة

ترتبط المخاطر المرتبطة بالمنظومة الإلكترونية للتصرف في الوثائق بأمن الوثيقة الإلكترونية والحفاظ على هويتها خاصة من الفيروسات والمخاطر السيبرانية خاصة عند ضعف تحديد حقوق العبور للمنظومة وحماية التجهيزات من حواسيب وموزعات.



مكنت منظومة التصرف الإلكتروني في الوثائق والأرشيف مراقبي هيئة الرقابة العامة للمالية التونسية خاصة من:

- حفظ آلي لمقررات الرقابة الصادرة عن الهيئة تسريعا للحصول عليها والاستفادة منها من طرف المراقبين وذلك:
- بتبويبها حسب معايير متفق عليها مسبقا (سنة الإصدار، اسم المراقب، موضوع المهمة...)،
- باستخدام طرق مختلفة للبحث، مع إمكانية وضع أكثر من صيغة بحث.
- حفظ آلي للوثائق الواردة والصادرة على مكتب الضبط.

وهو ما مكن من تحسين أداء المراقبين وهيئة الرقابة العامة للمالية بصفة عامة من خلال منظومة الكترونية للتصرف في الوثائق مبنية على قاعدة بيانات قوية تمكن من حسن مسك مخرجات الهيئة من مقررات رقابية. وتجدر الإشارة الي وجود محاور تطوير مبرمجة للمنظومة أهمها المرتبطة بتدعيم امنها وحقوق العبور اليها. وقد مثلت هذه المنظومة التي تم تطويرها داخليا بهيئة الرقابة العامة للمالية نموذجا تم اعتماده في مرحلة لاحقة بكافة هيكل وزارة المالية والذي يعتبر دليلا على نجاحها.

للتواصل مع الكاتب: [benali.marwen@gmail.com](mailto:benali.marwen@gmail.com)

# لعبة إلكترونية

## تزيد من نسبة معرفة الموظفين

بقلم السيد أحمد سلامة الملاحي، مدقق داخلي لدى هيئة تنظيم النقل البري، الأردن

هل اقوم انا بتصميمها؟

لا اخفيكم ان البرمجة هي من هواياتي المفضلة (نعم، قمت بتصميم عدة برامج قبل ذلك)؟

للأسف انا مصمم برامج سطح المكتب ( Desktop Application) ولم اقم بتصميم صفحات انترنت قبل ذلك (من المعلوم ان تصميم مواقع الانترنت تحتاج إلى معرفة عدة لغات برمجة حيث كان لي معرفة ببرمجة HTML وهي تقوم ببناء الهيكل الاساسي للموقع الالكتروني كما لي بمعرفة برمجة CSS وهي مسؤولة عن الشكل الجمالي للموقع ولي معرفة ايضا ببرمجة JavaScript وهي تجعل موقعك الالكتروني متفاعل ببعض الاوامر). جميع اللغات هذه كنت بحاجة لها.

للعلم هذه اللغات جميعها تسمى في عالم تكنولوجيا المعلومات Front - End اي انها برامج ذات تصميم واجهات رسومية لكن اللعبة بحاجة إلى ادخال معلومات بقاعدة بيانات (نسييت ان اخبركم اني قادر على بناء قواعد بيانات بعدة نظم ادارة قواعد البيانات مثل Microsoft Access , MySQL, SQL Server ) وتحتاج هذه البيانات عند تخزينها ومعالجتها وتحديثها ارسال طلبات إلى الخادم ويجب ان تكون سرية (مشكلة الامان تلاحقني دائما).

خلال عملي كمدقق داخلي في مؤسستي واجراء عدد من المقابلات مع الموظفين للتأكد من سير العمليات تم ملاحظة ضعف إلمام الموظفين بالأنظمة والتعليمات التي تخص الوظيفة كما تم ملاحظة عدد من الموظفين يقومون بالدخول إلى الالعاب الالكترونية عن طريق الانترنت.

تبادر إلى ذهني خلالها ان لا بد من الاستفادة من هذه الالعاب الالكترونية في تنمية الموظفين وفعاليتهم وبعد تفكير تم اقتراح عمل لعبة إلكترونية يتم من خلالها نشر المعرفة بالأنظمة والتعليمات وقليل من الامور الادارية , امور مالية ونبذة عن المؤسسة التي يعملون بها .

لاقت هذه الفكرة الاعجاب من الرئيس التنفيذي للتدقيق الداخلي (نعم، الابداع بحاجة إلى دعم).

ولكن من يقوم بتصميم هذه اللعبة؟

هل قسم تكنولوجيا المعلومات قادر على ذلك؟

نعم انه قادر على ذلك لكن لم تكن ضمن اولوياته فكبر المشاريع التكنولوجية لدى المؤسسة أنك موظفي تكنولوجيا المعلومات وأصبح غير قادر على تحمل المزيد.



صدقا اني لم اقم بتعلم لغة برمجة تقوم لي بهذا الدور مثل لغة ASP.net , PHP , Classic ASP وهي لغات برمجة تقوم ببرمجتها في الخادم تتلقى طلبات (وامر) من متصفح الانترنت ويقوم بتخزين البيانات في قاعدة البيانات و معالجتها وتحديثها كما تسمى في عالم تكنولوجيا المعلومات .Back – End



هيئة تنظيم  
النقل البري  
LAND TRANSPORT REGULATORY COMMISSION

## اهلا وسهلا بكم في لعبة المعرفة



انطلاقا من قناعتنا بأهمية المعرفة وبشربها ونقلها وتعزيزها  
فقد تم العمل على بناء لعبة إلكترونية لتشر وتحفيز  
العاملين لدى الهيئة على زيادة مخزونهم المعرفي بإحدى  
الأساليب وأسهل الطرق .

فما هي المعرفة وكيفية بناء قاعدة معرفية تخدم الموظف  
وتسهل عليه أداء أعماله .

**المعرفة وطرق تعزيزها:**

يمكن تعريف المعرفة بأنها عبارة عن مجموعة من المعلومات المرتبة والمنظمة التي تم تخزينها وتصنيفها  
لتخدم غرض معين .

البيانات << المعلومات >> المعرفة

**انواع المعرفة:**

**المعرفة الصريحة:** وهي المعرفة التي تتعلق بالمعلومات الموجودة والمخزنة في أرشيف المؤسسة

**المعرفة الضمنية:** وهي مجموع الخبرات المتراكمة ، والخرايط العقلية ، ومجموعة المهارات المكتسبة لدى  
أي موظف .

**وهناك بعض الأبعاد المهمة لتعريف المعرفة:**

- الغراء من المصادر المتوفرة .
- تخزين وتنظيم وفهرسة الأعمال المنجزة (توثيق) .
- الاستفادة قدر الامكان من خبرات الزملاء و من المشاركة باللجان .
- الاطلاع على أعمال الآخرين سواء من داخل المؤسسة او خارجها .
- محاولة معرفة الأساليب المختلفة لاتجاز الأعمال وعدم الاعتماد على طريقة واحدة .

1

المفهوم

مخبر الشركات والموارد

اهداف اللعبة

شروط اللعبة

راسلنا

على الفور قمت بالبحث عبر الانترنت ووجدت ان لغة Classic ASP قريبة جدا بل تكاد هي لغة برمجة تعلمت عليها قديما وكادت انساها وهي VB6 حيث قمت بتنزيل عده كتب إلكترونية وقراءتها وتطبيق ما فيها من امثلة لمدة ثلاثة أشهر من العمل المتواصل وخلال هذه الفترة قمت بتصميم الواجهات الخاصة باللعبة.



حيث تعمل هذه اللعبة كالتالي:

1. اختيار من متعدد عدة اسئلة نقوم بإدخالها من خلال اللعبة.
2. تظهر للموظف بعد التسجيل للعبة والدخول بالرقم السري واسم المستخدم على شكل مراحل لكل مرحلة خمسة أسئلة.
3. يتم تجميع النقاط حسب الاجابة الصحيحة وللراحل المتقدمة هنالك مساعدات:

- مساعده حذف اجابتين
- مساعده تبديل السؤال
- مساعده اضافة وقت اضافي





4. كما يتم ترتيب المتسابقين حسب النقاط

وقبل تفعيل اللعبة تراود إلى ذهني استقلالية وموضوعية المدقق الداخلي هل هذا يضعف الاستقلالية وموضوعية المدقق الداخلي حيث تنص المعايير الدولية للممارسة المهنية للتدقيق الداخلي وعدم ارتباطه بأي نشاط تنفيذي (معياري 1100).

الجواب هو لا.

عند تفسير هذا المعيار بشكل خاطيء فهو بمثابة خطوه للخلف في مجال عمل المدقق وحيث ان نشاط التدقيق الداخلي يضيف قيمة للمؤسسة فإنه يجب ان يكون بمثابة القائد والميسر في اي مجال يسمح له بذلك حيث تم تشكيل لجنة بعيده كل البعد عن التدقيق الداخلي لتقوم بوضع الاسئلة.

لا تنظر إلى هذا السؤال على انه سهل فدائما هنالك الاصعب

تم تفعيل اللعبة وتم تسجيل الدخول فعليا واللعبة بها من قبل الموظفين وليس ذلك فحسب بل هنالك أحد الموظفين رأيتهم (قام بفتح ملف الانظمة والتعليمات وهو يلعب اللعبة وكان متوترا قليلا لان لكل سؤال وقت محدد "أمل من الله ان لا يقوم بقراءة مقالي هذا"). وحيث ان اخر تحديث للعبة سوف يكون هنالك اختيار أحد الموظفين من قبل موظف اخر لتحديه باللعبة ومعرفة الفائز وكسب مزيد من النقاط.

والان انا اقوم بتعلم تصميم التطبيقات على الهواتف الذكية لتطوير اللعبة واتاحة اللعبة في جميع الاوقات وفي كل مكان.  
لا اعتقد ان هذه اللعبة قامت بزيادة المعرفة لدى الموظفين وحسب بل زادت من معرفتي انا شخصيا بتعلم المزيد من لغات البرمجة والفهم العميق لآمان تكنولوجيا المعلومات فقد تمكنت من اكتشاف ثغره خطيره في انظمة المعلومات الخاصة بإنظمة المؤسسة وتم التبليغ عنها.



للتواصل مع الكاتب: [ahmedmalaji@gmail.com](mailto:ahmedmalaji@gmail.com)

# A Practical Approach to Risk Tolerance

Written by : Mr. Hans Læssøe, AKTUS (www.aktus.dk), Denmark

**Risk** management textbooks, best in class presentations, white papers and standards etc., all identify that having a defined risk tolerance or risk appetite is pivotal for implementing a risk management process. Intuitively, it also makes perfect sense that you cannot validly discuss what is a big and a small risk, if you have not considered, what level of risk you are prepared to take. However, when it comes to explaining or inspiring a risk manager on “how” to define a risk appetite and make this a tangible metric ... the textbooks and white papers and standards seem to fade out. There are very few explicit best practices – at least outside the financial industries - where risk management is essentially an operational pricing process. Furthermore, risk appetite is by no means a static concept – just look at one’s personal level of risk appetite. Plenty of people enjoy riding a motorbike, even though it is known to be rather dangerous. Nevertheless, these same people, who choose to take the risk of driving a motorbike, systematically

look for traffic before crossing a road, even when the level of traffic is limited and the risk of being hit by a passing car is small.

Most risk literature as well as the ISO 31.000 standard suggests that risk management operates with a series of concepts :

**Risk capacity...** The level of risk the company is based to bear without “dying” in the process. Exposure beyond this level is essentially “lethal” to the company.

**Risk tolerance...** The level of risk the company is prepared to take, including the effect of treatments, to meet its targets. This level of risk taking is not to be exceeded by any individual risk or the risk portfolio.

**Risk appetite...** The level of risk the company is willing to take and retain in pursuit of defined targets, and hence the level of risk, the company accepts without further mitigation.

Modelled, it may look as the below sequence of increasing risk exposure :



One may choose to operate with all of these, but you can get a strong implementation just focusing on one, and be quite assertive about what this is. As risk professionals, we have to be aware that management and the board of directors we are addressing are not risk management professionals ; and are, hence, more prone to act on a simple and intuitively understandable concept than a combination of multiple metrics.

Below, it is assumed that we are working with the concept of “risk tolerance”, defined as the level of risk, the company is prepared (i.e. not necessarily willing) to take to prosper in their industry.

We look at a basic approach and definition and a consolidated approach with a maximum limit to defining risk tolerance.

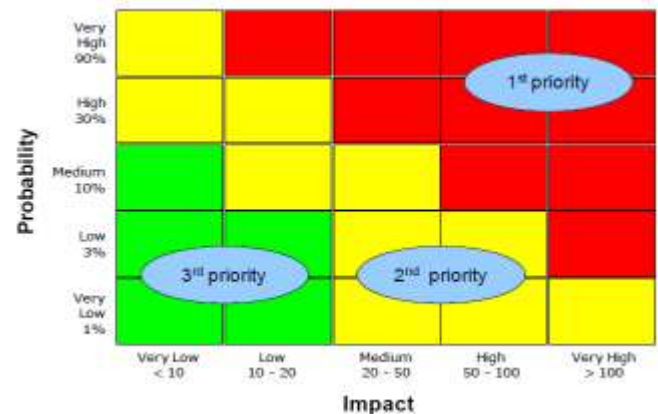
### A Basic Approach and Definition to Risk Tolerance

As mentioned, the “how” to define a risk tolerance for a company is not a matter of general knowledge, and many companies have implemented rather comprehensive risk management processes without having explicitly defined a risk tolerance. However, it really need not be very complex. Adhering to the 80/20 rule, will give the company 80% of the value using 20% of the efforts.

The suggested first step is to actively use a defined risk map, which most companies apply “the minute” they start obtaining an overview of their risk exposure. Here, for strategic risks, the underlying assessments are often estimates and coarse calculations as they do not have sufficiently detailed data to make in-depth statistics.

In this risk map, the probability and impact scales are defined explicitly--as they should be – and the cells have been color coded to indicate 1<sup>st</sup>, 2<sup>nd</sup>, and 3<sup>rd</sup> priority risks.

A company can now, define a risk tolerance in terms of : “We do not accept risks, which after mitigation, are still assessed to be 1st priority risks”. This limits the level of accepted net or residual risks to be those of 2<sup>nd</sup> or 3<sup>rd</sup> priority.

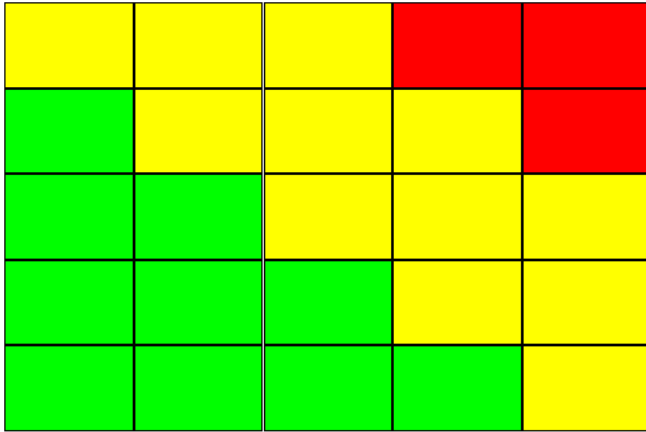


Furthermore, the scales can be used to define the risk tolerance. In this risk map it is stated that a very high impact is above 100 (e.g. million dollars), and the limits of the lower levels have been based on an approximate division factor of 2. These 100 million dollars may resemble, for example, projected earnings for the coming year, and hence essentially define the level of risk tolerance.

If/when the impact scale is “linked” to projected earnings this risk map becomes a dynamic expression of the exposure for the company.

Higher earnings will lead to a more “aggressive” impact scale, whereas lower earnings will lead to a more cautious one. For example, an explicit risk with an impact of 70 million dollars and a 10% probability would be a 1<sup>st</sup> priority risk ; but if the impact scale was “doubled” due to higher resilience it would be reduced to a 2<sup>nd</sup> priority. Beyond this, a company may choose different “designs” of risk maps. The below Risk Maps illustrates a risk-taking company and a more cautious/risk adverse company.

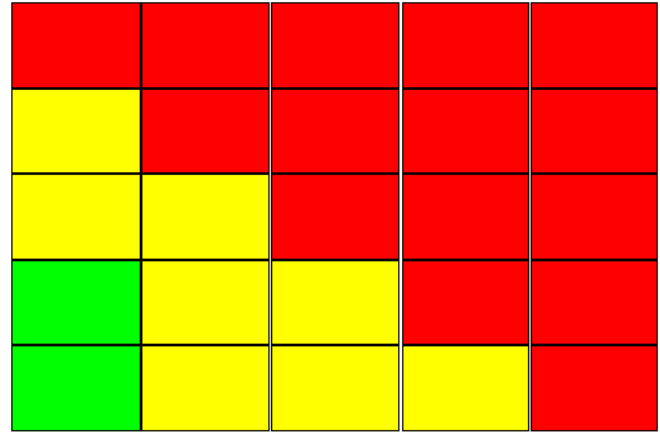
Risk Taking



This basic approach is seen as intuitively understandable and provides management with a clear guidance as to the risk management efforts needed. Furthermore, the reporting of the net/residual risk exposure immediately documents compliance to the defined tolerance. However, it is not complete. A company can be severely exposed to risks by having a huge number of risks which are not or cannot be mitigated to a sufficiently low level. It does not, therefore, enable the measure of a "total" or consolidated exposure, which is the basis for the next step in working with a defined risk tolerance.

**A Consolidated Approach : Assessing Risk Exposure**  
Risk management is about handling the extremes, where you cannot or will not live with the impact/consequences of the risk materializing ... irrespective of the probability. Referring back to the example of motorbike riding, if, whatever you do to drive carefully, still leaves a 1% risk of having an accident that damages your motorbike, and you Rather, one valid way to consolidate a risk portfolio is using Monte Carlo simulations. This is a mathematical technique where a computer is used to generate a huge number of "scenarios" based on the data provided and then compute the probability that outcome X will be higher than Y.

Risk Adverse

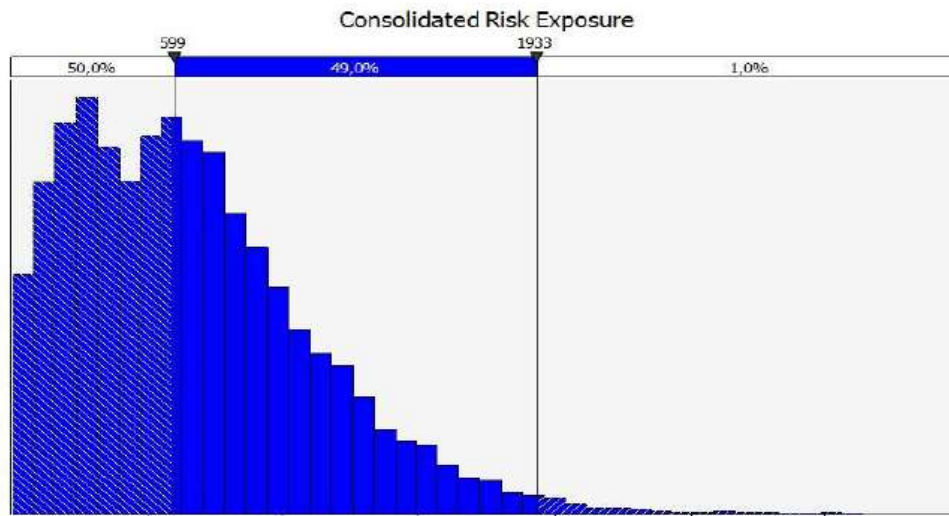


cannot afford to lose it, you will have to insure the value of the bike – irrespective of how low the probability of such an accident is (or alternatively, refrain from riding in the first place).

It is frequently seen that companies consolidate risks by multiplying the probability of each risk with the impact of that risk, and then adding the portfolio up. This is a systemic error as it drives risk management into an issue of averages.

If this were a valid approach, no-one would ever take out insurance on anything as the total costs of insurance premiums would exceed the average loss. (Insurance companies would be losing money every year.) Furthermore, one cannot validly add up the assessed impact of all risks in a portfolio as this inherently means that you assume ALL risks materialize at the same time. This is potentially not even possible. For example, if you lose your factory in a fire, it no longer has a consequence that a competitor limits your expansion into a new market.

For example, the Consolidated Risk Exposure Chart, shows the result of such a simulation--- there is a 50% chance that consolidated losses will be less than 599 million dollars and the 1% worst case is a loss of more than 1.933 million dollars.



There are a number of rather simple software tools and add-on packages that can make this kind of consolidation.

When defining the exposure of a risk portfolio, there is the possibility of defining the statistic/stochastic distribution of each risk individually. Some will have a 1% probability of happening with the impact specified, and thus have a 99% probability of not happening, i.e. have a zero impact. Others will have a 10% probability that they happen once, 1% they happen twice, or 0,1% chance they happen three times. There are mathematical distributions that describe this well. In your risk portfolio, you will need to define this for each risk, and then “run” the Monte Carlo simulation to get the results. See an example of a Monte Carlo simulation below.

As risk professionals, we have the mathematical background and insights to do these calculations and hence provide a valid consolidation of the risk exposure for the company. However, particularly for this reason, we should also be very cautious and recognize that no model can ever replace “common sense”.

Risk	Impact Mio USD	Probability %	Simulation
Competitor Move	80	30%	-
Loss of production capacity	200	3%	-
Failure to enter new market	50	10%	-
...			-
<b>TOTAL EXPOSURE</b>			

If a modeled calculation appears to be counter-intuitive, we have to validate our modeling before decisions are made. A key point to remember is that business trends follow simple logic more often than mathematical calculations.

### Assigning a Maximum Limit

Now that the consolidated risk exposure is made tangible and measurable, it makes sense to define a maximum limit that captures the essence of the company’s risk tolerance. This can hence be related to the metric on which the risks are assessed and defined in the risk map.



Assuming the impact scale is loss of profit compared to budget ... then the company risk tolerance can be defined as *“We do not accept that the net/residual risk exposure exceeds the budgeted earnings with more than 1% probability”* or *“We require a 99% certainty of a profit every year”*.

The degree of certainty must reflect the volatility of the industry. If the industry is highly volatile, one may find that a 99% assurance is either a larger than practical number, or essentially hampering management’s possibilities to develop and grow the company. The board of directors may then wish to use a 95% assurance. Such a metric is one that both management and the board of directors can understand and work with – without having to know the details of risk management terminology and mechanics. They have to assure themselves that they trust the underlying assessments and risk management processes.

#### **Non-financial risk taking**

The above has been all about the money, but evolving the risk management approach, we have to face that an organization may be hampered by and vulnerable to a rage on non-financial risks, where the risk tolerance has to be redefined. Some of these may be :

**Reputational** How much reputational “damage” do you accept as being your risk tolerance level. This may be measured in terms of press attention, negative social media attention, some image monitoring or the like.

**Environmental** How much environmental damage to your sites, and their surroundings will you be prepared to tolerate with mitigations.

Other scales may be safety, liquidity, collaborative trust, or whatever is pivotal for the company in question. The approach is the same, just applying other metrics and/or verbal descriptions to define risk exposure.

#### **Combining the Basic and Consolidated Approaches**

I recommend implementing both of the above approaches, and hence using the “no 1st priority risks” definition of risk tolerance to ensure that no single risk severely jeopardizes the performance of the company AND using the consolidated figure to ensure than the exposure of the full portfolio is still acceptable.

#### **Benefits of a Defined Risk Tolerance**

When management or the board of directors looks at the financial performance it is quite natural to compare this with the planned/budgeted performance and/or with the benchmark of other companies in a similar business. The outcome is an intelligent discussion of the performance, and how this can be sustained and improved in the future.

The same goes for risk exposure and risk tolerance. If the risk exposure is at or above the risk tolerance, the board of directors can have a serious discussion with management about how to limit the risks to an acceptable level. There is a balance between risks and rewards ... and if the defined risk tolerance is nowhere nearly utilized, the discussion could be on increasing the level of ambition and request that management becomes more aggressive and pursue even higher targets. Hence, the discussion of risks and risk exposure is not just one of restrictions and holding back.

Here are two generic examples of the benefits of having a defined risk tolerance :

\* **Company “A”** wishes to expand into a new market, but the project involves significant risks (and has potentially significant benefits). Management discusses whether they should “dare” to pursue the target.

If the potential risks of the project, when added to the ERM portfolio, still holds well within the defined risk tolerance, then the decision is probably a sound decision. Management can have discussions of how aggressive (costs and investments) they can allow themselves to be in the pursuit of the new target.

If, on the other hand, the project makes the company exceed their risk tolerance, the decision on the new venture is prudently “no”.

\* **Company “B”** has suffered a severe loss, and hence the approved risk tolerance in absolute value is reduced. This invokes that the company’s risk exposure exceeds the risk tolerance. Management needs to discuss measures to mitigate the risks, and possibly stop strategic development, which entails high levels of risk to comply with the risk tolerance defined by the board of directors. Management and the board of directors will need to discuss and re-define targets to a less ambitious level as the maneuverability of the company is reduced.

Comparing the risk exposure to a defined risk tolerance is providing a base from which strategic decisions can be made – prudently – and the explicit mitigation of risks becomes a strategic leverage/tool for the company.

## Closing Comments

In simple terms :

- a defined risk tolerance is needed to be able to address the risk exposure
- a risk tolerance can be defined based on the risk map alone
- you can [only] consolidate a risk portfolio by use of Monte Carlo simulation
- a consolidated exposure enables a portfolio based risk tolerance
- the risk tolerance can be used to discuss both whether the company is too exposed to risks or not exposed (ambitious) enough

The resulting reporting and discussions must be kept intuitively acceptable to management as well as to a board of directors, none of which are presumably risk management professionals. This is where strategic risk management becomes a competitive advantage, and the risk management community becomes value adding for the company.

---

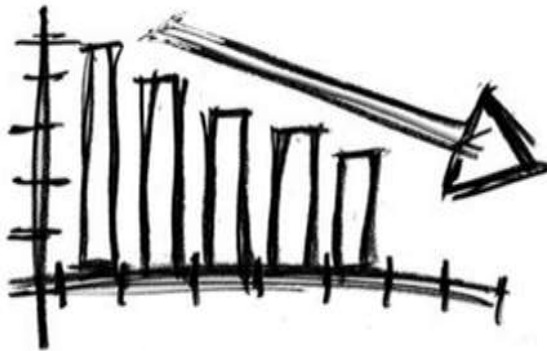
For further information, contact the author :  
hl@aktus.dk

# Sur l'usage des ratios par les auditeurs

Ecrit par : M. Jean-François Caron, Fondateur AUDITECOFI, France

## Un ratio pour tout dire...et parfois pas grand-chose

Un bon croquis vaut mieux qu'un long discours dit-on. En matière d'analyse, admettons volontiers qu'un bon ratio vaut mieux qu'une longue démonstration. Rapporтер deux variables entre elles pour les analyser conjointement et réciproquement est un exercice intéressant car il peut renseigner beaucoup à peu de frais. Cette méthode comparative est d'ailleurs recommandée par les normes internationales d'audit, avec la revue analytique. Les ratios font ainsi parties de la boîte à outils de l'auditeur. Il est possible de les exploiter aussi bien pour approfondir la connaissance des activités auditées que pour investiguer lors de la réalisation des travaux. Le rapport d'audit peut s'y référer également afin de synthétiser des constats. Simples sur la forme et faciles d'usage, leur multiplicité implique cependant que les ratios soient employés avec précaution. En effet, on peut facilement recevoir des signaux qui finalement ne reflètent pas grand-chose...



## Classer les ratios pour mieux les sélectionner

La sélection des outils d'audit à employer est fonction des objectifs de mission. S'agissant de la revue analytique, l'auditeur, en plus de s'assurer de son adéquation avec les attendus du programme de travail, doit sélectionner des ratios qui soient pertinents par rapport au domaine audité. Pour pratiquer de la sorte, l'auditeur doit connaître la signification des ratios utilisés par l'organisation et sur lesquels ils souhaitent s'appuyer pour ses travaux. Mais lorsque les informations sont multiples, leur agrégation induit le risque d'en perdre l'origine et donc le sens. En d'autres termes, trouver des ratios ne pose pas de difficulté pour l'auditeur, les mettre en « scène » par contre est plus délicat. Pour cet exercice, leur classement sera des plus utiles pour l'auditeur afin de retenir des indicateurs pertinents, notamment en les identifiant à partir :

**du bilan** : on trouvera dans cette rubrique le ratio d'endettement, le délai moyen de rotation des stocks, le ratio de recouvrement des créances clients, le délai moyen des paiements aux fournisseurs ;

**du résultat** : on distinguera ici les ratios liés au rendement des actifs et à la rentabilité des activités, à savoir le rapport entre les résultats et les moyens mis en œuvre pour atteindre ces résultats ;

**de données d'activité** : il s'agira de comparer des données réelles entre elles, ou avec des éléments monétaires, comme par exemple en matière de productivité.



### Les façons d'employer les ratios

L'emploi des ratios ne repose pas uniquement sur la pertinence du numérateur et du dénominateur, mais également sur la façon de les analyser, pour

finalement mettre en évidence des tendances de fonds ou identifier des écarts. A ce titre, les comparaisons peuvent être faites sur base :

**des arrêtés comptables**, entre plusieurs périodes. Sur ce point, l'auditeur prendra la précaution de bien définir la fréquence d'analyse selon les spécificités de l'activité audité, pour faire abstraction par exemple d'éventuels effets saisonniers ;

**du budget**, entre les données réelles et les éléments prévisionnels. L'auditeur s'assurera que l'analyse est faite à partir d'informations de même nature, qu'aucun biais n'impacte le passage d'une situation budgétée à la réalité ;

**des moyennes sectorielles**, entre les résultats de l'organisation et ceux d'entités du même secteur d'activité. L'auditeur interne prendra soin de contrôler la représentativité du panel sectorielle.



### Un exemple

التدقيق بقيادة ابداع تطوير

Dans le cadre de sa mission sur le processus client à fin décembre 2017, un auditeur obtient lors de l'enquête préliminaire des informations lui permettant de calculer les ratios suivants :

Nature du ratio	31 décembre 2017	31 décembre 2016
Délai moyen d'encaissement des créances clients	60 jours	50 jours
Taux de créances douteuses sur créances saines	15%	10%
Taux moyen de provisionnement	45%	20%

Sur cette base, l'auditeur peut identifier des points clés de contrôle :

le délai moyen d'encaissement des créances clients est-il cohérent avec les délais contractuels ? La hausse de 10 jours du délai moyen concorde-t-elle avec l'évolution des conditions de paiement accordées à la clientèle ? Cette hausse n'est-elle pas liée à un défaut de paiement significatif qui augmente d'autant le ratio moyen ? la hausse du taux de créances douteuses sur créances saines semble confirmer que les défauts de paiement ont augmenté, ceci concordant avec une hausse du délai moyen d'encaissement. L'auditeur doit donc obtenir le détail des créances douteuses par clients à fin 2017 pour comparaison avec le même détail à fin 2016 ; le taux moyen de provisionnement augmentant, l'auditeur vérifie si cette hausse est liée à un nouveau risque important constaté sur 2017, ou alors à un changement de méthode de provisionnement de l'organisation.

Cet exemple illustre l'intérêt pour l'auditeur d'employer des ratios, c'est-à-dire de se poser les bonnes questions pour établir un programme d'audit en phase avec la réalité !

---

Pour plus d'information, n'hésitez pas à contacter l'auteur : [jfcaron@outlook.fr](mailto:jfcaron@outlook.fr)

# 2019

## CIA Exam: Why, How, and What Is Changing January 2019

### Why ?

To ensure the material within all three parts of the CIA exam stays current and valid, the CIA underwent a global job analysis study to determine the knowledge, skills, and abilities most applicable to today's internal audit practitioners. The study results indicated the need to revise the exam syllabi to reflect the evolution of the internal audit profession worldwide.

### How ?

- Three exam parts are balanced, clear, and uniform.
- Minimal duplication and overlap among exam parts.
- Aligned with The IIA's International Standards for the Professional Practice of Internal Auditing.
- Up-to-date with the current global practice of internal auditing.
- Covers the knowledge, skills, and abilities exam candidates must possess to be the most competent and capable internal auditor possible.

### What ?

التدقيق قيادة ابداع تطوير

**1. CIA Exam Part One :  
Essentials of Internal  
Auditing**

**CURRENT VERSION**

- I. Mandatory Guidance
- II. Internal Control / Risk
- III. Conducting Internal Audit Engagements – Audit Tools and Techniques

**REVISED VERSION**

- I. Foundations of Internal Auditing
- II. Independence and Objectivity
- III. Proficiency and Due Professional Care
- IV. Quality Assurance and Improvement Program
- V. Governance, Risk Management, and Control
- VI. Fraud Risks

**2. CIA Exam Part Two :  
Practice of Internal  
Auditing**

**CURRENT VERSION**

- I. Managing the Internal Audit Function
- II. Managing the Individual Engagements
- III. Fraud Risks and Controls

**REVISED VERSION**

- I. Managing the Internal Audit Activity
- II. Planning the Engagement
- III. Performing the Engagement
- IV. Communicating Engagement Results and Monitoring Progress

**3. CIA Exam Part Three :  
Business Knowledge for  
Internal Auditing**

**CURRENT VERSION**

- I. Governance / Business Ethics
- II. Risk Management
- III. Organizational Structure / Business Processes and Risks
- IV. Communication
- V. Management / Leadership Principles
- VI. IT / Business Continuity
- VII. Financial Management
- VIII. Global Business Environment

**REVISED VERSION**

- I. Business Acumen
- II. Information Security
- III. Information Technology
- IV. Financial Management

## When ?

The updated CIA exams will take effect January 2019, in English only. Non-English exams will be released as follows :

Language	Availability Date
French and Spanish	June 1, 2019
German and Turkish	July 1, 2019
Arabic and Russian	August 1, 2019
Korean and Portuguese	September 1, 2019
Chinese Traditional and Japanese	October 1, 2019
Chinese Simplified	December 2019 or early 2020

Each candidate should review the changes and determine the best timing to complete their individual studies and take the exam.

Please review the CIA Exam : Why and How It's Changing Handbook and CIA Exam : FAQs for additional details.

<https://na.theiia.org/certification/CIA-Certification/Pages/cia-exam-why-and-how-its-changing.aspx>





## أعمقنا القراء

مجلة أوديتورز... الأولى في التدقيق

مجلة غير ربحية لا ينبغي أن تباع أو يعاد بيعها من قبل أي طرف

ندعج في تلقي آرائكم وتعليقاتكم حول المقالات والعدد الأول من مجلتكم

شاركونا مقترحاتكم عبر البريد الإلكتروني: [auditors.worldwide@gmail.com](mailto:auditors.worldwide@gmail.com)



ملاحظة: جميع الموضوعات والمشاركات التي تطرح في المجلة لا تعبر بالضرورة عن رأي فريق إعدادها، وإنما تعبر عن رأي كاتبها وتعتبر ملكية فكرية شخصية له.

حافة حقوق المؤلف والحقوق المجاورة والدفاع عن المصالح المادية والمعنوية لأصحاب تلك الحقوق محفوظة من قبل المؤسسة التونسية لحقوق المؤلف والحقوق المجاورة OTDAV ([www.otdav.tn](http://www.otdav.tn))