التدقيق الداخلي القائم على المخاطر

ممدوح الشنتير و سماح حسن

04/11/2023

ندوة / ويبنار

The Institute of
Internal Auditors

ما هو التدقيق الداخلي القائم على المخاطر؟

هل تطبق التدقيق الداخلي القائم على المخاطر ؟

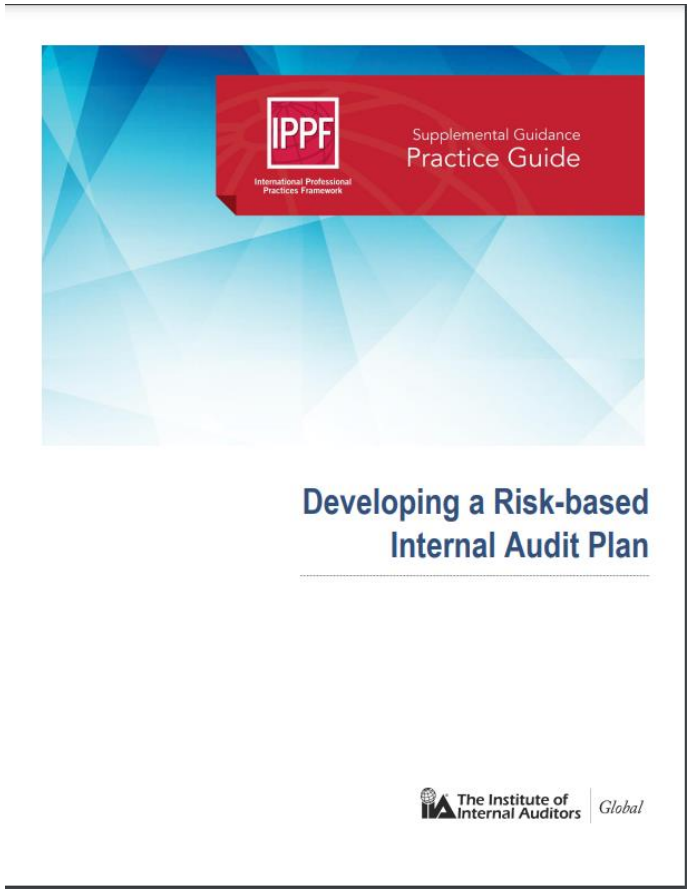
ما هو التدقيق القائم على المخاطر

هذه الندوة ستساعدك على :

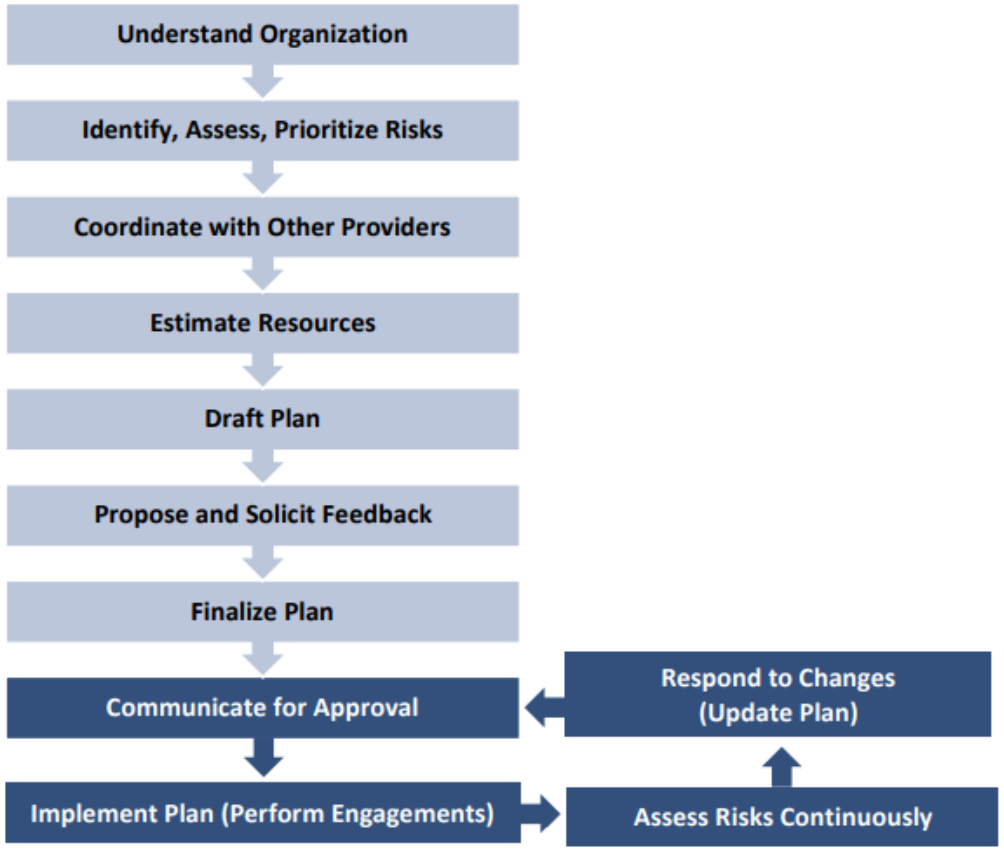
1. التعرف على أفضل الممارسات فيما يتعلق بالتدقيق على أساس المخاطر.
2. تقييم الوضع الحالي في مؤسستك.
3. القرار للخطوات التالية اللازمة لتطبيق التدقيق على أساس المخاطر في شركتك.

The Institute of
Internal Auditors

خطة التدقيق الداخلي القائم على المخاطر



دورة تطوير خطة التدقيق الداخلي



من المسؤول عن خطة التدقيق الداخلي القائمة على المخاطر؟

في حين أن الرئيس التنفيذي للتدقيق هو المسؤول عن خطة التدقيق الداخلي، إلا أن مديري التدقيق الداخلي ذوي الخبرة وموظفي التدقيق الداخلي قد يقومون ببعض الأنشطة ذات العلاقة لعملية التخطيط.

ومع ذلك، لا يوجد نهج واحد يناسب جميع الشركات، وتختلف الترتيبات من منظمة إلى أخرى (على سبيل المثال، بناءً على الحجم والموارد المتاحة لنشاط المراجعة الداخلية).

1- فهم عمليات الشركة

1- فهم عمليات الشركة

أ - تحديد الاهداف، الاستراتيجيات والهيكل

مثل ماذا ؟؟

1- فهم عمليات الشركة

ب - مراجعة الوثائق الأساسية

Information to Be Gathered	Potential Source Documents
▪ Which control and assurance roles are operating in the organization (i.e., first and second lines)? What are the responsibilities of each? ▪ Has the organization implemented an enterprisewide risk management (ERM) framework?	▪ Organizational chart. ▪ Minutes from meetings with senior management, second line management, and risk committees.

- جميع النصوص باللغة الإنجليزية في هذه المادة تم اخذها من دليل الممارسة Developing A Risk Based Internal Audit Plan

1- فهم عمليات الشركة

ب - مراجعة الوثائق الأساسية

Information to Be Gathered	Potential Source Documents
▪ What are the organization's main objectives, strategies, and initiatives? ▪ Are any major initiatives and change projects proposed in the upcoming period?	▪ Organization's strategic plan. ▪ Strategic plans for critical individual areas and major initiatives. ▪ Minutes of meetings between senior management and the board.

1- فهم عمليات الشركة

ب - مراجعة الوثائق الأساسية

Information to Be Gathered	Potential Source Documents
▪ What are the organization's key business processes? ▪ What are the potential risks and controls in each process? ▪ Are the strategies, objectives, and plans realistic? ▪ Have all relevant risks been captured?	▪ Annual reports and public/regulatory filings. ▪ Organizationwide risk register (also known as risk universe).[1] ▪ Management's risk registers (also known as risk inventories) and risk assessments, including risk and control self-assessments conducted by the leaders of each business area (operational risk assessments). ▪ Results of automated risk monitoring, if implemented. ▪ Previous assessments and reports from various assurance providers (second line functions, internal and external auditors). ▪ Detailed operational documentation (e.g., process maps). ▪ Annual reports and public/regulatory filings.

1- فهم عمليات الشركة

ج – الحصول على الاستشارات من أصحاب المصلحة

Stakeholders to Consider

- Board: audit committee, risk committee, governance committees, individual board members.
- Senior management, chief risk officer.
- Second line functions.
- Operational/line management.
- Human resources.
- Marketing.
- Employees performing key operational tasks.
- External auditors/regulators, as indicated (industry-specific).

Methods of Communication

- Face-to-face meetings.
- Phone/online conferences.
- Surveys.
- Interviews.
- Group brainstorming sessions, workshops.
- Ongoing, informal communication.

1- فهم عمليات الشركة

د. إنشاء (أو مراجعة) عالم التدقيق Audit Universe

- Organization's strategy and chain of value creation.
- All major areas, units, departments, and projects and their strategies, objectives, and processes (at high level, from the organizational chart, legal, and/or ERM framework).
- Third-party vendors (from legal, procurement, or contract management functions).
- Processes and subprocesses of all major functions (from process mapping activities such as those required by ISO).

- Major IT applications and information systems assets, including hardware, software, and the information they contain (from IT management).
- Regulatory and legal compliance requirements that apply to the organization.
- Nonfinancial performance indicators (e.g., environmental, health and safety, social, governance).

Figure C.1: Organizational Objectives, Strategies in Relation to Audit Universe

Organization's Objectives	
Objective 1	...
Objective 2	...
Objective 3	...
Objective 4	...
Objective 5	...
Objective 6	...

Strategy	Objective Links	Initiatives	Audit Universe Link
Strategy 1	Objectives 1, 6	1.1	Operations/service development, IT
		1.2	Legal, finance, compliance
		1.3	Governance
		1.4	Operations, IT
Strategy 2	Objectives 1, 2, 3, 4	2.1	Operations, finance
		2.2	Governance, legal
		2.3	Operations
Strategy 3	Objective 4	3.1	Governance
		3.2	Support/human resources
		3.3	Support/marketing
		3.4	Operations/service development, IT
		3.5	Operations, IT
Strategy 4	Objectives 5, 6	4.1	Governance, support/marketing
		4.2	Governance, risk management
		4.3	Support/purchasing
		4.4	Support/facilities

2. تقييم المخاطر للتدقيق الداخلي

2- تقييم المخاطر للتدقيق الداخلي

قد تكون المنظمات التي نفذت نظام إدارة المخاطر (ERM) قد أنشأت سجلًا شاملاً للمخاطر (والمعروف أيضًا باسم مخزون المخاطر أو كون المخاطر). يمكن للمدققين الداخليين استخدام معلومات إدارة المخاطر كإحدى المداخل في تقييم المخاطر الشامل للمؤسسة من قبل المراجعة الداخلية.

ومع ذلك، وفقًا لمبدأ النزاهة في ميثاق الأخلاق والمعيار 1100 - الاستقلالية والنزاهة، يجب على المدققين الداخليين أن يقوموا بأعمالهم الخاصة للتحقق من أن جميع المخاطر الرئيسية تم توثيقها بشكل صحيح وأن الأهمية النسبية للمخاطر تعكس بدقة.

2- تقييم المخاطر للتدقيق الداخلي

ماهي المخاطر؟
المخاطر الداخلية، والخارجية، والاستراتيجية
مخاطر تكنولوجيا المعلومات
مخاطر بيئية، واجتماعية، ومخاطر الحاكمية.
مخاطر الجهات الخارجية
مخاطر الاحتيال

تحديد المخاطر

- الهدف في التدقيق الداخلي القائم على تقدير المخاطر هو تحديد المخاطر التي يمكن أن تمنع الكيان من تحقيق أهدافه.
- يتطلب هذا الأمر تقدير مهني ومهارة.
- يجب أن تنظر إلى تأكيدات البيانات المالية بالإضافة إلى فعالية وكفاءة معالجة العمليات.
- طبيعة المخاطر ستحدد كيفية تصميم برنامج العمل.

تحديد المخاطر

- يمكن إدارة تصنيف المخاطر Risk classification بعدة طرق.
- يجب على مجموعات التدقيق الداخلي أن تحصل الى اتفاق مع الإدارة بشأن التصنيف.
- يحدد تقييم المخاطر طبيعة إجراءات التدقيق ووقتها ومداها.
- من الأمور الهامة تقييم المخاطر بشكل صحيح حتى يتم قضاء الوقت والجهد في التدقيق بكفاءة وفعالية.

طرق تقييم المخاطر

1. "نهج المخاطر المحددة" “specific-risk approach”

قد يُعتبر هذا النهج من الأسفل-الأعلى؛ لأنه يشمل تحديد المخاطر المرتبطة بكل auditable unit وحدة تدقيق/خاضعة للتدقيق محددة في كون التدقيق.

تُحدد المخاطر فيما يتعلق بأهداف الأعمال، عادةً من خلال الاجتماع مع الإدارة المعنية خصيصًا لهذا الغرض.

بناءً على المعايير المجتمعة (مثل التأثير واحتمالية حدوث المخاطر)، يتم حساب درجات المخاطر المجمعة لوحدات التدقيق الفردية.

يُستخدم هذا النهج بشكل متكرر في تقييم المخاطر المتعلقة بمهام التدقيق الفردية، ولكن قد يصبح معقدًا عندما يُمتد إلى مستوى المؤسسة، حيث يصبح عدد وحدات التدقيق والمخاطر كبيرًا إلى حد ما.

طرق تقييم المخاطر

1. "نهج المخاطر المحددة" “specific-risk approach”

مثال:

في هذا المثال عن (نهج المخاطر المحددة) ، الخطوة الأولى هي تحديد المعايير التي يتم بها تقدير كل مخاطر بناءً على التأثير واحتمالية حدوثها.

المعايير criteria الثلاثة المختارة في هذا المثال هي التنظيمية/القانونية، والتشغيلية، والمالية.
regulatory, operational, and financial

يتم تقدير التأثير على مقياس يتراوح بين 1 يمثل التأثير المنخفض و5 يمثل التأثير الكارثي.

تُقيَّم احتمالية حدوث المخاطر على مقياس يتراوح بين 1 يمثل احتمالية منخفضة جدًا و5 يمثل احتمالية عالية جدًا.

طرق تقييم المخاطر

1. "نهج المخاطر المحددة"

Figure D.1: Risk Impact Scale and Criteria

Impact Description	Impact Score	Regulatory Criteria	Operational Criteria	Financial Criteria
Catastrophic	5	Complex, highly regulated environment with strict enforcement; consequences for noncompliance likely to cause legal liabilities and penalties that may result in partial or complete shutdown. Significant financial and reputational impacts.	One or more business units or entire organization may be unable to operate. Impact on reputation.	Greater than $25 million
Highly Significant	4	Complex regulatory environment; legal liabilities and penalties for noncompliance may receive public attention and have lasting impact financially and reputationally.	Multiple business units may be significantly affected. Organization's ability to operate or serve customers may be severely reduced. Impact on reputation.	$10 million to $25 million
Significant	3	Laws and regulations are consistently enforced. Legal liabilities and penalties for noncompliance are material.	One or more business units may be materially affected. Organization's ability to operate or serve customers may be significantly reduced.	$5 million to $10 million (material)
Moderate	2	Active regulatory environment with small to moderate penalties for noncompliance.	Operational effectiveness and efficiency are moderately damaged.	$1 million to $5 million
Low	1	Regulatory environment is lax or penalty for noncompliance is small.	Operational effectiveness or efficiency could be improved, but operations proceed uninterrupted.	Less than $1 million

طرق تقييم المخاطر

1. "نهج المخاطر المحددة"

Figure D.2: Risk Likelihood Scale and Descriptions

Rating	Score	Description	Criteria
Very high	5	Likelihood of risk occurring is very high relatively.	Operational processes are complex and controls are not effective.
High	4	Likelihood of risk occurring is high relatively.	Operational processes are complex and some control weaknesses are noted.
Moderate	3	Likelihood of risk occurring is moderate relatively.	Operational processes are moderately complex; minor control weaknesses are noted.
Low	2	Likelihood of risk occurring is low relatively.	Operational processes are not complex; controls are effective.
Very low	1	Likelihood of risk occurring is very low relatively.	Operational processes are not complex. Controls are effective.

طرق تقييم المخاطر

1. "نهج المخاطر المحددة"

Step 2. List auditable units vertically and specific risks horizontally and rate impact and likelihood for each risk specific to each auditable unit.

Figure D.3 shows one customized example with each auditable unit in its own row and each risk in a column. Each risk column is subdivided into impact and likelihood ratings specific to the auditable unit. The ratings in this table are not weighted, so impact and likelihood ratings for each risk are added together across each auditable unit to arrive at a total risk score for each unit. The total risk score indicates the relative level of risk for each unit. This is only a simplified example. In practice, formats vary greatly; and generally, impact should be weighted more heavily than likelihood.

Figure D.3: Specific-risk Approach with Total Risk Score

L = likelihood I = impact	Risk 1		Risk 2		Risk 3		Risk 4		Risk 5		Risk 6		Risk 7		Risk 8		Total Score	Level
	L	I	L	I	L	I	L	I	L	I	L	I	L	I	L	I		
Auditable Unit 1	3	2	2	4	3	5	2	3	1	5	1	3	1	2	2	5	44	M
Auditable Unit 2	2	3	1	4	1	5	2	2	1	3	1	1	2	3	2	2	35	M
Auditable Unit 3	1	3	1	3	2	3	3	3	2	1	1	1	3	4	1	4	36	M
Auditable Unit 4	4	4	3	5	2	5	1	2	1	5	3	2	2	5	2	5	51	H
Auditable Unit 5	1	3	2	4	3	4	3	3	4	4	2	4	2	5	1	4	49	H
Auditable Unit 6	1	1	1	2	2	1	1	3	2	1	2	2	2	3	1	2	27	L
Auditable Unit 7	4	5	4	5	4	5	4	4	4	5	4	5	3	5	3	5	69	E
...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...

Rating for Score Ranges

Low (L) = 0 to 32 Moderate (M) = 33 to 45 High (H) = 46 to 59 Extreme (E) = 60+

طرق تقييم المخاطر

1. "نهج المخاطر المحددة"

Step 3. Score effectiveness of risk management and controls.

Figure D.4: Criteria to Assess Risk Management and Control Processes

Assessment of Design	Criteria for Risk Management and Control Processes
Adequate	▪ Risk management, control, and governance processes are operating effectively. May be efficient or have room to improve efficiencies. ▪ Risk ownership is clearly defined and active. ▪ Management remediates control deficiencies or other issues discovered by auditors and regulators. ▪ Management is proactive in risk identification and mitigation.
Needs Improvement	▪ Some risk management and control processes are operating effectively, but many are not documented or monitored. ▪ Most key risks are mitigated to an acceptable level. ▪ Some risks but not all risks have owners.
Inadequate	▪ Risk management and controls processes are poorly designed, inconsistently executed, or do not exist. ▪ Risk information is not documented and risks are not remediated fully. ▪ Risk management is reactive.

طرق تقييم المخاطر

1. "نهج المخاطر المحددة"

Step 4. Determine residual risk.

The assessment of inherent risk, control effectiveness, and residual risk may be shown as a chart (or "matrix") that includes a column quantifying risks in their inherent form, a column quantifying the effectiveness of the corresponding risk responses and controls, and a column for corresponding residual risk. Figure D.5 shows a sample chart.

Figure D.5: Determination of Residual Risk

Auditable Unit	Inherent Level of Risk	Control Effectiveness	Residual Level of Risk
Auditable Unit 1	Moderate	Need improvement	Moderate
Auditable Unit 2	Moderate	Adequate	Low
Auditable Unit 3	Moderate	Inadequate	Moderate
Auditable Unit 4	High	Adequate	Low
Auditable Unit 5	High	Needs improvement	High
Auditable Unit 6	Low	Adequate	Low
Auditable Unit 7	Extreme	Need improvement	Extreme
...	...	...	...

طرق تقييم المخاطر

2. نهج تقييم مخاطر العملية "risk-by-process approach"

هذا النهج مشابه لنهج المخاطر المحددة، ولكن:

يبدأ المدققون الداخليون والإدارة بالنظر في عمليات الأعمال في جميع أنحاء المؤسسة كوحدات قابلة للتدقيق.

تُخطط او يتم ربط المخاطر الرئيسية لكل عملية.

بالإضافة إلى ذلك، يعمل المدققون الداخليون على تحديد العمليات التي تلعب أدوارًا رئيسية في تحقيق الأهداف وكيفية إدارة المخاطر لتلك العمليات بفعالية.

تُعطى الأولوية للعمليات التي تحمل أعلى درجة من المخاطر المتبقية لتضمينها في خطة التدقيق الداخلي.

طرق تقييم المخاطر

3. نهج تقييم عوامل الخطر "risk factor approach"

يُعتبر هذا النهج من الأعلى-للأسفل لأنه ينظر إلى الظروف على المستوى العالي التي تكون مشتركة عبر معظم الوحدات القابلة للتدقيق.

يحدد المدققون الداخليون العوامل المشتركة بين جميع وحدات التدقيق التي تؤثر في قدرة المؤسسة على تحقيق أهدافها.

عوامل المخاطر ليست المخاطر بذاتها بل بدلاً من ذلك هي الظروف التي من المرجح أن ترتبط بوجود مخاطر.

هذه الظروف تشير إلى احتمالية أعلى لحدوث عواقب مخاطر كبيرة. قد يصبح قائمة العوامل المحتملة للمخاطر كبيرة، مما يعقد عملية تقييم المخاطر.

قد يبسط مديرو التدقيق الداخليون الأمور عن طريق تصنيف هذه العوامل إلى فئات مثل الاستراتيجية، والامتثال، والتشغيل، والمالية.
في بعض المؤسسات، يمكن للإدارة العليا ومجلس الإدارة أن يقدموا نصائح لنشاط التدقيق الداخلي بشأن العوامل المحتملة للمخاطر التي يعتقدون أنها أكثر أهمية.

بعض العوامل المحتملة للمخاطر قد تكون مرتبطة بعدة فئات. ومع ذلك، يمكن أن يكون تصنيف العوامل المحتملة للمخاطر مناسبًا عند تلخيص تقييم المخاطر للإدارة العليا ومجلس الإدارة.

طرق تقييم المخاطر

3. نهج تقييم عوامل الخطر "risk factor approach"

أمثلة على عوامل المخاطر وفئات عوامل المخاطر تشمل:

- مستوى النشاط النسبي (على سبيل المثال، عدد الحركات او الصفقات).
- الجدوى (حجم الإيرادات أو النفقات).
- سيولة الأصول المشمولة.
- التأثير على العلامة التجارية (الإدراك العام، السمعة).
- عدم تحقيق الأهداف.
- كفاءة الإدارة، الأداء، التداول.
- العيوب المعروفة (نتائج المشاركة غير المرضية سابقًا).
- درجة التغيير في الأنظمة والسياسات والإجراءات والعقود والعلاقات.
- عرضة للاحتيال.
- تعقيد العمليات.
- درجة الاعتماد على الأطراف الثالثة.
- قوة ضوابط الرقابة الداخلية وبيئة الرقابة.
- درجة التشريع والقوانين، واهتمامات الامتثال.
- الوقت منذ آخر تقييم أو تدقيق.

طرق تقييم المخاطر

3. نهج تقييم عوامل الخطر "risk factor approach"

Figure E.1: Example of Defining Risk Factors, Criteria, and Ratings

Risk Factor Name	Considerations/Criteria	Ratings and Definition
Loss/Material Exposure	▪ Dollar value at risk. ▪ Annual operating expenses. ▪ Number of transactions. ▪ Impact on other areas of organization. ▪ Degree of reliance on IT.	5 = high exposure. 4 = above average exposure. 3 = average exposure. 2 = less than average exposure. 1 = little exposure.
Strategic Risk	▪ Public perception / reputation. ▪ Local economic conditions. ▪ Volatility. ▪ Significance to strategy. ▪ Degree of external regulation. ▪ Recent change in legislation or regulatory scrutiny. ▪ Changes in business lines or services. ▪ Significant new contracts.	5 = high risk. 4 = above average risk. 3 = average risk. 2 = less than average risk. 1 = low risk.

Figure E.1: Example of Defining Risk Factors, Criteria, and Ratings

Risk Factor Name	Considerations/Criteria	Ratings and Definition
Control Environment (CE)	▪ Degree of process isolation. ▪ Degree of formalization and alignment of objectives. ▪ New process/system implementation. ▪ In-house vs. third-party process. ▪ Operational management turnover. ▪ Degree of performance monitoring is in place. ▪ Tone at the top. ▪ Formality of processes/procedures. ▪ Impact on customers.	5 = high risk (very weak CE). 4 = above average risk (weak CE). 3 = average (average CE). 2 = below average risk (strong CE). 1 = low risk (very strong CE).
Complexity	▪ Degree of automation. ▪ Degree of specialization required to perform. ▪ Level of technical detail. ▪ Complexity of structure, architecture involved. ▪ Frequency of change.	5 = highly complex. 4 = above average complexity. 3 = average complexity. 2 = less than average complexity. 1 = simple.

Figure E.1: Example of Defining Risk Factors, Criteria, and Ratings

Risk Factor Name	Considerations/Criteria	Ratings and Definition
Assurance Coverage	▪ Type of engagement. ▪ Other reviews (external, regulatory). ▪ Second line coverage. ▪ Follow-up already in place.	5 = not reviewed in last 4 years (3 years for compliance or high-impact risks). 4 = not reviewed in last 3 to 4 years (2 to 3 years for compliance or high-impact risks). 3 = reviewed in last 2 to 3 years (1 to 2 years for compliance or high-impact risks). 2 = review in last 1 to 2 years (1 year for compliance, high impact). 1 = reviewed in last year or initiative in place currently.
Management Awareness	▪ Concerns expressed in responses to surveys. ▪ Concerns expressed in interviews. ▪ Level of risk awareness.	5 = management concerned, has specific issue and reason. 4 = management has general concerns. 3 = management is neutral. 2 = management has no specific concerns. 1 = management can demonstrate effective control over risks.

Figure E.2: Example of Determining Total Risk Score

	Impact-related Risk Factors			Likelihood-related Risk Factors					
Auditable unit	Loss/ material exposure	Strategic risk	Subtotal	Control environment	Complexity	Assurance coverage	Manage-ment awareness	Subtotal	Total risk score
Weight	*50%*	*50%*		*35%*	*35%*	*20%*	*10%*		
Unit 1	1	2	1.5	2	1	3	1	1.75	**3.25**
Unit 2	5	5	5	3	1	5	1	2.5	**7.5**
Unit 3	1	5	3	4	5	4	2	4.15	**7.15**
Unit 4	5	5	5	5	4	5	4	4.55	**9.15**
Unit 5	5	2	3.5	4	2	2	4	2.9	**6.4**
...	...	...	...	...	...	...	...	...	...

Total Risk Score Key	2 to 4 = Low	4.1 to 6.5 = Moderate	6.6 to 8.5 = High	8.6 to 10 = Very High

Ranking scale: 1 is lowest; 5 is highest. Lowest possible total score = 2. Highest possible total score = 10.

2- تقييم المخاطر للتدقيق الداخلي

كيف نقيس المخاطر؟

المخاطر الكامنة / المتأصلة Inherent Risk

يجب على المدققين الداخليين في تقييم المخاطر تقدير المخاطر الكامنة - وهي المخاطر التي تكون موجودة إذا لم تكن هناك أي ضوابط - والمخاطر المتبقية residual risk.

هذا التمييز مهم لأن الإدارة عادةً ما تفكر بشكل رئيسي فيما يتعلق بالمخاطر المتبقية، ولكن يجب على المدققين الداخليين أن يكونوا قادرين على النظر في ما إذا كانت تقنيات تخفيف المخاطر مصممة وتعمل بشكل فعال.

تبدأ تقييمات المخاطر للتدقيق الداخلي بالنظر في المخاطر الكامنة، وهي مزيج من المخاطر الداخلية والخارجية في حالتها الخالصة وغير المُسيطر عليها.

2- تقييم المخاطر للتدقيق الداخلي

استراتيجيات إدارة المخاطر والمخاطر المتبقية

المخاطر المتبقية، أو المخاطر الصافية، هي الجزء من المخاطر الكامنة الذي يبقى بعدما تنفذ الإدارة استراتيجيات إدارة المخاطر.

بالاستعانة بالإدارة، يقوم المدققون الداخليون بتحديد/التعرف على استراتيجيات إدارة المخاطر والضوابط الرقابية وترجمتها إلى مصطلحات تشغيلية أو قابلة للقياس للمساعدة في تحديد المخاطر المتبقية.

يجب على مدير التدقيق الداخلي أو المدققين الداخليين المعينين توثيق أسباب تقديرهم للمخاطر المتبقية.

2- تقييم المخاطر للتدقيق الداخلي

الترجيح Weighting، إجمالي درجة المخاطر

بعض العوامل أكثر أهمية لتحقيق الأهداف من غيرها، وبالتالي يمكن أن يتم ترجيحها (عددياً).

تُقيم كل وحدة يمكن تدقيقها بناءً على كل عامل مخاطر، وتُجمع تقييمات عوامل المخاطر لإنشاء درجة مخاطر مجتمعة واحدة للوحدة التي يمكن تدقيقها، وتسمى بإجمالي درجة المخاطر.

توفر هذه الدرجة أساسًا للمقارنة في تحديد أولويات وتصنيف وحدات التدقيق.

2- تقييم المخاطر للتدقيق الداخلي

خريطة الحرارة

يمكن تصوير نتائج تقييم المخاطر بمستويات المخاطر لكل وحدة يمكن تدقيقها بشكل رسومي في خريطة حرارة أو رسم بياني مماثل لمساعدة في إظهار تصنيف الأولويات.

تكون خرائط الحرارة مفيدة بشكل خاص عندما تكون معايير معينة مرتبطة بأهمية أكبر من غيرها وعند العروض البصرية لمجلس الإدارة والإدارة العليا.

RISK MANAGEMENT HEAT MAP

SEVERITY						
	CATASTROPHIC	HIGH	HIGH	HIGH	EXTREME	EXTREME
	MAJOR	MODERATE	MODERATE	HIGH	HIGH	EXTREME
	MODERATE	LOW	MODERATE	MODERATE	HIGH	HIGH
	MINOR	LOW	LOW	MODERATE	MODERATE	MODERATE
	INSIGNIFICANT	LOW	LOW	LOW	LOW	MODERATE
		RARE	UNLIKELY	POSSIBLE	LIKELY	ALMOST CERTAIN
		PROBABILITY				

2- تقييم المخاطر للتدقيق الداخلي

التحقق من تقييم المخاطر مع الإدارة

يأخذ نشاط التدقيق الداخلي في اعتباره اراء المعنيين طوال عملية تطوير خطة التدقيق الداخلي، وتُشكل هذه الردود فعل تقييم المخاطر لنشاط التدقيق الداخلي.

في الوقت نفسه، يجب أن يظل نشاط التدقيق الداخلي مستقلاً وموضوعياً، بما في ذلك تقييم المخاطر.

يجب على مديري التدقيق الداخلي أن يلتقوا مع الإدارة العليا لمراجعة تقييم التدقيق الداخلي، وضمان الشمول والتفاهم المتبادل، ومناقشة أسباب أي اختلافات كبيرة في تصورات المخاطر أو التصنيفات.

يمكن لمديري التدقيق الداخلي أخذ مستوى وعي الإدارة بالمخاطر في اعتبارهم بتمثيله كعامل مخاطر وإضافة أو خصم النقاط من الإجمالي لتقدير المخاطر لزيادة أو تقليل أهمية المخاطر مقارنة بالوحدة التي يمكن تدقيقها.

إعتبارات التخطيط الإضافية

The Institute of
Internal Auditors

إعتبارات التخطيط الإضافية

استيعاب طلبات الإدارة ومجلس الإدارة

يمكن للإدارة العليا و/أو مجلس الإدارة طلب خدمات التأكيد والاستشارة، ويجب على مدير التدقيق الداخلي استيعاب هذه الطلبات.

يمكن طلب خدمات الاستشارة/التوجيه في مجالات أو عمليات لم تظهر ضمن أعلى الأولويات في تقييم المخاطر؛ وغالبًا ما تكون هذه الفرص فرصًا لنشاط التدقيق الداخلي لتقديم نصائح تخفض من احتمالية حدوث المخاطر في المستقبل.

على سبيل المثال، يُمكن أن يُطلب من مدققين داخليين تحديد السبب الجذري لفشل تدقيق خارجي أو مراجعة تنفيذ عملية أو تكنولوجيا جديدة. وبالتالي، يحتفظ العديد من مدراء التدقيق بنسبة من خطة التدقيق الخاصة بهم لأداء الخدمات الاستشارية المطلوبة وأيضًا الخدمات غير المخططة التي تنشأ بين وقت تقييم المخاطر ووقت تعديل الخطة. يجب أن يتم تعبئة/عكس استثمارات موارد تدقيق الجودة الشاملة في خدمات الاستشارة في موازنة وخطة التدقيق الداخلي.

إعتبارات التخطيط الإضافية

تكرار مهمة التدقيق والتوقيت

لا يمكن مراجعة جميع المجالات التي يمكن تدقيقها في كل دورة تدقيق، ولا ينبغي أن تكون كذلك.

المفترض، أن يتم تحديد تكرار التدقيق استنادًا إلى تقييم المخاطر.

يجب على مديري التدقيق الداخلي أن ينظروا في أي مهام تدقيق ستعزز بشكل أكبر من قدرة المؤسسة على تحقيق أهدافها وأيها لديه الإمكانية لإضافة أكبر قيمة.

إعتبارات التخطيط الإضافية

تحديد التكرار استنادًا إلى المخاطر

في خطة التدقيق الداخلي القائمة بناءً على المخاطر بشكل كامل، يمكن لمديري التدقيق الداخلي تطبيق إحدى استراتيجيتين للوصول إلى التكرار الامثل لمهام التدقيق المخططة:

1. يمكن أن تعتمد خطة التدقيق على تقييم مستمر للمخاطر دون تحديد مسبق لتكرار مهام التدقيق. نظرًا لزيادة معدل التغيير في المخاطر في الوقت الحالي، تقوم العديد من المؤسسات بتنفيذ التدقيق المستمر، مما يتيح لهم الاستجابة بشكل ديناميكي للتغييرات طوال العام، مع إجراء تغييرات دورية في خطة التدقيق حسب الحاجة. تُعرَف هذه الخطط بأنها "rolling," "fluid," and/or "dynamic." "متداولة"، "متغيرة"، و/أو "دينامية".

2. تعتمد تكرار التدقيق على مستوى المخاطر المتبقية الذي تم تحديده في تقييم المخاطر. على سبيل المثال، قد يتم تدقيق وحدات أو بنود بتصنيفها على أنها عالية المخاطر على الأقل سنويًا (أو مرة واحدة كل 12 إلى 18 شهرًا)، والتي تصنف بمستوى معتدل من المخاطر قد تتم مراجعتها كل 19 إلى 24 شهرًا، وقد تكون الوحدات المصنفة على أنها منخفضة المخاطر قد تدقق مرة واحدة فقط كل 25 إلى 36 شهرًا (أو لا تدقق).

إعتبارات التخطيط الإضافية

تحديد التكرار استنادًا إلى المخاطر

لضمان أن يشمل خطة التدقيق الداخلي جميع المهمات الإلزامية والمستندة إلى المخاطر، يجب على المدققين الداخليين أن يأخذوا بعين الاعتبار:

- المهمات المطلوبة بموجب القانون أو التنظيم.
- المهمات ذات الأهمية بأهداف ومهمة الشركة.
- الوقت والموارد المطلوبة للمهمات الإلزامية وأولويات المهام القائمة على المخاطر.
- ما إذا كانت جميع المخاطر الكبيرة تحظى بتغطية كافية من مقدمي الخدمات التوكيدية.
- نسبة الخطة التي يجب أن تخصص لمشاريع خاصة، والاستشارات، أو الطلبات العرضية.

إعتبارات التخطيط الإضافية

تكرار مهمات التدقيق في القطاعات ذات التشريع والتنظيم العالي

في بعض القطاعات، مثل الخدمات المالية، تخضع المؤسسات للتشريعات التي تتطلب منها إعداد كون من التدقيق/المخاطر، وتقييمات المخاطر، والحفاظ على دورية مهام التدقيق.

حتى إذا كانت المخاطرة الكامنة لعدم الامتثال صغيرة، يجب أن تُدرج هذه الالتزامات في كون التدقيق لضمان أداء نشاط التدقيق الداخلي بالحرفية والكفاءة المهنية المستحقة.

عندما تتطلب القوانين أو التنظيمات أو معايير الصناعة/القطاع إجراء بعض مهام التدقيق دوريًا، يمكن لرئيس التدقيق الداخلي تصميم خطط تدقيق متعددة السنوات يوثق توقيتها وأي موارد متخصصة أو إضافية قد تكون مطلوبة.

بالإضافة إلى تنسيق المعلومات التي تم جمعها، يجب على المدققين الداخليين العمل مع المدققين الخارجيين لمزامنة توقيت مهام التدقيق والتداخل الأدنى في عمليات المؤسسة.

إعتبارات التخطيط الإضافية

تكرار مهمات التدقيق في القطاعات ذات التشريع والتنظيم العالي

على الرغم من أن هذه المهمات الدورية مطلوبة، إلا أنها تتنافس على الموارد مع مهمات التدقيق التي تم تحديدها بناءً على مستوى المخاطر.
إلى حد ما، قد تبدو متعارضة مع مفهوم التدقيق القائم على المخاطر.

لمعالجة هذا التحدي، يمكن لرؤساء التدقيق الداخليين القيام بما يلي:

- تقليل نطاق المهمات الإلزامية، بحيث يتعاملون مع المجالات المطلوبة دون الاستثمار خارج الحد الأدنى المطلوب.
- تمديد الجدول الزمني للخطة على المدى الطويل (مثلاً لسبع سنوات) ،مع استمرار تقييم المخاطر وضبط الخطط القصيرة الأجل بشكل أكثر تواترًا لتحديد أولويات المهمات المرتبطة بالمخاطر الكبيرة.
- التنسيق مع مقدمي خدمات التأكيد الآخرين والاعتماد عليهم. على الرغم من أن المهمات الدورية تشكل إحدى المداخل في خطة التدقيق الداخلي، يجب على رؤساء تدقيق الحسابات الداخليين أن يكونوا حذرين في الاعتماد بشكل كبير على خططهم طويلة الأمد في ظل التغير السريع في المخاطر الحالية.

3- التنسيق مع مقدمي الخدمات الاخرين

3- التنسيق مع مقدمي الخدمات الاخرين

- يضيف نشاط التدقيق الداخلي أكبر قيمة من خلال تقديم خدمات التأكيد والاستشارات في حال تواجد المخاطر المتبقية العالية.
- ومع ذلك، في الشركات ذات التنظيم العالي، فان بعض المجالات ذات المخاطر العالية تتم السيطرة عليها بشكل فعال من خلال خط الدفاع الأول، وقد يكون لها تغطية لتقديم خدمات توكيد كافية يوفرها خط الدفاع الثاني مثل إدارة المخاطر ووظائف الامتثال، بالإضافة إلى تغطية إضافية من قبل المدققين الخارجيين.
- قد يقوم كبير موظفي المعلومات أو كبير موظفو أمن المعلومات في الشركة بتقييم مخاطر تكنولوجيا المعلومات، وقد يدعم نشاط التدقيق الداخلي نتائج التقييم.
- لتحقيق أقصى استفادة من الموارد الماتحة، يجب على الرئيس التنفيذي للتدقيق تنسيق الأنشطة ومشاركة المعلومات والنظر في خدمات التوكيد والاستشارات المقدمة من مزودي الخدمة الداخليين والخارجيين (معيار 2050 - التنسيق والاعتماد). إن الاعتماد على عمل مزودي الخدمة الآخرين بدلاً من تكرار تغطية نفس الخدمات من الداخل يقلل من ازدواجية العمل ويزيد من الكفاءة التي يتم بها تقديم خدمات التوكيد.

3- التنسيق مع مقدمي الخدمات الاخرين

خرائط التوكيد

- توثق خرائط التوكيد التنسيق لتغطية خدمات التوكيد.
- كذلك فهي تدرج جميع المخاطر المحددة وتربطهم بخدمات التوكيد ذات الصلة.
- واستنادًا إلى المعلومات المجمعة، يمكن تصنيف درجة أو مستوى تغطية خدمات التوكيد المقدمة على أنها كافية أو غير كافية بحيث تصبح الفجوات والازدواجية واضحة. يتضمن إنشاء خرائط التوكيد تعاون مختلف مقدمي خدمات التوكيد من منظور شامل على مستوى المؤسسة .
- إن تحديد مكان تداخل عمل مزودي الخدمة الآخرين مع نشاط التدقيق الداخلي يساعد في تبرير قرار الرئيس التنفيذي للتدقيق بشأن المهام التي يجب تضمينها أواستبعادها من خطة التدقيق الداخلي. توفر الخريطة أيضًا دليلاً واضحًا على الثغرات في خدمات التوكيد، حيث قد تكون هناك حاجة إلى موارد إضافية .

مثال حول خرائط خدمات التوكيد

Processes	Three lines of defence assurance providers											
	First line of defence			Second line of defence				Third line of defence				
	Management-based assurance			Risk and legal-based assurance				Independent assurance				
	Control self assess-ment	Special project	Manage-ment review	Risk manage-ment	Health and safety	SOX	Com-pliance	External audit	Internal audit	ISO certifica-tion	Consult-ing engineers	Special project
Strategic												
Cash/finance and treasury												
Funding												
Sustainability												
Growth / mergers & acquisitions												
Alliances												
Operational												
Financial												
IT												
Treasury												
Human resources												
Supply chain management												
Quality												
Environment												
Customers												
Products & services												

4- تقدير الموارد اللازمة

4- تقدير الموارد

- يجب على الرئيس التنفيذي للتدقيق تحديد الموارد اللازمة لتنفيذ الخطة .
- قد تشمل الموارد الأشخاص (على سبيل المثال، ساعات العمل والمهارات)، والتكنولوجيا (على سبيل المثال، أدوات وتقنيات التدقيق)، والتوقيت/الجدول الزمني (توافر الموارد)، والتمويل .
- يجب على الرئيس التنفيذي للتدقيق تقدير نطاق المهام والمهارات والوقت والميزانية اللازمة لأداء تلك المهام .
- قد يفكر الرئيس التنفيذي للتدقيق في طبيعة كل مهمة وتعقيدها، والموارد التي تم إنفاقها على المهام المماثلة التي تم تنفيذها سابقًا، وتاريخ آخر مراجعة للمنطقة أو العملية .

4- تقدير الموارد

متطلبات مصادر التدقيق الداخلي

المعيار 2030 – ادارة المصادر

يجب على الرئيس التنفيذي للتدقيق التأكد من أن موارد التدقيق الداخلي مناسبة وكافية وموزعة بشكل فعال لتحقيق الخطة المعتمدة

التفسير:
المصادر اللازمة لتنفيذ الخطة يجب أن تتشكل من مزيج من المعرفة والمهارات والكفاءات الأخرى.

تشير "كافية" إلى كمية الموارد اللازمة لإنجاز الخطة. يتم استخدام الموارد بشكل فعال عندما يتم استخدامها بطريقة تعمل على تحسين تحقيق الخطة المعتمدة.

4- تقدير الموارد

مهارات التقييم

يصف معيار 2030 "الموارد المناسبة" من حيث المعرفة والمهارات والكفاءات .

تحظى كفاءة نشاط التدقيق الداخلي باهتمام كبير في المعايير وهي أحد المبادئ الأربعة في ميثاق الأخلاقيات الخاص بمعهد المدققين الداخليين .

كجزء من تخطيط التدقيق الداخلي، يجب أن يعرف الرؤساء التنفيذيون للتدقيق كفاءات فريق التدقيق الداخلي. قد يقوم رؤساء التدقيق الداخلي بوضع والاحتفاظ بجرد للمهارات والمعرفة المتخصصة لكل مدقق، إلى جانب مقياس للمهارات اللازمة لتلبية توقعات واحتياجات ومتطلبات المنظمة والصناعة.

قد تقدم بعض الشركات ذات التنظيم العالي قائمة بالحد الأدنى من المهارات المتوقعة وقد يتطلب ذلك إجراء تحليل للمهارات بانتظام. ويمكن بعد ذلك ضبط المعيار المحدد لتحديد المهارات المحددة اللازمة لتحقيق خطة التدقيق الداخلي .

4- تقدير الموارد

الحاجة لمهارات اضافية

إذا كان نشاط التدقيق الداخلي يفتقر إلى المعرفة أو المهارات اللازمة لإكمال مهمة تأكيد معينة، فقد يستعين الرئيس التنفيذي للتدقيق بخبير أو متخصص من داخل الشركة لتوفير الخبرة الفنية وتزويد موظفي التدقيق الداخلي في نفس الوقت بالمعرفة الجديدة.

وتشمل الخيارات الأخرى الاستعانة بمصادر خارجية كشركاء في مهمة التدقيق، حيث يقوم خبراء من خارج الشركة بأداء عمل متخصص تحت إشراف مدقق داخلي من ذوي الخبرة.

والاستعانة بشكل كامل، حيث يتم تنفيذ العمل بالكامل من قبل شركة خارجية. ويجب على الرئيس التنفيذي للتدقيق أن يأخذ في الاعتبار ترتيبات هذه الخدمات ضمن موازنة الخطة .

4- تقدير الموارد

احتساب ساعات العمل للخطة

لحساب ساعات موارد التدقيق الداخلي "المتاحة"، يقوم الرئيس التنفيذي للتدقيق بحساب إجمالي عدد الساعات التي يستطيع كل عضو في فريق التدقيق الداخلي المساهمة فيها في إكمال خطة التدقيق في فترة معينة (عادةً سنة واحدة) .

بحيث يأخذ إجمالي الساعات المتاحة في عين الاعتبار نتائج تقييم المهارات، واستخدام الموارد الخارجية والموظفين المساعدين، والمهام التي لا تساهم في إنجاز الخطة .

على سبيل المثال

قد يبدأ الرئيس التنفيذي للتدقيق بافتراض أن الموظف بدوام كامل يمثل ما يعادل إجمالي 2080 ساعة (أي 40 ساعة في الأسبوع، 52 أسبوعًا في السنة).

بعد ذلك، يجوز للرئيس التنفيذي للتدقيق طرح ما يلي لتحديد الساعات المتاحة المتبقية :

4- تقدير الموارد

احتساب ساعات العمل للخطة

اطرح الوقت غير المتعلق بالمراجعة، أو الوقت غير المنتج، بناءً على الأنشطة التي لا تساهم في إكمال المهام وتنفيذ خطة المراجعة:

إجازة مدفوعة الأجر (الإجازات، الإجازات، الإجازات المرضية مدفوعة الأجر).

- التدريب والتطوير الشخصي.
- الاجتماعات (داخل فريق التدقيق الداخلي، ومع الإدارة ومجلس الإدارة).
- مبادرات ضمان الجودة والتحسين لنشاط التدقيق الداخلي.
- انخفاض معدلات الاستخدام للموظفين الجدد المتوقعين في العام المحدد.
- الوقت المستغرق في التشاور مع الخبراء المختصين لتطوير استراتيجيات/أطر عمل التدقيق.
- معدل دوران غير متوقع خلال العام (أي "عامل الشغور"، الذي يستخدم عادةً لعدد كبير من الموظفين) .
- احتياطي للمهام غير المتعلقة بالتدقيق والتي لم يتم تعيينها بعد.

4- تقدير الموارد

احتساب ساعات العمل للخطة

- اطرح الوقت الذي تقضيه في مساعدة مقدمي خدمات التوكيد الآخرين، على سبيل المثال، التدقيق الخارجي، إن أمكن.
- اطرح الساعات المخصصة من قبل الرئيس التنفيذي للتدقيق للإشراف والأنشطة ذات الصلة (على سبيل المثال، التقدير بنسبة 80 بالمائة).
- اطرح الساعات الإنتاجية التي سيتم إنفاقها على المتطلبات المستمرة، والمراقبة، وتحليل البيانات، ومتابعة المهمات التي تم تنفيذها بالفعل، واحتياطي للطلبات المخصصة. ملاحظة: يعتبر بعض رؤساء التدقيق الداخلي عمليات المراقبة/التدقيق المستمر كجزء من الساعات الإنتاجية المتاحة.
- والباقي عبارة عن ساعات عمل متاحة (وقت التدقيق أو الوقت القابل للتحميل) ليتم إنفاقها في أداء المهام (بما في ذلك تقييمات المخاطر والتحليل والتقييم والتوثيق وإعداد التقارير) لالتزام بتنفيذ خطة التدقيق الداخلي القائمة على المخاطر.

5- تحضير خطة التدقيق الداخلي

5- تحضير خطة التدقيق الداخلي

قد تتضمن خطة التدقيق الداخلي المقترحة الأقسام التالية:

الملخص التنفيذي - يتضمن هذا الملخص النظرة العامة المختصرة للنقاط الرئيسية لأهم المخاطر، والتعاقدات المخططة والجدول الزمني الأساسي، وخطة التوظيف. وعادة ما تكون مكونة من صفحة وحدة.

السياسات والاجراءات - تعطي هذه النظرة العامة لمجلس الإدارة فهمًا للعناية المهنية الواجبة والشمولية لسياسات ونهج تخطيط التدقيق الداخلي، مع الأوصاف الأساسية للعمليات المستخدمة لإنشاء عالم التدقيق، وإجراء تقييم المخاطر، وتنسيق تغطية خدمات التوكيد، وتوظيف الموظفين. أي تغييرات في السياسات والإجراءات يفترض ان يتم تسليط الضوء عليها للمناقشة.

ملخص تقييم المخاطر - إن وصف عملية تقييم المخاطر ونتائجها يعزز فهم مجلس الإدارة لأولويات التدقيق الداخلي. قد يتضمن ذلك المعلومات التالية: الاستراتيجية التنظيمية، ومجالات التركيز الرئيسية، والمخاطر الرئيسية، واستراتيجيات خدمات التوكيد المرتبطة بها في خطة التدقيق. وقد يحتوي أيضا:

1- ملخص المخاطر. 2- تحليل (أو ملخص) مستويات المخاطر الكامنة و/أو المتبقية للوحدات القابلة للتدقيق. 3- درجات/تقييمات المخاطر للوحدات القابلة للتدقيق. 4- خريطة حرارية لعالم التدقيق بأكمله تشير إلى الأولويات والإدراج والاستثناءات.

5- تحضير خطة التدقيق الداخلي

نظرة عامة على المهمات في الخطة

1- قائمة بمهمات التدقيق المقترحة (وما إذا كانت مهمات التدقيق ذات طبيعة تأكيدية أو استشارية).

2- النطاقات والأهداف الأولية للمهمات.

3- التوقيت المبدئي والمدة (الجدول الزمني يوضح الربع الذي سيتم خلاله تنفيذ المهمة والمدة التي سيستغرقها إكمالها) .

تغطية التأكيد واستثناءاته

قد يتضمن هذا القسم خريطة التوكيد أو ملخصًا أو أداة أخرى لتوصيل تغطية خدمات التوكيد في مناطق المخاطر المهمة. تشير الاستثناءات إلى الوحدات القابلة للتدقيق أو مجالات المخاطر التي لم تتم معالجتها، وإذا لم تتم تغطية أي مجالات عالية المخاطر (على سبيل المثال، بسبب محدودية الموارد)، فقد يتضمن هذا القسم توصيات إلى مجلس الإدارة للحصول على تأكيد، مثل المصادر المشتركة أو الاستعانة بمصادر خارجية .

الأساس المنطقي للتضمين والاستثناءات

هذا التفسير مهم، خاصة إذا تم تجاوز تقييمات المخاطر أو تحديدات التكرار. قد تشمل الأسباب التغيير في تصنيف المخاطر، وطول الفترة الزمنية منذ آخر عملية تدقيق، والتغيير في الإدارة، والمزيد.

خطة الموارد

يحدد هذا القسم نوع وكمية الموارد اللازمة لتنفيذ الخطة. قد يتضمن الوصف عدد الموظفين المطلوبين لإكمال خطة التدقيق (القدرة)، وعدد موظفي الدعم اللازمين، وملخصًا لنتائج تقييم المهارات، وخطة عمل لمعالجة فجوات المهارات .

5- تحضير خطة التدقيق الداخلي

متطلبات الميزانية/الموازنة المالية

تتضمن الخطة ميزانية مالية لتغطية رواتب موظفي التدقيق الداخلي، بالإضافة إلى تكلفة الخدمات المشتركة و/أو الخارجية والأدوات (أي التكنولوجيا) والتدريب والنفقات الأخرى.

IPPF والمعايير ذات الصلة

الإشارات إلى التوافق مع IPPF والمعايير ذات الصلة تدعم المناقشة مع الإدارة العليا ومجلس الإدارة حول أهمية خطة التدقيق الداخلي القائمة على المخاطر بالإضافة إلى جوانب التخطيط الأخرى (مثل الاتصال والتنسيق والاعتماد).

الموافقة على الخطة

يجب على الإدارة العليا ومجلس الإدارة الموافقة على الخطة.

الأقسام الفرعية أو الخطط الفرعية

ضمن الخطة، يمكن دمج المخاطر من جميع المجالات القابلة للتدقيق في فئات المخاطر، مع تحديد تغطية خدمات التوكيد ذات الصلة بكل مجال خطر رئيسي (التشغيلية، المالية، الامتثال، تكنولوجيا المعلومات/الأمن السيبراني، الثقافة). الخدمات الاستشارية (مثل المبادرات الإستراتيجية والتقييم الأولي للنظام الجديد) المهام الخاصة المطلوبة (مثل التحقيقات) واالمتابعة (أي تتبع تنفيذ التوصيات).

مثال : خطة التدقيق الداخلي

- يوضح هذا المثال الأساسي لملخص خطة التدقيق الداخلي المناطق القابلة للتدقيق حسب الصفوف.
- يتم توسيع كل صف ليشمل معلومات المخاطر التي تشير إلى أولوية الوحدة القابلة للتدقيق والسنة والربع الذي سيتم فيه تنفيذ المهمة.
- الجداول الزمنية المقترحة للسنوات اللاحقة للعام الحالي عرضة للتغيير، اعتمادًا على تحديثات تقييمات المخاطر.
- يتم ترميز كل مربع يمثل المشاركة باللون، مع وسيلة إيضاح تشير إلى نوع المشاركة.
- تشير الأرقام الموجودة داخل كل مربع إلى عدد الساعات التي ستتطلبها المشاركة.
- يتم جمع الساعات في أسفل كل عمود، مما يشير بوضوح إجمالي الموارد المطلوبة. تُظهر الحسابات الموجزة أيضًا الساعات المطلوبة لمهام التدقيق الداخلي غير المرتبطة بارتباطات التدقيق.

Example: Internal audit plan summary

(Subject to Change Based on Risk Assessment)

Full audit | Limited audit

Current Risk Assessment				Year of Recent Reviews			Proposed Staff Hours Current Year			Proposed Schedule Current Year					Proposed Schedule Next Year					Proposed Schedule Two Years from				
Rank	Auditable Unit	Residual Risk Rating	Priority	Three Years Ago	Two Years Ago	Last Year	Service Provider	IAA	Total	Q1	Q2	Q3	Q4	Total Annual Effort	Q1	Q2	Q3	Q4	Total Annual Effort	Q1	Q2	Q3	Q4	Total Annual Effort
1	Auditable unit 6	4.5	High	✓	✓		15	20	35	20	15					5	15							
2	Auditable unit 3	4.4	High	✓		✓	20	20	40	20	20												25	
3	Auditable unit 7	4.2	High	✓	✓		20	20	40		20	20			15	5								
4	Auditable unit 5	3.1	Medium	✓		✓		30	30			20	10									25		
5	Auditable unit 11	3.0	Medium		✓											30	10							
6	Auditable unit 8	2.8	Medium		✓										5	10								
7	Auditable unit 9	2.6	Medium		✓												15	15						
8	Auditable unit 1	2.2	Medium		✓											25	10							
9	Auditable unit 2	2.1	Medium			✓														10	20			
10	Auditable unit 4	1.2	Low			✓																15	5	
11	Auditable unit 10	1.0	Low		✓																	15	5	
							55	90	145	40	55	40	10	145	20	75	50	15	160	10	20	55	35	120
Nonauditable Areas																								
1	Preparation for Audit & Risk Committee Meetings							30	30	9	7	7	7		9	7	7	7		9	7	7	7	
2	Updating Risk Assessment and Internal Audit Plan							50	50		15	15	20			15	15	20			15	15	20	
3	Consulting Assignments and Other Projects							15	15	10	5				10	5				10	5			
4	Follow-up Audits							80	80	20	20	20	20		20	20	20	20		20	20	20	20	
5	Staff Training							30	30	10	10	10			10	10	10			10	10	10		
6	Strategic Initiatives						20	45	65	20	20	0	25		10	10	10	10		10	10	10	10	
7	Engagements Carried Forward							10	10	10					10					10				
8	Quality Assurance							15	15				15					15					15	
Total Effort Required in a Year							75	365	440	119	132	92	97	440	89	142	112	87	430	79	87	117	107	390

6- اقتراح الخطة والتماس ردود الفعل

6- اقتراح الخطة والتماس ردود الفعل

- بمجرد وضع خطة مسودة قائمة على المخاطر، يناقش الرئيس التنفيذي للتدقيق أو مدير التدقيق الداخلي الخطة مع الإدارة العليا قبل إضفاء الطابع الرسمي عليها لعرضها على لجنة التدقيق و/أو مجلس الإدارة للاعتماد.
- عادةً ما ينفذ الرئيس التنفيذي للتدقيق عملية قياسية لهذه المراجعة المتبادلة وقد يجتمع مع كل مدير كبير على حدة .
- ويجوز للرئيس التنفيذي للتدقيق أيضًا التشاور مع لجان محددة، مثل تلك المسؤولة عن إدارة المخاطر والامتثال والأخلاقيات وغيرها.
- يمكن أيضًا جدولة الاجتماعات مع مالكي العمليات الفردية لمناقشة النطاق الأولي وتوقيت التعاقدات.
- في المناقشات، يجب على الرئيس التنفيذي للتدقيق توصيل نتائج تقييم المخاطر، وكيف يمكن أن تؤثر المخاطر الكبيرة على أهداف المنظمة، وكيف تساعد النتائج في تحديد خطة عمليات التدقيق.

6- اقتراح الخطة والتماس ردود الفعل

- يجب على الرئيس التنفيذي للتدقيق أيضًا أن يصف تخصيص الموارد، مثل المجالات التي سيوفر فيها نشاط التدقيق الداخلي الضمانات وتلك التي سيعتمد فيها على مقدمي خدمات التأكيد الآخرين.
- خلال الاجتماعات، يمكن للرئيس التنفيذي للتدقيق معالجة أي مخاوف للإدارة العليا. قد يتم تغيير الخطة بناءً على المناقشات المتعلقة بالقدرة على تحمل المخاطر ونطاق و/أو توقيت تغطية عمليات التوكيد (استنادًا إلى التنسيق مع مقدمي الخدمة الآخرين). ويفكرالرئيس التنفيذي للتدقيق والإدارة العليا معًا في أسئلة مثل :

1. هل تمت دراسة جميع المخاطر والوحدات القابلة للتدقيق بشكل شامل؟
2. هل هناك أي تغييرات قادمة لم نأخذها في الاعتبار بشكل منهجي - على سبيل المثال، عمليات الاستحواذ أو الدمج أو ترقيات النظام أو الموردين الخارجيين أو تنفيذ البرامج؟
3. كيف ترتبط مهمات التدقيق الواردة في الخطة بأهداف المنظمة وأهم المخاطر؟
4. كيف تضيف التعاقدات قيمة للإدارة العليا والمنظمة؟
5. هل يعتبرتنسيق تغطية خدمات التوكيد والجدول الزمني/توقيت التعاقدات منطقيًا؟ إذا لم يتم تلبية أي طلبات، لماذا لا؟

6- اقتراح الخطة والتماس ردود الفعل

قيود تغطية خدمات التوكيد المتعلقة بموازنة الخطة

- عند توصيل خطط نشاط التدقيق الداخلي ومتطلبات الموارد، يجب على الرئيس التنفيذي للتدقيق التعبير عن العلاقة بين المخاطر التي تواجه المنظمة والميزانية/الموازنة المتاحة لتغطية الضمان.
- يجب على الرئيس التنفيذي للتدقيق لفت الانتباه إلى المناطق عالية المخاطر التي لن تتمتع بتغطية ضمانية كافية ويجب أن يكون مستعدًا لطلب موارد إضافية إذا لزم الأمر.

7-وضع اللمسات الأخيرة على الخطة

7- وضع اللمسات الأخيرة على الخطة

العرض على لجنة التدقيق

- يقوم الرئيس التنفيذي للتدقيق بتقييم تعليقات الإدارة العليا ويدمج المعلومات ذات الصلة للتأكد من أن الخطة تعكس أولويات المنظمة بشكل مناسب، وأن الإدارة تدعم تنفيذ الخطة.
- يتم تقديم الخطة المعدلة إلى لجنة التدقيق لإجراء مراجعة إضافية.
- قد تقترح لجنة التدقيق تعديلات على الخطة بناءً على رؤيتها لمدى تقبل المنظمة للمخاطر.
- كما يمنح الاجتماع الرئيس التنفيذي للتدقيق فرصة لشرح الميزانية وعلاقتها بتغطية التوكيد، مع الإشارة إلى أي فجوات كبيرة في التغطية.

7- وضع اللمسات الأخيرة على الخطة

العرض على مجلس الادارة

- للتواصل مع مجلس الإدارة، يقوم الرئيس التنفيذي للتدقيق عادةً بإنشاء عرض تقديمي يلخص المهمات في الخطة، ويشرح تقييم المخاطر وراء الاختيارات، ويعبر عن قيمة الخدمات التوكيدية والمشورة المستقلة والموضوعية المقدمة من نشاط التدقيق الداخلي.
- يجوز لرئيس لجنة التدقيق تقديم ملخص المعلومات إلى مجلس الإدارة للموافقة النهائية.
- بمجرد موافقة الإدارة العليا ومجلس الإدارة على الخطة رسميًا، تتلقى جميع مجالات العمل المتأثرة في المؤسسة عادةً نسخة.

7- وضع اللمسات الأخيرة على الخطة

التواصل المستمر

- في بعض الشركات، يتواصل الرئيس التنفيذي للتدقيق بشكل ربع سنوي من خلال تقرير رسمي.
- قد يؤثر توقيت التقارير المقدمة إلى الإدارة العليا ومجلس الإدارة (لجنة التدقيق) على كيفية إدراك مجموعتي أصحاب المصلحة لنشاط التدقيق الداخلي.
- قد يؤدي تقديم الكثير من المعلومات في وقت واحد (على سبيل المثال، نهاية الربع) إلى تقليل تقبل أصحاب المصلحة لنشاط التدقيق الداخلي.
- يجب على المدققين الداخليين الحرص على التواصل بانتظام مع الإدارة العليا وإعداد أي تغييرات على خطة التدقيق الداخلي مع إشعار مسبق كاف لإتاحة الفرصة للمناقشة.

7- وضع اللمسات الأخيرة على الخطة

التواصل مع التغييرات المقترحة

اذا تغيرت خطة التدقيق الداخلي و/أو متطلبات الموارد بشكل كبير، فيجب على الرئيس التنفيذي للتدقيق إبلاغ الإدارة العليا ومجلس الإدارة بهذه التغييرات والحصول على موافقتهم، وفقًا لمعيار 2020 - الاتصال والموافقة.

حتى عندما تكون التعديلات على الخطة بسيطة، فإنها قد توفر فرصًا للأطراف الثلاثة لمناقشة تصوراتهم للمخاطر، لتحسين دقة المعلومات المشتركة، ومواءمة أولويات إدارة المخاطر الخاصة بهم.

يقوم بعض الرؤساء التنفيذيين للتدقيق الداخلي أو مديري التدقيق الداخلي بمراجعة خطة التدقيق الداخلي الخاصة بهم شهريًا. ويقومون بتقييم ما إذا كانت أي تغييرات في ملف تعريف المخاطر تضمن استبدال المهمات المجدولة وما إذا كانت الموارد الكافية متاحة لإضافة مهمات جديدة إلى الخطة.

على الرغم من أن إبلاغ هذه التغييرات بشكل ربع سنوي ليس مطلوبًا، إلا أن العديد من رؤساء التدقيق الداخلي يختارون هذا الجدول من أجل الاتساق. قد يتضمن الحوار طلب الموارد.

يفكر المدققون الداخليون في أسئلة مثل: "هل سيكون التغيير في خطة التدقيق حدثًا فريدًا، أم أنه سيتطلب تعديلًا طويل المدى للموازنة؟" لاستيعاب التعاقدات الجديدة ضمن الموازنة الحالية، قد يتعين على نشاط التدقيق الداخلي حذف شيء ما من الخطة. قد يقدم الرئيس التنفيذي للتدقيق أو مدير التدقيق الداخلي دراسة جدوى للتغييرات المرغوبة أو قد يطلب من الإدارة العليا ومجلس الإدارة تحديد المشروع الذي يرغبون في إلغائه لتحرير الموارد اللازمة للتغيير.

7- وضع اللمسات الأخيرة على الخطة

أسباب تعديل خطة التدقيق

تشمل التغييرات التي قد تغير ملف تعريف المخاطر في المنظمة (على سبيل المثال لا الحصر):

- حيازة أو بيع وحدة أعمال أو أصل.
- التغيير في عضوية مجلس الإدارة أو الملكية التنظيمية أو القيادة.
- التغييرات في القوانين أو اللوائح أو معايير الصناعة، والتي قد تؤدي إلى مخاطر امتثال جديدة.
- التغييرات في المبادرات الإستراتيجية، بما في ذلك البحث عن فرص جديدة.
- اكتشاف مؤشرات المخاطر غير المتوقعة أثناء عمليات التدقيق الداخلي أو الخارجي.
- التغيرات الخارجية، مثل التطورات السياسية أو البيئية.
- تنفيذ الأنظمة الجديدة .

هل التدقيق الداخلي القائم على المخاطر يقتصر فقط على التخطيط؟

- بالطبع لا

علينا التعامل مع المخاطر في جميع مراحل عملنا.

أثناء العمل الميداني

تصميم برنامج التدقيق للتعامل مع المخاطر المحددة يتضمن:

- تحديد أهداف الاختبار.
- التعرف على ما إذا كان هناك حاجة لاستخدام متخصصين.
- تحديد متى يجب التعامل مع المخاطر (خلال الفترة المؤقتة/نهاية العام).
- تحديد ما إذا كان يمكن استخدام الأدلة من التدقيق السابق.
- فهم ما إذا تم تقييم مناطق الامتثال الأخرى المرتبطة بالمنطقة.
- التحقق مما إذا كانت هناك أهداف ذات صلة للاختبار.
- تحديد نوع الاختبار للمجالات ذات المخاطر العادية وتلك ذات المخاطر الكبيرة.
- تحديد مدى الاعتماد على نتائج الاختبار.
- تحديد الإجراءات الدورية الإضافية التي يجب اتباعها إذا تم التعرف على مشكلات أو قضايا أثناء الاختبار.

أثناء إعداد التقارير

- تقييم الأدلة التي تم الحصول عليها لتحديد ما إذا كان التقييم الأولي للمخاطر لا يزال مناسبًا.
- تحديد أهمية تأثير المخاطر بناءً على تحمل الإدارة للمخاطر.
- تحديد نتيجة الكفاءة والفعالية للعمليات

يوفر نهج التدقيق القائم على المخاطر وسيلة لإجراء التدقيق بأقصى كفاءة وفعالية ممكنة، مما يعود بالفائدة على فريق التدقيق والكيان.

يجب أن تكون المخاطر التي تم الإبلاغ عنها إلى لجنة التدقيق تلك التي يجب اتخاذ إجراءات سريعة وإصلاحية بحيث يمكن الحفاظ على عملية مالية، وامتثال، وتنظيمية، أو تشغيلية قوية.

تأسيس دليل للتحمل في مجال المخاطر مع مجلس الإدارة والإدارة يمكن أن يساعد في تحديد المسائل التي يجب الإبلاغ عنها إلى لجنة التدقيق وتلك التي يكفي الإبلاغ عنها فقط للإدارة. بالنسبة للكثيرين، يصعب تطوير مصفوفات التحمل. ومع ذلك، عند تنفيذها بشكل صحيح، يمكن أن تقدم دليلًا قويًا للمدقق الداخلي في تقدير التعرض للمخاطر.

تحمل المخاطر

- تحمّل المخاطر هو مقدار المخاطرة التي يمكن للمؤسسة تحملها.
- على الرغم من أنها تُستخدم في كثير من الأحيان كمرادف لتقبل المخاطر،إلا أنها مختلفة تمامًا.
- تعتبر الحدود التي يجب أن ترشد العاملين عند النظر في المخاطر. يجب على العاملين أن يفهموا المستويات التي لا ينبغي تجاوزها أو تلك الحدود التي إذا تم تجاوزها تتطلب تدابير إصلاحية إضافية ومراقبة. هناك العديد من الأدلة على أمثلة تحمل المخاطر على الإنترنت. المفتاح هو تحديد "العوامل" المهمة لمؤسستك ووضع مقياس للقياس بشكل صحيح.

مثال : تحمل المخاطر

		Technical Performance	Cost	Schedule
5 Severe	A risk event that, if it occurs, will have a severe impact on achieving desired results, to the extent that one or more of its critical outcome objectives will not be achieved	Performance unacceptable; Does not meet a KPP requirement.	Program budget impacted by greater than $20 million.	Key program event or milestone delayed by more than 3 months.
4 Significant	A risk event that, if it occurs, will have a significant impact on achieving desired results, to the extent that one or more stated outcome objectives will fall below acceptable levels.	Performance unacceptable; Significant changes required; Does not meet a Threshold requirement.	Program budget impacted by greater than $10 million but less than $20 million.	Increases critical path schedule by 2-3 months.
3 Moderate	A risk event that, if it occurs, will have a moderate impact on achieving desired results, to the extent that one or more stated outcome objectives will fall well below goals but above minimum acceptable levels.	Performance below goal; Moderate changes required; Does not meet a Threshold requirement.	Program budget impacted by greater that $2 million, but less than $10 million. Does not require significant use of program cost and/or schedule reserves	Moderate schedule slip. 1 – 2 month schedule slip.
2 Minor	A risk event that, if it occurs, will have a minor impact on achieving desired results, to the extent that one or more stated outcome objectives will fall below goals but well above minimum acceptable levels.	Performance below goal but within acceptable limits; No changes required; Does not meet an objective requirement.	Program budget impacted by less than $2 million; Development or production cost goals exceeded by 1-5%.	Minor schedule slip. Non-critical path activities late; impact to critical path up to 1 month slip.
1 Minimal	A risk event that, if it occurs, will have little or no impact on achieving outcome objectives.	Requires minor performance trades within the threshold – objective range; No impact on program success.	Program budget not affected; Cost increase can be managed within plan.	Schedule not affected; Schedule adjustments can be managed within plan. Able to meet key milestones with no schedule float

شكرا لحضوركم