

وزارة التعليم العالي والبحث العلمي
جامعة عبد الحميد بن باديس – مستغانم –
كلية العلوم الاقتصادية، التجارية وعلوم التسيير
قسم العلوم المالية والمحاسبة



مطبوعة بيداغوجية موجهة لطلبة السنة الأولى ماستر
تخصص: التكنولوجيا المالية

عنوان المطبوعة

حوكمة تكنولوجيا المعلومات

من إعداد:
الأستاذة دراعو اسمهان

السنة الجامعية:

2027/2026

الصفحة	العنوان	المحور
05	مقدمة	
09	أولاً: مدخل إلى حوكمة الشركات	
09	تمهيد	
09	1. مفهوم حوكمة الشركات	
10	2. الفرق بين الحوكمة والادارة	
11	3. نشأة وتطور حوكمة الشركات	
12	4. أهمية حوكمة المؤسسات	
13	5. النظريات المفسرة لحوكمة المؤسسات	
15	6. مبادئ الحوكمة	
17	7. آليات حوكمة الشركات	
18	8. النماذج الدولية لحوكمة الشركات	
19	9. حوكمة الشركات في السياق العربي	
20	10. حوكمة الشركات في الجزائر	
20	11. الحوكمة والاستراتيجية	
20	12. الحوكمة وإدارة المخاطر	
21	13. الحوكمة والاستدامة	
21	14. حدود حوكمة الشركات	
22	ثانياً: مدخل إلى تكنولوجيا المعلومات	
22	تمهيد	
22	1. مفهوم تكنولوجيا المعلومات	المحور الأول
23	2. التطور التاريخي لتكنولوجيا المعلومات	مدخل إلى حوكمة
24	3. مكونات تكنولوجيا المعلومات	الشركات وتكنولوجيا
26	4. تكنولوجيا المعلومات ونظم المعلومات	المعلومات
26	5. أنواع نظم المعلومات المرتبطة بتكنولوجيا المعلومات	
28	6. البنية التحتية لتكنولوجيا المعلومات	
28	7. تكنولوجيا المعلومات والميزة التنافسية	
29	8. تكنولوجيا المعلومات والتحول الرقمي	
30	9. البيانات، المعلومات والمعرفة في المؤسسة	
30	10. حماية المعلومات والأمن السيبراني	
31	11. الحوكمة الرقمية وحوكمة تكنولوجيا المعلومات	
31	12. الآثار التنظيمية لتكنولوجيا المعلومات	
32	13. تكنولوجيا المعلومات والأخلاقيات	
32	14. تحديات تكنولوجيا المعلومات في المؤسسات	
33	15. خصائص تكنولوجيا المعلومات	
33	16. فوائد استخدام تكنولوجيا المعلومات	
34	17. تطور دور تكنولوجيا المعلومات من التشغيلية الى الاستراتيجية	
34	18. مساهمة تكنولوجيا المعلومات في تحسين العمل الإداري	
35	خاتمة	
36	أسئلة المناقشة	
37	تمهيد	
37	1. مفهوم مخاطر تكنولوجيا المعلومات	المحور الثاني
38	2. الفرق بين الخطر، التهديد، نقطة الضعف، والحادث	مخاطر تكنولوجيا
39	3. خصائص مخاطر تكنولوجيا المعلومات	المعلومات
40	4. تصنيف مخاطر تكنولوجيا المعلومات	
43	5. مصادر مخاطر تكنولوجيا المعلومات	
45	6. أثر مخاطر تكنولوجيا المعلومات على المؤسسة	

47	7. ادارة مخاطر تكنولوجيا المعلومات	
48	8. مصفوفة المخاطر Risk Matrix	
49	9. الأمن السيبراني كمدخل التحكم في المخاطر	
51	10. الرقابة الداخلية على تكنولوجيا المعلومات	
51	11. مخاطر جودة البيانات	
52	12. مخاطر التحول الرقمي	
53	13. مخاطر الذكاء الاصطناعي والأنظمة الخوارزمية	
53	14. مخاطر الخصوصية وحماية البيانات	
54	15. مخاطر الاستعانة بالمصادر الخارجية	
54	16. ادارة الحوادث المعلوماتية	
55	17. استمرارية الاعمال و التعافي من الحوادث	
55	18. الثقافة الامنية داخل المؤسسة	
56	19. منهجية مقترحة لتحليل مخاطر تكنولوجيا المعلومات في المؤسسة	
57	خاتمة	
58	أسئلة المناقشة	
59	تمهيد	
59	1. مفهوم حوكمة تكنولوجيا المعلومات	
60	2. الفرق بين ادارة تكنولوجيا المعلومات وحوكمة تكنولوجيا المعلومات	
61	3. نشأة وتطور حوكمة تكنولوجيا المعلومات	
62	4. أهمية حوكمة تكنولوجيا المعلومات	
65	5. المبادئ الأساسية لحوكمة تكنولوجيا المعلومات	
66	6. أبعاد حوكمة تكنولوجيا المعلومات	
67	7. علاقة حوكمة تكنولوجيا المعلومات بحوكمة الشركات	
69	8. حوكمة تكنولوجيا المعلومات والتحول الرقمي	
70	9. حوكمة تكنولوجيا المعلومات وادارة المخاطر	
70	10. آليات تطبيق حوكمة تكنولوجيا المعلومات	
71	11. مؤشرات نضج حوكمة تكنولوجيا المعلومات	
72	12. تحديات حوكمة تكنولوجيا المعلومات في البلدان العربية	
73	13. خصوصية حوكمة تكنولوجيا المعلومات في السياق الجزائري	
74	14. نموذج مفاهيمي مقترح لحوكمة تكنولوجيا المعلومات	
74	خاتمة	
75	أسئلة المناقشة	
76		
77	تمهيد	
77	1. الركيزة الأولى: الموازنة الاستراتيجية لتكنولوجيا المعلومات	
79	2. الركيزة الثانية: خلق القيمة من تكنولوجيا المعلومات	
81	3. الركيزة الثالثة: ادارة المخاطر المرتبطة بتكنولوجيا المعلومات	
83	4. الركيزة الرابعة: ادارة موارد تكنولوجيا المعلومات	
85	5. الركيزة الخامسة: قياس أداء تكنولوجيا المعلومات والمساءلة	
86	6. الركيزة السادسة: الامتثال والرقابة الداخلية	
87	7. الركيزة السابعة: حوكمة البيانات والمعلومات	
88	8. الركيزة الثامنة: القيادة الرقمية والثقافة التنظيمية	
89	9. التكامل بين الركائز	
89	10. نموذج مقترح لركائز حوكمة تكنولوجيا المعلومات	
89	خاتمة	
91	أسئلة المناقشة	
92	تمهيد	
92	1. مفهوم القرار في حوكمة تكنولوجيا المعلومات	
93	2. الفرق بين القرار التقني والقرار الحوكماتي	
93	3. القرارات المرتبطة بحوكمة تكنولوجيا المعلومات	

104	4. المسؤولين عن القرارات في حوكمة تكنولوجيا المعلومات	المعلومات "القرارات
105	5. مصفوفة مقترحة للقرارات المرتبطة بحوكمة تكنولوجيا المعلومات	المرتبطة بها"
105	6. منهجية اتخاذ القرار في حوكمة تكنولوجيا المعلومات	
106	خاتمة	
107	أسئلة المناقشة	
108	تمهيد	
108	1. مفهوم COBIT ونشأته	
109	2. أهمية COBIT في حوكمة تكنولوجيا المعلومات	
110	3. الفرق بين الحوكمة و الإدارة في COBIT	
111	4. المبادئ العامة لنظام COBIT	
112	5. مكونات نظام الحوكمة وفق إطار COBIT	
113	6. مجالات COBIT الأساسية	
116	7. أهداف الحوكمة والإدارة في COBIT	المحور السادس
116	8. عوامل تصميم نظام الحوكمة في COBIT	حوكمة تكنولوجيا
117	9. نموذج النضج والقدرة في نظام COBIT	المعلومات "نظام"
118	10. COBIT وعلاقته بالأطر والمعايير الأخرى	
118	11. خطوات تصنيف COBIT داخل المؤسسة	
119	12. تطبيق نظام COBIT في المؤسسات الجزائرية	
120	13. مزايا نظام COBIT	
121	14. حدود نظام COBIT	
122	15. نموذج مقترح مبسط لنظام COBIT	
122	خاتمة	
124	أسئلة المناقشة	
125	تمهيد	
125	1. مفهوم حوكمة تكنولوجيا المعلومات وفق ISO	
126	2. مكانة ISO 38500 في حوكمة تكنولوجيا المعلومات	
127	3. الفرق بين حوكمة تكنولوجيا المعلومات وإدارة تكنولوجيا المعلومات من منظور معيار ISO	
128	4. مبادئ حوكمة تكنولوجيا المعلومات وفق ISO 38500	المحور السابع
129	5. نموذج التقييم، التوجيه، والمراقبة وفقا لـ ISO 38500	حوكمة تكنولوجيا
130	6. علاقة معيار ISO 38500 بباقي معايير ISO الداعمة	المعلومات وفق معايير
131	7. تطبيق حوكمة تكنولوجيا المعلومات نظام ISO داخل المؤسسة	ISO
133	8. مؤشرات تقييم حوكمة تكنولوجيا المعلومات وفق نظام ISO	
134	9. مزايا حوكمة تكنولوجيا المعلومات وفق نظام ISO	
135	10. حدود تطبيق معايير ISO في حوكمة تكنولوجيا المعلومات	
135	11. حوكمة تكنولوجيا المعلومات وفق ISO في المؤسسات الجزائرية	
136	12. نموذج مقترح لحوكمة تكنولوجيا المعلومات وفق نظام ISO	
137	خاتمة	
139	أسئلة المناقشة	
140	تمهيد	
140	1. مفهوم ITIL ومكانته في حوكمة تكنولوجيا المعلومات	
141	2. تطور ITIL من إدارة العمليات الى إدارة المنتجات والخدمات الرقمية	
141	3. علاقة ITIL بحوكمة تكنولوجيا المعلومات	المحور الثامن
142	4. المفاهيم الأساسية في ITIL	حوكمة تكنولوجيا
143	5. نظام قيمة الخدمة في ITIL	المعلومات وفق معايير
144	6. الأبعاد الأربعة لإدارة الخدمات في ITIL	ITIB
144	7. أهم ممارسات ITIL في دعم حوكمة تكنولوجيا المعلومات	
146	8. ITIL كأداة لتحسين جودة الخدمات الرقمية	
147	9. علاقة بين ITIL و ISO 20001	
147	10. العلاقة بين ITIL و COBIT	

147	11. تطبيق بين ITIL و COBIT	
148	12. ITIL والتحول الرقمي	
148	13. تحديات تطبيق ITIL في المؤسسات الجزائرية	
149	14. مزايا معيار ITIL	
149	15. حدود ITIL	
150	خاتمة	
151	أسئلة المناقشة	
152	خاتمة	
156	المراجع	

مقدمة

تعتبر حكم التكنولوجيا المعلومات من الموضوعات الحديثة في علوم الإدارة وتزايدت أهميتها بصورة واضحة مع التحول الرقمي الذي عرفته المؤسسات المعاصرة لأن تكنولوجيا المعلومات أصبحت عنصراً بينيوي في نشاط المؤسسة، وليست مجرد أداة تقنية مساعدة. فهي تؤثر في التخطيط، اتخاذ القرار، الرقابة، إدارة المخاطر، جودة الخدمات، العلاقة مع الزبائن، أمن البيانات، وخلق القيمة التنظيمية. فأصبح سؤال مطروح داخل المؤسسة ليس كيف تقتلني المؤسسة التكنولوجية؟ ولكن كيف يتم توجيه التكنولوجيا ومراقبتها بطريقة تضمن أنها تخدم الأهداف الاستراتيجية للمؤسسة؟

ومعظم الأدبيات أوضحت أن فعالية التكنولوجيا لا تتحقق بمجرد توفر الأجهزة والبرمجيات ولكن من خلال تكامل ولها مع العنصر البشري، الإجراءات التنظيمية، تدفقات المعلومات وأساليب اتخاذ القرار. فقد أكد (ياسين، 2005) إن نظم المعلومات الإدارية لا تعد مجرد أدوات تقنية بل هي نظم موجهة لدعم وظائف الإدارة الأساسية خاصة التخطيط، التنظيم، الرقابة واتخاذ القرار. كما يرى (سالي، 2006) أن المعلومات داخل المؤسسة تحتاج إلى تنظيم متكامل للموارد التقنية، البشرية الإجرائية، بطريقة تسمح بتحويل البيانات إلى معلومات نافعة تدعم الأداء المؤسسي. وعليه فإن حوكمة التكنولوجيا المعلومات تمثل مرحلة متقدمة في التفكير الإداري، لأنها تكتفي بتسيير الأنظمة، بل تهتم بكيفية توجيهها ومساءلتها وربطها الإستراتيجية. أصبحت التكنولوجيا مورداً استراتيجياً يخضع لمنطق الحوكمة كما تخضع الموارد المالية، البشرية والمادية حيث أن المؤسسة يمكن أن تستثمر مبالغ كبيرة في الأنظمة الرقمية، قواعد البيانات، التطبيقات، الحوسبة السحابية، الأمن السيبراني والذكاء الاصطناعي دون أن تحقق قيمة فعلية إذا كانت هذه الاستثمارات غير مرتبطة برؤية استراتيجية واضحة. وهذا ما أكد عليه (الطائي، العابدي ؛ 2009) أن نظم المعلومات لا تحقق فعاليتها إلا عندما تكون منسجمة مع الهيكل التنظيمي، احتياجات المستخدمين، وطبيعة القرار الإداري. وهذا يعني أن فشل المشاريع الرقمية لا يكون دائماً خلل تقني ولكن قد يكون ناتج عن ضعف الحوكمة، أو غياب التنسيق، أو ضعف القيادة، أو سوء تحديد المسؤوليات. تعتبر حوكمة تكنولوجيا المعلومات مجموعة الهياكل والعمليات والآليات التي تضمن توجيه ومراقبة استخدام تكنولوجيا المعلومات داخل المؤسسة، بما يحقق المواءمة مع الأهداف الاستراتيجية وخلق القيمة وإدارة المخاطر وضمان الامتثال وترشيد استعمال الموارد الرقمية.

ويعتبر (Weill, Ross, 2004) أن حوكمة تكنولوجيا المعلومات تتمثل في تحديد حقوق القرار وأطر المساءلة التي تشجع السلوك المرغوب في استعمال التكنولوجيا داخل المؤسسة. كما أكد (De Haes, Van Grembergen, 2015) أن جوهر حوكمة تكنولوجيا المعلومات يتمثل في تحقيق المواءمة بين الأعمال والتكنولوجيا وضمان خلق القيمة من الاستثمارات الرقمية، مع التحكم في المخاطر وقياس الأداء. وتزايدت الحاجة إلى حوكمة تكنولوجيا المعلومات بتزايد درجة الاعتماد على الأنظمة الرقمية في المؤسسة، حيث أصبحت البيانات أصلاً استراتيجياً وأصبحت الخدمات الإلكترونية واجهة أساسية للتفاعل مع الزبائن والمواطنين، كما أصبحت القرارات الإدارية تعتمد بصورة أكبر على نظم التحليل ولوحات القيادة والذكاء الاصطناعي. وقد أشار (ابو نصر ، 2017) أن إدارة المعرفة، تداولها، حمايتها، وتوظيفها في تحسين الأداء. وعليه فإن حوكمة تكنولوجيا المعلومات لا يمكن اختزالها في الجانب التقني فقط لأنها تشمل كذلك الجانب المعرفي، الثقافي، الأخلاقي، الرقابي، الاستراتيجي.

وقد ارتبطت حوكمة تكنولوجيا المعلومات بتطور نظم المعلومات داخل المؤسسة، ففي البداية كانت التكنولوجيا تستخدم أساساً في العمليات الروتينية مثل: المحاسبة، المخزون، الرواتب، الفوترة. ثم تطورت إلى دعم القرار من خلال نظم المعلومات الإدارية ونظم دعم القرار. وظهور الإنترنت وتطور التجارة الإلكترونية، الحوسبة السحابية، البيانات الضخمة الذكاء الاصطناعي، أصبحت التكنولوجيا تؤثر في نموذج الأعمال بحد ذاته.

وحسب (Laudon, Laudon 2022) فإن نظم المعلومات الحديثة أصبحت عنصر حاسماً في إدارة المؤسسة الرقمية، لأنها تربط بين التكنولوجيا، الإدارة، التنظيم والبيئة التنافسية، وعليه أصبحت إدارة تكنولوجيا المعلومات غير كافية وأصبح من الضروري تبني حوكمة تضمن أن القرارات الرقمية تخضع لتوجيه، المراقبة، والمساءلة.

وتظهر أهمية حوكمة تكنولوجيا المعلومات في عدة أبعاد، يتمثل البعد الأول في المواءمة الاستراتيجية أي ضمن أن التكنولوجيا تخدم أهداف المؤسسة ولا تعمل بمعزل عنها، أما البعد الثاني فيتمثل في خلق القيمة، حيث يجب على تكنولوجيا المعلومات تحسين الأداء، تقليل التكاليف، رفع جودة الخدمات، تحسين القرار أو دعم الابتكار. أما البعد الثالث فيتعلق بإدارة المخاطر خاصة مخاطر الأمن السيبراني، فقدان البيانات، توقف الأنظمة، ضعف جودة المعلومات، و الامتثال القانوني. في حين البعد الرابع يرتبط بإدارة الموارد الرقمية مثل البنية التحتية، قواعد البيانات، التطبيقات، الكفاءات البشرية و الميزانيات. أما البعد

الخامس فيتمثل في قياس الأداء والمساءلة من خلال مؤشرات واضحة تسمح بتقييم ماذا فعالية التكنولوجيا في تحقيق أهداف المؤسسة.

تعد الأطر المرجعية الدولية مثل : ISO ، COBIT ، ITIL، من أهم الأدوات التي تساعد المؤسسات على تنظيم حوكمة تكنولوجيا المعلومات. حيث يركز إطار COBIT على حوكمة وإدارة معلومات وتكنولوجيا المؤسسة من خلال ربط أهداف الأعمال بأهداف تكنولوجيا المعلومات، تنظيم العمليات، قياس الأداء، وإدارة المخاطر. أما معيار ISO 38500 فيخدم المبادئ العامة لحوكمة المؤسسة لتكنولوجيا المعلومات، وذلك من خلال التركيز على التقييم، التوجيه والمراقبة. في حين يركز ITIL على إدارة خدمات تكنولوجيا المعلومات، من حيث تصميم الخدمات، تشغيلها، دعمها، وتحسينها المستمر. كما أن هذه الأطر لا تتنافس فيما بينها ولكن تتكامل، حيث COBIT يقدم منظورا حوكميا شاملا أما ISO فيقدم مرجعية معيارية، في حين ITIL يعزز البعد الخدماتي والتشغيلي.

في الجزائر، تزايد الاهتمام بحوكمة تكنولوجيا المعلومات بسبب التحولات الرقمية التي تعرفها الإدارة والمؤسسات نحو الرقمنة والإدارة الإلكترونية. غير أن هذه التحولات تواجه العديد من التحديات مثل الثقافة الرقمية، نقص الكفاءات المتخصصة، غياب مؤشرات الأداء، مقاومة التغيير وضعف توثيق. حيث أشار (ياسين، 2018) أن الإدارة الإلكترونية في البيئة العربية لا يمكن أن تنجح بإدخال الحاسوب ورقمنة الإجراءات فقط، بل يجب أن ترتبط بإصلاح إداري، تنظيمي، وثقافي شامل. وهذا ما يجعل من حوكمة تكنولوجيا المعلومات مدخلا ضروريا لفهم التحول الرقمي في هذه المؤسسات.

كما تطرح حوكمة تكنولوجيا المعلومات قضية أخلاقية وقانونية هامة، لأن الكميات الكبيرة من البيانات التي تجمعها المؤسسة حول الزبائن، المستخدمين، العمال ووردين يفرض عليها مسؤولية حماية الخصوصية، وضمان الاستخدام المشروع والعادل للبيانات. وعليه فإن الحوكمة الرقمية لا تهتم فقط بالكفاءة ولكن بتقوى والمسؤولية والشرعية أيضا. تمثل دراسة حوكمة تكنولوجيا المعلومات مجالا أساسيا في علوم الإدارة، نظم المعلومات، المالية، التدقيق، إدارة المخاطر، والحوكمة. لأنها تسمح بفهم كيفية اتخاذ القرارات الرقمية داخل المؤسسة، وكيفية تقييم المشاريع التكنولوجية، وكيفية ضبط المخاطر السيبرانية وكيفية بناء مؤشرات الأداء الرقمي وكيفية الربط بين التكنولوجيا والاستراتيجية، كما تمنح أدوات تحليلية

لفهم دور الإدارة العليا، إدارة تكنولوجيا المعلومات، المستخدمين، المدققين، الموردين وأصحاب المصالح.

وعليه فإنه حوكمة تكنولوجيا المعلومات ليست مجرد مجال تقني متخصص ولكن حقل علمي وإداري ذو أبعاد عديدة يجمع بين الإدارة، الاستراتيجية، نظم المعلومات، الرقابة، الأمن، المخاطر، تحول الرقمي، الأخلاقية والقانون. وهي شرطا أساسيا لبناء مؤسسة رقمية فعالة، آمنة، شفافة، قادرة على خلق القيمة والاستجابة لمتطلبات البيئة المعاصرة.

وعليه فإن هذه المطبوعة البيداغوجية تسعى إلى تقديم معالجة علمية وبيداغوجية لموضوع حوكمة تكنولوجيا المعلومات من خلال مفاهيمها، مخاطرها، ركائزها، قراراتها، أطرها المرجعية الدولية. مع التركيز على قابلية تطبيقها في الجزائر، فالرهان الرئيسي لا يتمثل فقط في استخدام التكنولوجيا، بل في حوكمتها بطريقة تجعلها أداة للتطوير المؤسسي، تحسين القرار، تعزيز الثقة، وتحقيق القيمة المستدامة.

المحور الاول

مدخل إلى حوكمة الشركات وتكنولوجيا المعلومات

أولاً: مدخل إلى حوكمة الشركات

تمهيد

إن دراسة حكم المؤسسات تندرج ضمن منظور تاريخي طويل لتطور الرأسمالية حسب ما عرفها (Fernand Braudel, 1976, 1979) وذكرها P. Roland في كتابه حوكمة المؤسسات، وبذلك تعود نشأتها إلى ارتباطها بالمسار التاريخي لعملية عولمة الأسواق المالية، وبمعنى أوسع تطور المرجعيات الاستراتيجية التي تستند عليها الشركات في تحديد توجهها وقراراتها. تعتبر حوكمة الشركات من المفاهيم الأساسية في علم الإدارة الاقتصادية المالية وحتى القانون، خاصة بعد توسع شركات المساهمة وتعدد هياكلها.

وقد اعتمد مفهوم الحوكمة الحديثة على إشكالية فصل الملكية عن الإدارة وهذا ما تناوله كل من Means و Berle في كتابهما حول الشركة الحديثة والملكية الخاصة، الذي أظهر أن تطور الشركات الكبرى أدى إلى انتقال السيطرة من المالكين إلى المديرين المحترفين وهذا ما أدى إلى فجوة بين من يملك رأسمال متخذ القرار داخل المؤسسة (Berle, Means, 1932). وعليه تطور مفهوم حوكمة الشركات من كونه آلية تسمح بحماية حقوق المساهمين إلى إطار مؤسسي متكامل يهدف إلى الشفافية والعدالة، حماية أصحاب المصالح، وكذا ضمان استدامة الأداء داخل المؤسسة.

وهذا ما أكد عليه كل من Tricker و Mallin أن الحوكمة ليست مجرد التزام قانوني رقابي، بل هي نظام شامل في تنظيم السلطة داخل المؤسسة وتوجيهها نحو خلق القيمة على المدى الطويل (Tricker, 2019 ; Mallin, 2019).

كما تطرح حوكمة المؤسسات عدة إشكاليات منها عدم تناظر المعلومات، ترسخ نفوذ المسيرين واستمرارهم في اتخاذ القرار داخل المؤسسة، والإجراءات المقترحة لانضباطهم بالاضافة إلى ضرورة استعمال مؤشرات التحليل المالي لتقييم أداء المؤسسات. (H. de La Bruslerie, 2010)

1. مفهوم حوكمة الشركات

تعرف حوكمة الشركات حسب (OECD, 2004) على أنها مجموع الآليات التنظيمية التي تؤدي إلى تحديد الصلاحيات والسلطات وتؤثر في قرارات المديرين، كما تعرف في تقرير (Cadbury, 1992) على أنها النظام الذي يوجه وتراقب به الشركات. أما (Charreaux, 1997) فيضيف على تعريف OECD أنها مجموعة من الآليات التي تسمح بالحد من السلوكيات الانتهازية

للمديرين من جهة وتحسين عملية خلق قيمة داخل المؤسسة من جهة أخرى، ومن خلال هذا المنظور يفهم على أن الحوكمة لا تقتصر فقط على الوقاية بل تشمل أيضا توجيه القرار الاستراتيجي، تنظيم العلاقة بين الاطراف وضبط التوازن بين السلطة والمسؤولية. وبناء على ما سبق يمكن تعريف حوكمة الشركات على أنها مجموعة من القواعد، الهياكل، العلاقات والآليات التي تدار وتراقب من خلالها المؤسسة، والتي تنظم كيفية اتخاذ القرار وتحدد من يمتلك سلطة التوجيه والرقابة كما تحدد كيفية توزيع الحقوق والمسؤوليات بين مختلف الأطراف ذات العلاقة مثل مجلس الادارة، الادارة التنفيذية، المساهمين، الدائنين، العمال، الزبائن، الموردين، الدولة والمجتمع. كما تحدد كيف يتم محاسبة أصحاب القرار، ولصالح من تدار المؤسسة.

2. الفرق بين الحوكمة والادارة

لفهم طبيعة السلطة داخل المؤسسة، لابد من التمييز بين الادارة والحوكمة فحسب (Tricker, 2019) الادارة تهتم بتسيير العمليات اليومية مثل الانتاج، التمويل، التسويق، الموارد البشرية، و المبيعات. في حين الحوكمة تهتم بالاطار الذي يحدد من يراقب الادارة، ويضع الاستراتيجية الكبرى وكذلك من يتحمل المسؤولية عن القرارات الاستراتيجية. و عليه فان الادارة تجيب عن السؤال «كيف تسيير المؤسسة؟». أما الحوكمة فتجيب عن السؤال: «من يوجه المؤسسة ومن يراقب من يوجهها؟، وكذلك وفق أي قواعد تتم هذه الرقابة». ويعتبر مجلس الادارة جهازا حوكمانيا بينما الادارة التنفيذية فتمثل جهازا تسييري وبينهما علاقة تكامل حيث أن مجلس الادارة يضع التوجيهات ويراقب القرارات، بينما الادارة التنفيذية فتقوم بتنفيذ هذه القرارات وتقديم تقارير كما تتحمل مسؤولية الأداء التشغيلي. ويمكن مقارنة الادارة والحوكمة من خلال عدة جوانب كما يصفها الجدول الموالي.

جدول 1: مقارنة بين الادارة والحوكمة

الجانب	الادارة	الحوكمة
الغرض الرئيسي	تنفيذ العمليات اليومية وضمان يسر العمل بفعالية.	توجيه الاستراتيجية وتوافقها مع اهداف المؤسسة.
الوقت	قصيرة المدى: اذ تركز على الأداء الروتيني والتشغيلي	طويلة المدى اذ تركز على التخطيط الاستراتيجي.

قرارات تنفيذية وتفصيلية متعلقة بعمليات محددة.	قرارات توجيهية عامة تحدد السياسات العامة.	محتوى القرارات
مسؤولية تنفيذية تحدد على المديرين والموظفين.	مسؤولية استشرافية على مجلس الدارة والدارة العليا.	المسؤولية والمراقبة
التركيز على الادارة للموارد اليومية.	بناء أطر تنظيمية (مثلا لجانا لحوكمة، سياسات الرقابة) وذلك من تحقيق الاهداف الاستراتيجية.	التركيز التنظيمي
ادارة المخاطر التشغيلية اليومية.	وضع الاطر الرقابية وكذا بشروط الامتثال للقوانين والمعايير.	المخاطر والرقابة

من خلال هذه المقارنة يمكن ملاحظة أن الحوكمة تعنى بوضع الاطر وتحديد الاهداف، أما الادارة فتعنى بالعمل داخل هذه الأطر.

3. نشأة وتطور حوكمة الشركات

حوكمة المؤسسة هي ظاهرة قديمة ترجع جذورها الى منتصف القرن الماضي، تطور الشركات المساهمة خصوصا في اقتصادات الرأسمالية المتقدمة بعد المطالبة بالفصل بين الملكية و الادارة أي الأطراف الحائزة على الحقوق على المؤسسة و مختلف المسيرين للعمليات داخل المؤسسة، حيث يبين (Berle, Means, 1932) أن المساهمين في الشركات الكبرى لم يكونوا يمارسوا رقابة مباشرة على المديرين مما أدى الى ظهور ما يسمى بالسيطرة الادارية حيث تطور مفهوم حوكمة الشركات في نهاية الثمانينات وبدأ في الولايات المتحدة الأمريكية مع ظهور العديد من قضايا الغش في التقارير المالية ما أدى الى صدور قانون مكافحة ممارسات الفساد الذي يضمن قواعد ملزمة للمؤسسات بصياغة ومراجعة نظم الرقابة الداخلية المطبقة بها و التزامهم بوضعها في حالة عدم وجودها (ابراهيم الخلوف المكاوي).

وتطورت بعد ذلك هذه الاشكالية في اطار نظرية الوكالة التي تعتبر ان العلاقة بين المساهمين والمديرين هي علاقة تعاقدية بين الرئيس والوكيل، حيث يمكن للمدير أن يتصف بصفته وكيلا بما يخدم مصالحه الخاصة بدلا من مصالح المالكين (Jensen, Meckling, 1976).

وتزايدت أهمية الحوكمة بعد الفضائح المالية مثل انهيار Enron و WorldCom، وكذلك الازمة العالمية 2008 التي كشفت أن ضعف استقلالية مجالس الادارة، غياب الشفافية، تضارب المصالح بالإضافة الى ضعف التدقيق قد يؤدي الى انهيار مؤسسات كبرى وبالتالي فقدان الثقة في الأسواق المالية (Solomon, 2020).

ومما سبق ذكره، أصبحت حوكمة المؤسسات أداة أساسية للرقابة والمساءلة وجدار وقاية من الانحرافات المالية والادارية وكذلك تحسين مناخ الاعمال وتعزيز الثقة في المؤسسة وبالتالي جذب الاستثمار.

4. أهمية حوكمة المؤسسات

تكتسي حوكمة المؤسسات أهمية بالغة داخل المؤسسة وخارجها لأنها تميز عدة أبعاد اقتصادية، قانونية، أخلاقية واستراتيجية كما تسعى إلى تحقيق التوازن بينها. فمن الناحية الاقتصادية تساعد الحوكمة على تحسين كفاءة استخدام الموارد، تقليل تكلفة رأس المال، تعزيز ثقة المستثمرين وكذلك تحسين قدرة المؤسسة على الوصول الى التمويل (Monks, Minow, 2011). أما من الناحية القانونية فهي توفر إطار يسمح باحترام القوانين واللوائح خاصة فيما يتعلق بحماية حقوق المساهمين، مكافحة الفساد، منع استغلال المعلومات الداخلية وكذا ضمان الإفصاح العادل عن المعلومات الجوهرية (OECD, 2023). ومن الناحية الأخلاقية فإن الحوكمة تعزز قيمة المسؤولية، النزاهة، العدالة والشفافية لأن المؤسسة لا تقيم بحسب نشاطها أرباحها فحسب بل أيضا بطريقة تحقيق هذه الأرباح ومدى احترامها للقوانين لأصحاب المصالح (Solomon, 2020).

في حين على المستوى الاستراتيجي، فتساهم الحوكمة في توجيه القرارات الكبرى مثل: التمويل، الاستثمار، التوسع، ادارة المخاطر، الاندماج وكذلك التحول الرقمي. وبناء على ذلك فان الحوكمة لاتعد مجرد نظام رقابي فقط، بل عامل من عوامل الأداء الاستراتيجي طويل الأجل (Clarke, 2017 ; Tricker, 2019).

5. النظريات المفسرة لحوكمة المؤسسات

- **نظرية الوكالة:** تعتبر نظرية الوكالة من أكثر النظريات استخداماً في تفسير حوكمة الشركات، إذ أنها تقوم على أن العلاقة بين المساهمين والمديرين هي علاقة تعاقدية من الرئيس والوكيل. ونتيجة لاختلاف المصالح بينهما وعدم تماثل المعلومات، قد يسعى المدير إلى تعظيم مصالحه الخاصة مثل الأجر، النفوذ، الامتيازات، وغيرها بدلاً من تعظيم ثروة المساهمين (Jensen, Meckling, 1976).
- تهتم نظرية الوكالة بمعالجة مشكلتين يتوقع أن يحدثا عند وجود علاقة وكالة، يتمثل المشكل الأول عن تعارض أهداف ورغبة كل من الرئيس والوكيل أما المشكل الثاني فيتمثل في سلوكيهما المختلف اتجاه المخاطرة حيث يفضل كلاهما تصرفات مختلفة اتجاه المخاطر (Clarke Thomas, 2004).
- وتؤدي هذه الوضعية إلى ما يسمى بتكاليف الوكالة التي قسمها (Jensen, Meckling, 1976) إلى أقسام وهي: التكاليف الناتجة عن مراقبة المديرين وهذه التكاليف يتحملها الرئيس من أجل ضمان أن تصرفات الوكيل تصب في مصلحته، وكذلك تكاليف الالتزام التي يتحملها الوكيل حتى يطمئن الرئيس أنه يتصرف بطريقة تخدم مصالحه لإعداد تقارير بالإضافة إلى تكاليف ما يسمى بالخسارة المتبقية أي ارتفاع تكلفة الاستثمار الناتجة عن انخفاض الرضا، حيث تمثل الخسارة المتبقية الفرق بين درجة الرضا في حالة الوكيل الانتهازي وحالة الوكيل الغير انتهازي. هذا ما يؤدي إلى البحث على طرف تعاقدية مكلفة (Josse Roussel, 2011). في حين أضاف (Jensen, Meckling, 1976) تكاليف مرتبطة بالمبالغة في تقييم المؤسسة في الأسواق التي تؤدي إلى تغيير تصرفات المديرين الذين يقدمون على اتخاذ قرارات استراتيجية محفوفة بالمخاطر.
- ولهذا تقترح نظرية الوكالة مجموعة من آليات الحوكمة مثل استقلالية مجلس الإدارة، لجان التدقيق، الإفصاح المالي، تفعيل رقابة المساهمين وكذا ربط مكافآت المديرين بالأداء (Fama, Jensen, 1983).
- **نظرية أصحاب المصالح**
- تنتقد نظرية أصحاب المصالح التركيز الحصري على المساهمين، وترى أن المؤسسة ليست مجرد أداة لتعظيم ثروة أصحاب رأس المال (المساهمين)، بل هي شبكة

منال علاقات تضم أطرافاً عديدة تؤثر في نشاط المؤسسة كما تتأثر به. حيث يرى (Freeman, et al., 2010) أبرز مؤسسي هذه النظرية، أن المؤسسة يجب أن تراعي مصالح جميع الأطراف من عمال، زبائن، موردين، دائنين، مجتمع محلي، والدولة، بالإضافة إلى المساهمين (Freeman, et al., 2010).

وتطور أهمية هذه النظرية مع مرور الوقت بسبب زيادة الاهتمام بمفاهيم المسؤولية الاجتماعية، التنمية المستدامة، والحوكمة البيئية والاجتماعية والمؤسسية ESG. وبناء عليه فإن فعالية الحوكمة لا تقاس فقط بقدرة الشركة على حماية المساهمين، ولكن أيضاً بقدرة الشركة على بناء توازن عادل بين مختلف أصحاب المصالح (Freeman, et al., 2010).

- **نظرية الاشراف:** تقدم نظرية الإشراف تصوراً مختلفاً عن سلوك المديرين. فبينما تفترض نظرية الوكالة أن المدير قد يتصرف بأنانية، ترى نظرية الإشراف أن المدير يمكن أن يكون أميناً ومسؤولاً وملتزماً بمصلحة المؤسسة، خاصة عندما يشعر بالثقة، الانتماء، والتقدير (Donaldson, Davis, 1991).

وتبرز هذه النظرية أهمية الثقة، الثقافة التنظيمية، القيادة الأخلاقية، وتمكين المديرين. وتفيد هذه المقاربة خاصة في الشركات العائلية أو المؤسسات ذات الهوية القوية، حيث قد يكون الولا للمؤسسة عاملاً مهماً في توجيه سلوك الإداري.

- **نظرية الاعتماد على الموارد:** تعتبر هذه النظرية مجلس الإدارة أداة أساسية في توفير الموارد الاستراتيجية للمؤسسة، مثل الخبرة، المعلومات، العلاقات، الشرعية، والقدرة على الوصول إلى مصادر التمويل، ولا يقتصر فقط على الدور الرقابي (Pfeffer, Salancik, 1978).

وبناء عليه، يصبح تنوع مجلس الإدارة من حيث التخصص، الخبرة، الجنس، العلاقات المهنية، والخلفيات المعرفية عنصراً مهماً في تحسين قدرة المؤسسة على التكيف مع البيئة الخارجية. فمجلس الإدارة لا يراقب فقط، بل يربط المؤسسة على التطابق مع بيئتها الخاصة حيث يسمح بربط المؤسسة مع محيطها الاقتصادي والاجتماعي والسياسي.

- **النظرية المؤسسية:** تركز هذه النظرية المؤسسية على تأثير البيئة الخارجية سواء كانت قانونية، ثقافية أو اجتماعية في ممارسات الحوكمة. لأن المؤسسات لا تتبنى

قواعد الحوكمة لأنها فعالة اقتصاديا فقط، ولكن لأنها تمنحها الشرعية والقبول داخل المجتمع والسوق (Meyer , Rowan, 1977 ; DiMaggio, Powell, 1983). وهذا ما يفسر اختلاف ممارسات الحوكمة من دولة إلى أخرى، وكذلك أسباب تبني بعض المؤسسات قواعد الحوكمة بصفة شكلية دون تطبيق فعلي. لأن البيئة المؤسسية قد تدفع المؤسسات إلى تقليد ممارسات معينة للحصول على الشرعية فقط، حتى لو لم تكن هذه الممارسات تؤثر فعليا على أدائها.

- **نظرية حقوق الملكية:** تعتبر هذه النظرية ان أهمية حقوق الملكية تكمن في أن تحديد حقوق الأفراد يبين طريقة تخصيص كل من التكاليف والعائدات عند المساهمة في أي منظومة. وإن سلوك الافراد داخل المؤسسة بما فهمه المديرين، تعتمد على طبيعة العقد والتي تنظم هذه الحقوق (محمد الشريف بن زاوي، 2016). كما يمكن لحق الملكية أن يؤثر على السلوك الاقتصادي للأفراد من خلال خصائص حق الملكية المتمثلة في حق حصرية الملكية (أي أن المالك له الحق في تقرير ما يريد فعله بالأصل، حق الاستعمال، حق الاستغلال وحق التصرف أي حق نقلية الملكية للآخرين سواء بوهب الاصل أو بيعه. وكذلك حق الادارة وحق الحصول على عائدات (Christman John, 1994).

6. مبادئ الحوكمة

تقوم حوكمة الشركات على مجموعة من المبادئ الأساسية التي تمثل الإطار المرجعي للحكم الرشيد في المؤسسة. وحسب (OECD , 2023) فإن الحوكمة الفعالة تركز على الشفافية، حماية حقوق المساهمين، المعاملة العادلة، دور أصحاب المصالح، الإفصاح، ومسؤوليات مجلس الإدارة.

- **الشفافية والإفصاح:** تتمثل الشفافية والإفصاح في توفير معلومات دقيقة، واضحة وفي الوقت المناسب حول الوضعية المالية وغير المالية للمؤسسة. وتشمل هذه المعلومات القوائم المالية، هيكل الملكية، المخاطر، المعاملات مع الأطراف ذات العلاقة، مكافآت المديرين، ومختلف السياسات الاجتماعية والبيئية للمؤسسة.

وحسب (Mallin, 2019) تعد الشفافية شرطاً أساسياً لبناء الثقة بين المؤسسة، أصحاب المصالح، والمستثمرين لأنها تحد من عدم تماثل المعلومات وكذلك من السلوكيات الانتهازية.

- **المساءلة:** تتمثل المساءلة في محاسبة كل من يمتلك سلطة داخل المؤسسة عن قراراته. فمثلاً الإدارة التنفيذية مسؤولة أمام مجلس الإدارة، في حين مجلس الإدارة مسؤول أمام المساهمين، أما المدقق الخارجي فهو مسؤول عن إبداء رأي مهني مستقل حول القوائم المالية. ويعتبر (Tricker, 2019) أن المساءلة هي جوهر الحوكمة لأنها تمنع تركيز السلطة دون رقابة، وتضمن أن القرارات لا تتخذ بعيداً عن مصلحة المؤسسة وأصحاب المصالح.

- **العدالة:** تتمثل العدالة في حماية حقوق جميع المساهمين، خاصة صغار المساهمين، والأجانب، وضمان عدم استغلال المساهمين المسيطرين لبقية المساهمين. وكذلك احترام حقوق جميع الأطراف من عمال، دائنين، موردين، وزبائن ومنع المتاجرة الداخلية وإتمام النفقات ومنع المديرين من اتخاذ القرارات المتكلفة بمصالحهم الخاصة. اذ يؤكد (Shleifer, Vishny, 1997) أن ضعف حماية صغار المساهمين يؤدي إلى ضعف الثقة في الأسواق المالية وبالتالي إحجام المستثمرين عن تمويل الشركات.

- **المسؤولية:** تتمثل المسؤولية في التزام المؤسسة بالقوانين المهنية والأخلاقية، مع مراعاة آثار قراراتها على المجتمع والبيئة. ويرى (Soloman, 2020)، أن المسؤولية لم تعد مقتصرة على الالتزام القانوني، بل أصبحت تشمل المسؤولية الاجتماعية والتنمية المستدامة. في حين (A.C Fernando, 2009) يركز على مسؤولية مجلس الإدارة داخل المؤسسة، حيث يعتبر مجلس الإدارة مسؤول عن الإشراف على عملية الإفصاح والاتصال، الرقابة وفعالية ممارسات الحوكمة (A.C Fernando, 2009).

- **الاستقلالية:** تعتبر الاستقلالية أحد المبادئ الأساسية لضمان موضوعية الرقابة. وتشمل استقلالية أعضاء مجلس الإدارة غير التنفيذيين، استقلالية

لجنة التدقيق، استقلالية المدقق الخارجي، واستقلالية وظيفة التدقيق الداخلي. حيث تساعد هذه الاستقلالية على الحد من تضارب المصالح وتحسين جودة القرارات الرقابية (Monks, Minow, 2011).

7. آليات حوكمة الشركات

● مجلس الإدارة: يمثل مجلس الإدارة الجهاز المركزي في نظام حوكمة المؤسسات.

فهو المسؤول عن توجيه المؤسسة، مراقبة الإدارة التنفيذية، مرافقة الإدارة التنفيذية، اعتماد الاستراتيجية، متابعة الأداء، إدارة المخاطر، وضمان حماية مصالح المساهمين وأصحاب المصالح (Tricker, 2019). ويجب على مجلس الإدارة أن يتمتع بالاستقلالية، حتى يكون قادراً على ضبط سلوك المديرين وضمان أن يكون تصرفهم في خدمة مصالح المساهمين وليس مصالحهم. الفكرة هنا تتمثل في وجود شخصيات مستقلة تشهد باستقلالية سلطة التقدير والحكم وكذا اتخاذ القرارات. كما تتكفل بضمان دور الرقابة والفعالية بالنسبة لمجلس الإدارة.

فعالية المجلس تزداد عندما يتمتع أعضاؤه بالكفاءة، الاستقلالية، التنوع، وكذلك القدرة على الوصول إلى المعلومات المناسبة. كما أن وجود فصل واضح بين منصب رئيس مجلس الإدارة ومنصب المدير العام يمكن أن يساعد على تقليل تركيز السلطة (Mallin, 2019).

● لجان مجلس الإدارة: يتعين على مجلس الإدارة أن يكون منظماً وفق لجان

متخصصة، تعتبر هذه الأخيرة من أهم أدوات الحوكمة الداخلية، لأنها تسمح بتعميق الرقابة في مجالات مهمة. وتكون مسؤولة عن تحضير دراسات في مواضيع حساسة في ما يتعلق بتضارب المصالح من أجل تحقيق تسيير فعال لعدم تناظر المعلومات (Peter Wirtz, 2002). وتتمثل هذه اللجان في لجنة التدقيق، لجنة المكافآت، لجنة الترشيحات، ولجنة المخاطر.

تلعب لجنة التدقيق دوراً محورياً في متابعة جودة التقارير المالية، فعالية نظام الرقابة الداخلية، استقلالية المدقق الخارجي، وكذلك إدارة المخاطر المالية. ومن أجل قيامها بدورها بفعالية يجب أن تكون لجنة التدقيق مستقلة عن إدارة الشركة وأن لا يكون لها نشاطات إدارية ولا تفويض لمسؤوليات مالية.

أما لجنة المكافآت فتسعى إلى وضع نظام أجور وحوافز يربط بين مكافآت الإدارة والأداء طويل الأجل، حتى لا تتحول الحوافز إلى عامل لتشجيع المخاطرة المفرطة (Solomon, 2020).

- **التدقيق الداخلي والخارجي:** يمثل التدقيق الداخلي آلية رقابية مهمة تساعد كل من الإدارة ومجلس الإدارة على تقييم فعالية الرقابة الداخلية وكذا إدارة المخاطر. في حين التدقيق الخارجي فيمنح مستخدمي القوائم المالية درجة عالية من الثقة في عدالة ومصداقية المعلومات المحاسبية. وهذا ما أظهرته الأزمات المالية، إذ أن ضعف التدقيق أو فقدان استقلاليته قد يؤدي إلى تضليل المستثمرين وتضخيم الأرباح وإخفاء المخاطر، وهذا ما يجعل التدقيق عنصرا جوهريا في نظام الحوكمة (Mallin, 2019).
- **الإفصاح المالي وغير المالي:** يعد الإفصاح من أبرز آليات الحوكمة، إذ يسمح بتقليل عدم تماثل المعلومات بين الإدارة وأصحاب المصالح. ولم يعد الإفصاح حصرا على البيانات المالية، بل أصبح يشمل تقارير الاستدامة، المعلومات الاجتماعية والبيئية، إدارة المخاطر، رأس المال البشري، وكذلك الحوكمة المؤسسية (OECD, 2023).
- **هيكل الملكية:** يلعب هيكل الملكية دورا كبيرا في تشكيل نظام الحوكمة. حيث تكون المشكلة الأساسية في الشركات ذات الملكية المشتتة، ضعف رقابة المساهمين على المديرين. أما في الشركات ذات الملكية المركزة، فقد تكون المشكلة في استغلال المساهم المسيطر لصغار المساهمين (Shleifer, Vishny, 1997).

8. النماذج الدولية لحوكمة الشركات

- **النموذج الأنجلوسكسوني:** ينتشر هذا النموذج في بريطانيا والولايات المتحدة الأمريكية، ويركز على حماية حقوق المساهمين وتعظيم قيمة الأسهم وتحقيق الربح المالي. ويتميز بوجود أسواق مالية متطورة، ملكية مشتتة داخل الشركات، درجة إفصاح مالي قوية، وحضور قوي للمستثمرين (Clarke, 2017). فهو نموذج قائم على السوق، حيث تلعب البورصة، المستثمرون، المحللون الماليون، ووسائل الإعلام دورا مهما في مراقبة الشركات.

- **النموذج الألماني والياباني:** يقوم هذا النموذج على العلاقات طويلة الأجل بين المؤسسة، البنوك، الموردين والعمال، فهو يعطي أهمية كبيرة لأصحاب المصالح وليس فقط للمساهمين. ففي ألمانيا، مثلاً، يوجد نظام المجلسين: مجلس الإدارة التنفيذي وكذلك مجلس الرقابة، كما يوجد ممثلين للعمال في بعض مجالس الرقابة. في حين النموذج الياباني، فلعبت العلاقات الشبكية بين الشركات والبنوك دوراً مهماً في الحوكمة (Clarke, 2017). حيث يعتبر هذا النموذج المؤسسي ليس مجرد وسيلة لتحقيق الربح بل هي مجموعة إنتاجية مستقرة تسعى إلى الاستمرارية على المدى الطويل. فهو نموذج موجه نحو أصحاب المصالح، وليس فقط نحو المساهمين.
- **النموذج العائلي:** ينتشر هذا النموذج في الدول النامية والعربية والمتوسطة. ويتميز بتركيز الملكية داخل المؤسسة العائلية، مما قد يوفر استقراراً ورؤية استراتيجية طويلة الأجل، لكنه في المقابل قد يؤدي إلى ضعف الشفافية، الخلط بين الإدارة والملكية، المحسوبية، وفي بعض الأحيان تهميش الكفاءات المهنية (La Porta, et al., 1999).
- **النموذج القائم على أصحاب المصالح:** يرتكز هذا النموذج على إدماج مصالح جميع الأطراف المعنية من عمال، مجتمع، بيئة، دولة في عملية اتخاذ القرار. ففكرة نجاح المؤسسة واستمراريتها حسب هذا النموذج لا يتحققان فقط من خلال تحقيق الربح بل من خلال بناء توازن بين المصالح الاقتصادية، الاجتماعية والبيئية. فالمؤسسة حسب هذا المنظور لا تعد كياناً مالياً فقط، بل هي فاعل اقتصادي واجتماعي له مسؤوليات اتجاه محيطه الداخلي والخارجي. وقد تعزز هذا النموذج مع تطور التنمية المستدامة ومعايير ESG، حيث أصبحت المؤسسات مطالبة بتقديم أداء مسؤول يتجاوز النتائج المالية قصيرة الأجل (Freeman, et al., 2010 ; Solomon, 2020).

9. حوكمة الشركات في السياق العربي

تواجه حوكمة الشركات في الدول العربية العديد من التحديات، مثل تركيز الملكية، الطابع العائلي للمؤسسات، ضعف استقلالية مجالس الإدارة، محدودية الإفصاح المالي، وضعف

الحماية بالنسبة لصغار المساهمين. وفي بعض الاحيان تكون الممارسات الحوكمية شكلية فقط، حيث يتم تبني اللجان دون تفعيل دورها الرقابي. ونتيجة لذلك يتوقف تطوير الحوكمة على تعزيز الشفافية، استقلالية التدقيق، تكوين أعضاء مجالس الإدارة، تطوير التشريعات، ونشر ثقافة المساءلة داخل المؤسسات (حماد، 2005؛ الخضير، 2005؛ ابراهيم الخلف المكاوي، 2023).

10. حوكمة الشركات في الجزائر

تكتسب حوكمة الشركات في الجزائر أهمية خاصة في ظل التحولات الاقتصادية الراهنة، ومحاولات تنويع الاقتصاد، بالإضافة الى تشجيع الاستثمار الخاص. حيث تستدعي الحاجة إلى مؤسسات أكثر شفافية وقدرة على المنافسة، في ظل تحديات التحول الرقمي، العولمة والاستدامة. بالإضافة الى تطوير مهمة التدقيق، تكوين أعضاء مجالس الادارة، دعم الافصاح وتفعيل دور الهيئات الرقابية.

وتبرز الحاجة إلى تطبيق الحوكمة نتيجة لعدة أسباب منها: وجود مؤسسات عمومية اقتصادية تحتاج إلى تحسين الرقابة والأداء، وكذلك تطور المؤسسات الخاصة والعائلية، ضعف السوق المالي، وكذلك الحاجة إلى جذب الاستثمار الأجنبي، وأهمية مكافحة الفساد بالإضافة الى تعزيز الثقة الاقتصادية.

11. الحوكمة والاستراتيجية

توجد علاقة قوية بين الحوكمة والاستراتيجية، حيث لم تعد الحوكمة وظيفة رقابية فقط، بل أصبحت مرتبطة مباشرة بالاستراتيجية. حيث أن دور مجلس الإدارة لا يقتصر فقط على مراقبة الإدارة التنفيذية، بل يشارك في تحديد الرؤية الاستراتيجية، تقييم المخاطر، متابعة تنفيذ الخطط، وكذلك توجيه المؤسسة نحو خلق القيمة المستدامة (Tricker, 2019).

كما تساعد الحوكمة الفعالة في ضمان أن القرارات الاستراتيجية تبني وفق رؤية متوازنة تراعي مصالح المساهمين وأصحاب المصالح. وهذا ما يجعلها عنصرا أساسيا في بناء الميزة التنافسية واستدامة المؤسسة. فمثلا الحوكمة تؤثر في القرارات التمويلية والاستثمارية، لأنها تحدد درجة الثقة التي يمنحها الدائنون والمستثمرون للمؤسسة. فكلما كانت الحوكمة فعالة وقوية، زادت قدرة المؤسسة على تعبئة الموارد المالية والبشرية والمعرفية.

12. الحوكمة وادارة المخاطر

ترتبط الحوكمة ارتباطا وثيقا بإدارة المخاطر، إذ أن مجلس الإدارة يعتبر المسؤول عن التأكد من وجود نظام فعال لتحديد المخاطر وقياسها ومراقبتها. وتتمثل هذه المخاطر في مخاطر مالية، تشغيلية، قانونية، استراتيجية، تكنولوجية، بيئية، وكذلك مخاطر متعلقة بالسمعة. وقد أظهرت الأزمة المالية العالمية أن ضعف الحوكمة في المؤسسات المالية ساهم تضخيم المخاطر، خاصة عندما ارتبطت أنظمة المكافآت بالأرباح القصيرة الأجل دون مراعاة مستوى المخاطرة (Solomon, 2020). وهذا ما جعل إدارة المخاطر جزءا أساسيا من مسؤوليات مجلس الإدارة ولجان الحوكمة، خاصة في المؤسسات المالية والبنوك.

13. الحوكمة والاستدامة

لقد توسع مفهوم الحوكمة في السنوات الأخيرة ليشمل قضايا الاستدامة والمسؤولية الاجتماعية. ولم تعد المؤسسات مطالبة فقط بالإفصاح عن أدائها المالي، بل أصبحت مطالبة بالإفصاح عن آثارها الاجتماعية والبيئية وكذلك ممارساتها في مجال الحوكمة. ويظهر ذلك من خلال تطور مفهوم ESG، الذي يربط الحوكمة بالبيئة والمجتمع، فالجانب الاجتماعي يشمل حماية حقوق العمال، الصحة والسلامة، التنوع، والعلاقة مع المجتمع. في حين الحوكمة تشمل الشفافية، المساءلة، محاربة الفساد، استقلالية مجلس الإدارة، وحقوق المساهمين. أما الجانب البيئي فيشمل قضايا الانبعاثات، الطاقة، المياه، وكذلك النفايات (OECD, 2023; Solomon, 2020). وعليه أصبحت الحوكمة ليس فقط وسيلة لحماية المستثمرين بل أداة فعالة لتحقيق الاستدامة.

14. حدود حوكمة الشركات

تمثل الحوكمة اطارا عمليا لتنظيم السلطة داخل المؤسسة، وضمان التوازن بين الرقابة والتوجيه وبين المسؤولية والربحية وبين مصالح المساهمين ومصالح أصحاب العلاقة. وقد تطورت الحوكمة من منظورها الضيق الذي يركز على المساهمين الى منظور واسع يشمل الاستدامة، ادارة المخاطر، والمسؤولية الاجتماعية. ان دراسة الحوكمة يسمح بفهم أعمق

لكيفية عمل المؤسسات الحديثة وكيفية توزيع السلطة داخلها، بالإضافة الى كيفية بناء أنظمة رقابية واستراتيجية تضمن الأداء المستدام.

ثانياً: مدخل إلى تكنولوجيا المعلومات

تمهيد

تعد تكنولوجيا المعلومات أحد المفاهيم الأساسية لفهم التحولات الاقتصادية، الإدارية والاجتماعية. فقد أصبحت المؤسسات الحديثة تعتمد على المعلومات باعتبارها مورداً استراتيجياً لا يقل أهمية عن الموارد المادية أو البشرية. ومع تطور الحوسبة، الشبكات، قواعد البيانات، الإنترنت، الذكاء الاصطناعي، والحوسبة السحابية، تطورت تكنولوجيا المعلومات من كونها مجرد أداة تقنية مساعدة، بل أصبحت بنية تحتية أساسية لتسيير المؤسسات، دعم القرار، تحسين الأداء، وخلق القيمة ويشير (Laudon et Laudon, 2022) إلى أن تكنولوجيا المعلومات تمثل أحد المكونات الجوهرية لنظم المعلومات الإدارية، لأنها توفر الوسائل التقنية اللازمة لجمع البيانات ومعالجتها، تخزينها، نقلها، واستخدامها في عمليات التسيير واتخاذ القرار. كما يؤكد (Turban, et al., 2021) أن تكنولوجيا المعلومات أصبحت مرتبطة بشكل كبير مع التحول الرقمي، حيث أن المؤسسات لم تعد تستخدم التكنولوجيا لتحسين عملياتها فقط، بل لإعادة تصميم نماذج الأعمال وكذلك العلاقات مع الزبائن والشركاء (Turban, et al., 2021).

وعلى هذا الأساس، يهدف هذا المحور إلى تقديم مدخل علمي لتكنولوجيا المعلومات من خلال تحليل المفهوم، تطوره، مكوناته، مجالات استخدامه، آثاره التنظيمية، تحدياته، ودوره في التحول الرقمي.

1. مفهوم تكنولوجيا المعلومات

تعتبر تكنولوجيا المعلومات عن كل الوسائل المادية، البرمجية، الشبكية، والتنظيمية التي تسمح بجمع البيانات، معالجتها، تخزينها، استرجاعها، نقلها، وتحويلها إلى معلومات قابلة للاستخدام. فهي بذلك تجمع بين الحاسوب، البرمجيات، قواعد البيانات، شبكات الاتصال، أنظمة الأمن، وكذلك المهارات البشرية اللازمة لتشغيلها وإدارتها (علاء عبد الرزاق سالمي، 2008).

ويعرف (O'Brien, Marakas, 2010) تكنولوجيا المعلومات على أنها مجموعة من الموارد التقنية التي تدعم نظم المعلومات داخل المؤسسة، بما في ذلك الأجهزة، البرمجيات، شبكات الاتصال، إدارة البيانات، والموارد البشرية المتخصصة. أما (Reix, Rowe, 2016) فيؤكد أن تكنولوجيا المعلومات لا يمكن فهمها بمعزل عن نظم المعلومات، لأنها تصبح ذات قيمة عندما يتم دمجها داخل العمليات التنظيمية واتخاذ القرار. ولابد من التمييز بين ثلاثة مفاهيم أساسية: البيانات هي حقائق خام لم يتم معالجتها بعد مثل أرقام المبيعات، أسماء الزبائن، أو كميات المخزون.

المعلومات هي بيانات تمت معالجتها وتنظيمها حتى يتسنى استخدامها. أما المعرفة فهي القدرة على تفسير المعلومات واستخدامها في حل المشكلات واتخاذ القرارات.

فقد بين (Davenport, Prusak, 1998) أن القيمة الحقيقية للمعلومات تكمن في تحويلها إلى معرفة قابلة للتطبيق والاستعمال داخل المؤسسة، وليس فقط تخزينها.

2. التطور التاريخي لتكنولوجيا المعلومات

مرت تكنولوجيا المعلومات في تطورها بعدة مراحل كل مرحلة تميزت بتطور تقني وتنظيمي معين.

- **مرحلة الحوسبة المركزية:** ظهرت هذه المرحلة مع استخدام الحواسيب الكبرى داخل المؤسسات الكبرى والهيئات الحكومية وكذلك البنوك. كانت هذه الحواسيب ضخمة ومكلفة، وتستخدم فقط في معالجة العمليات الحسابية والمالية المعقدة. حيث تمحورت وظيفة التكنولوجيا في هذه المرحلة في الجانب التشغيلي، وتركزت على أتمتة العمليات المتكررة وكذلك تقليل الأخطاء. ويرى (Alter, 2002) أن الاستخدام الأولي للحوسبة في المؤسسات كان مرتبطاً بمعالجة المعاملات Transaction Processing، مثل الرواتب، الفواتير، الحسابات، والمخزون.

- **مرحلة الحاسوب الشخصي:** أصبحت التكنولوجيا أكثر انتشاراً في المؤسسات والأسر مع ظهور الحاسوب الشخصي في فترة الثمانينات، حيث سمحت هذه

المرحلة بانتقال جزء من القدرة الحاسوبية إلى المستخدم النهائي، وهذا ما ساعد على تطوير تطبيقات مكتبية عديدة مثل معالجة النصوص، الجداول الإلكترونية، وكذلك برامج العروض.

سمحت هذه المرحلة بتغيير علاقة المستخدم بالتكنولوجيا، حيث لم يعد الحاسوب أداة بيد المختصين فقط، بل أصبح وسيلة عمل روتينية للمديرين والموظفين والباحثين.

- **مرحلة الشبكات والأنترنت:** أديتطور الإنترنت الى حدوث تحول جذري في تكنولوجيا المعلومات، حيث انتقلت المؤسسة من كونها نظام مغلق إلى بيئة مترابطة. كما ظهرت خلال هذه المرحلة التجارة الإلكترونية، البريد الإلكتروني، المواقع الإلكترونية، المنصات الرقمية، بالإضافة الى نظم إدارة العلاقات مع الزبائن.

ويؤكد (Castells, 2010) أن ظهور شبكات الاتصال الرقمية ساهم في بناء مجتمع الشبكة، حيث أصبحت المعلومات والتدفقات الرقمية عناصر مركزية في الاقتصاد والمجتمع.

- **مرحلة التحول الرقمي:** أصبحت تكنولوجيا المعلومات في المرحلة المعاصرة مرتبطة بالتحول الرقمي، حيث يتم إعادة تصميم العمليات ونماذج الأعمال باستخدام التقنيات الرقمية. وتشمل هذه التقنيات الحوسبة السحابية، البيانات الضخمة، الذكاء الاصطناعي، إنترنت الأشياء، سلاسل الكتل، والأمن السيبراني.

ويرى (Westerman, et al., 2014) أن التحول الرقمي لا يعني فقط إدخال تقنيات جديدة، بل يعني تغيير كبير في الاستراتيجية، الثقافة التنظيمية، وكذلك العمليات الداخلية.

3. مكونات تكنولوجيا المعلومات

تتكون تكنولوجيا المعلومات من مجموعة عناصر المترابطة مع بعضها البعض والمكملة لبعضها بحيث لا يمكن لأي عنصر منها أن يحقق قيمة بمفرده.

- **الأجهزة Hardware:** تشمل الأجهزة كل المكونات المادية المستخدمة في معالجة المعلومات، مثل الحواسيب، الخوادم، وحدات التخزين، الطابعات، أجهزة الشبكات، الهواتف الذكية، ومراكز البيانات ... الخ
وتعتبر الأجهزة البنية المادية التي تقوم عليها تكنولوجيا المعلومات، لكنها لا تحقق منفعة فعلية بمعزل عن البرمجيات، البيانات، والمستخدمين.
 - **البرمجيات Software:** البرمجيات تتمثل في مجموعة من الأطر والتعليمات التي توجه الأجهزة للقيام بوظائف معينة. ويؤكد (Stair, Reynolds, 2017) أن البرمجيات هي التي تمنح الأجهزة قيمتها التشغيلية، لأنها تحول القدرة الحاسوبية الخام إلى وظائف مفيدة للمستخدمين والمؤسسات. وتنقسم هذه البرمجيات إلى عدة أقسام منها: برمجيات النظام، مثل أنظمة التشغيل. وبرمجيات التطبيقات، مثل برامج المحاسبة، إدارة الموارد البشرية، إدارة المخزون، أنظمة ERP، وأنظمة CRM.
 - **قواعد البيانات Databases:** تمثل قواعد البيانات عنصرا مهما في تكنولوجيا المعلومات، إذ أنها تسمح بتنظيم البيانات، تخزينها واسترجاعها بطريقة فعالة. ويتم استخدام قواعد البيانات في العديد من المجالات مثل: المبيعات، الموارد البشرية، الإنتاج، التمويل، والتسويق، الزبائن. كما أوضح (Date, 2004) أن نظام إدارة قواعد البيانات لا يقتصر على تخزين البيانات، بل يوفر كذلك الآليات اللازمة لضمان سلامتها، أمنها، تكاملها، وكذلك إمكانية الوصول إليها.
 - **الشبكات والاتصالات:** تسمح الشبكات بربط الحواسيب، الأجهزة، وكذلك المستخدمين داخل المؤسسة وخارجها. وتشمل الشبكات المحلية LAN، الشبكات الواسعة WAN، الإنترنت، الشبكات اللاسلكية، وشبكات الجيل الخامس.
- وحسب (Tanenbaum, Wertherall, 2010) فإن أهمية الشبكات تنبع من كونها تجعل المعلومات قابلة للتبادل الفوري، مما يعزز التعاون، التنسيق، وكذلك العمل عن بعد. كما أصبحت الشبكات عنصرا مهما في المؤسسات الحديثة لأنها تسمح بدمج الفروع، الموردين، الزبائن، وكذلك الشركاء في منظومة معلوماتية واحدة.

- الموارد البشرية المتخصصة: يعتبر العنصر البشري، العنصر الفعال في تكنولوجيا ويشمل كل من مهندسي النظم، مبرمجي التطبيقات، مسؤولي قواعد البيانات، محلي البيانات، مهندسي الشبكات، خبراء الأمن السيبراني، وكذلك مديري نظم المعلومات. ويؤكد (Laudon, Laudon, 2022) أن التكنولوجيا لا تحقق قيمة تنظيمية إلا عندما تتكامل مع الكفاءات البشرية، العمليات الإدارية والاستراتيجية المؤسسية.
- الإجراءات والسياسات: تعتبر الإجراءات ضرورية لضمان الاستخدام الأمثل، المنظم والأمن للتكنولوجيا. وتشمل هذه الإجراءات: قواعد استخدام التكنولوجيا، سياسات الأمن، آليات النسخ الاحتياطي، صلاحيات الوصول، معايير حماية البيانات وكذلك خطط استمرارية العمل.

4. تكنولوجيا المعلومات ونظم المعلومات

تختلف تكنولوجيا المعلومات عن نظم المعلومات، في كون تكنولوجيا المعلومات تمثل الجانب التقني، بينما نظم المعلومات فتشمل التكنولوجيا بالإضافة إلى الأشخاص، الإجراءات، البيانات، وكذلك العمليات التنظيمية.

ويعرف (Laudon, Laudon, 2022) نظام المعلومات بأنه مجموعة متكاملة من المكونات التي تقوم بجمع البيانات، معالجتها، تخزينها، وتوزيع المعلومات لدعم اتخاذ القرار والتنسيق والرقابة داخل المؤسسة. أما (Reix, Rowe, 2016) فيؤكد أن نظام المعلومات هو بناء اجتماعي تقني، لأن فعاليته لا تعتمد فقط على البرمجيات والأجهزة، بل على طريقة استخدامه من طرف الأفراد والمؤسسة.

ومن هذا المنظور، يمكن القول أن تكنولوجيا المعلومات تمثل جزء من نظام المعلومات، وليس النظام ككل.

5. أنواع نظم المعلومات المرتبطة بتكنولوجيا المعلومات

- نظم معالجة المعاملات: وهي نظم مبنية على استخدام الحاسوب، تقوم بجمع، تسجيل، ومعالجة البيانات الخاصة بالأحداث اليومية والمتعلقة بنشاط المؤسسة

مثل: البيع، الشراء، الدفع، الرواتب، المخزون، والحجوزات. وتعرض هذه المعلومات في شكل تقارير روتينية لمستخدميها كما تعتبر أساسية لأنها توفر البيانات الخام التي تعتمد عليها بقية الأنظمة (فريد كورتل، أمال يوب، 2016).

وقد أوضح (Alter, 2002) أن هذه النظم تمثل الطبقة التشغيلية الأولى في نظم المعلومات، لأنها تضمن تسجيل المعاملات بدقة وانتظام.

- **نظم المعلومات الإدارية:** تعرف نظم المعلومات الإدارية بأنها مجموعة من الأجزاء المترابطة والتي تعمل بطريقة متفاعلة من أجل تحويل البيانات العمليات من أجل استخدامها والاستفادة منها. وعليه فإن نظم المعلومات الإدارية تقوم بتحويل بيانات العمليات إلى تقارير تساعد المديرين في التخطيط والرقابة. فمثلا تستخدم لإعداد تقارير المبيعات، الإنتاج، التكاليف، الغيابات، وكذلك المخزون.
 - **نظم دعم القرار:** تقوم نظم دعم القرار بتقييم النتائج والاختيار بين الاستراتيجيات البديلة، كما تساعد المديرين على تحليل المشكلات المعقدة. وتعتمد هذه النظم على النماذج الرياضية، قواعد البيانات، التحليل الإحصائي، والمحاكاة.
- ويشير (Turban, et al., 2021) أن نظم دعم القرار أصبحت أكثر تطوراً بفضل الذكاء الاصطناعي وتحليل البيانات الضخمة، وهذا ما يسمح بدعم القرارات.
- **نظم تخطيط موارد المؤسسة ERP:** تسمح نظم ERP بدمج مختلف وظائف المؤسسة في نظام واحد مثل: الموارد البشرية، المحاسبة، المشتريات، الإنتاج، المبيعات، المخزون. والهدف من هذه النظم تحسين التنسيق، تقليل التكرار، وتوفير رؤية موحدة للمؤسسة.

أما بالنسبة إلى (Monk, Wagner, 2012) فإن نظم ERP تمثل تحولا تنظيميا بالإضافة إلى كونها مشروعا تقنيا، لأنها تفرض إعادة تنظيم العمليات وتوحيد البيانات والإجراءات.

- نظم إدارة العلاقة مع الزبائن CRM: هي مجموعة من الأدوات والبرامج والجراءات التي تستعملها المؤسسة من أجل تنظيم علاقتها مع الزبائن الحاليين وكذلك المحتملين، وتحسين التواصل معهم، فهم حاجاتهم وزيادة رضاهم وولائهم. وعليه تستخدم نظم CRM لجمع وتحليل بيانات الزبائن، بهدف تحسين التسويق، المبيعات، الخدمة، وكذلك ولاءهم. فهي تساعد على فهم سلوك الزبون ومنه تخصيص العروض والخدمات المناسبة له.

- نظم ذكاء الأعمال Business Intelligence: تهدف نظم ذكاء الأعمال إلى تحويل البيانات الضخمة إلى معلومات استراتيجية قابلة للتحليل. وتشمل لوحات القيادة، التقارير التفاعلية، التحليل التنبئي وغيرها.

وعليه يؤكد كل من (Kimball, Ross, 2013) أن مستودعات البيانات وذكاء الأعمال تسمح للمؤسسات ببناء ذاكرة تحليلية تساعد على فهم الأداء واتخاذ قرارات مبنية على الأدلة.

6. البنية التحتية لتكنولوجيا المعلومات

تتمثل البنية التحتية لتكنولوجيا المعلومات في الموارد التقنية المشتركة التي تعتمد عليها المؤسسة في تشغيل أنظمتها الرقمية. وتشمل الخوادم، الشبكات، قواعد البيانات، مراكز البيانات، منصات الحوسبة السحابية، أنظمة الدعم، وخدمات الدعم التقني.

ويشير (Ross et al., 2006) إلى أن البنية التحتية الرقمية، تشكل أساس المرونة التنظيمية، حيث أنها تسمح للمؤسسة بتطوير خدمات جديدة بسرعة، وربط العمليات، وكذلك تحقيق التكامل بين الوحدات التنظيمية. وهذا ما تسعى اليه المؤسسات الحديثة في تبني بيانات أكثر مرونة مثل الحوسبة السحابية، والخدمات الرقمية القابلة للتوسع. وهذا التحول يسمح بتقليل الاعتماد على التجهيزات المحلية، كما يطرح العديد من التحديات المتعلقة بالأمن، حماية البيانات، وكذلك تكاليف الاشتراك.

7. تكنولوجيا المعلومات والميزة التنافسية

أصبحت تكنولوجيا المعلومات مصدرا للميزة التنافسية وليس فقط أداة تشغيلية. فهي تساعد على تخفيض التكاليف في المؤسسة، وكذلك تحسين الجودة، دعم الابتكار، تسريع الخدمة، تحسين العلاقة مع الزبائن، وتخصيص العروض.

وحسب (Porter, Millar, 1985) فإن تكنولوجيا المعلومات تسمح بتغيير قواعد المنافسة لأنها تؤثر في سلسلة القيمة، كما تسمح بخلق روابط جديدة بين الأنشطة، وبظهور منتجات وخدمات جديدة.

في حين أكد (Carr, 2004) أن امتلاك تكنولوجيا وحده لا يكفي لتحقيق ميزة تنافسية مستدامة. لأن التكنولوجيا عندما تكون متاحة للجميع قد تفقد قدرتها على التمييز ما لم يتم ادراجها في استراتيجية تنظيمية واضحة وكفاءات يصعب تقليدها.

وعليه، فإن القيمة الاستراتيجية لتكنولوجيا المعلومات لا تتحقق من خلال الشراء التقني فقط، بل تحتاج الى حسن التوظيف، التكامل مع العمليات، التكوين، القيادة، والثقافة التنظيمية.

8. تكنولوجيا المعلومات والتحول الرقمي

يختلف التحول الرقمي عن الرقمنة، حيث أن الرقمنة تتمثل في تحويل الوثائق أو العمليات من شكل ورقي إلى شكل رقمي، في حين التحول الرقمي هو تغيير عميق في خلق القيمة، حيث يتمثل في عملية استخدام التقنيات الرقمية لإعادة بناء العمليات، نماذج الأعمال، طرق العمل، وتجربة الزبون.

ويرى (Westerman, et al., 2014) أن التحول الرقمي الناجح يتطلب الجمع بين القدرات التقنية والقيادة الإدارية، لأن التقنية دون قيادة لا تؤدي إلى تغيير فعلي، والقيادة دون قدرات تقنية لا تستطيع تنفيذ الرؤية الرقمية. وتشمل تقنيات التحول الرقمي على البيانات الضخمة، الذكاء الاصطناعي، الانترنت، الحوسبة السحابية، الروبوتات، المنصات الرقمية، سلاسل الكتل، والتحليلات المتقدمة.

ويؤكد (Bharadwaj, et al. 2013) أن الاستراتيجية الرقمية هي جزء من الاستراتيجية العامة، لأن التكنولوجيا أصبحت تؤثر في المنتجات، الأسواق والعلاقات التنظيمية.

9. البيانات، المعلومات والمعرفة في المؤسسة

تقوم تكنولوجيا المعلومات على إدارة البيانات وتحويلها إلى معلومات ومعرفة. فالبيانات تمثل المادة الخام، في حين المعلومات تمثل البيانات المنظمة ذات المعنى، أما المعرفة فهي القدرة على استخدام المعلومات في الفهم والتفسير وكذلك اتخاذ القرار.

وعليه يبين (Davenport, Prusak, 1998) أن إدارة المعرفة لا تتمثل فقط في تخزين الوثائق في قواعد البيانات، بل تشمل خلق المعرفة، تبادلها، توظيفها، وكذلك حمايتها داخل المؤسسة.

ومع ظهور البيانات الضخمة Big Data، أصبحت المؤسسات تجمع كميات هائلة من البيانات من مصادر مختلفة، مثل المعاملات، المواقع الإلكترونية، وسائل التواصل الاجتماعي، وتطبيقات الهاتف. لكن البيانات الضخمة لا تعني بالضرورة معرفة أفضل لأن القيمة لا تتحقق إلا عندما تتوفر جودة البيانات، أدوات التحليل، الكفاءات البشرية.

10. حماية المعلومات والأمن السيبراني

تزداد المخاطر الرقمية كلما زاد اعتماد المؤسسات على تكنولوجيا المعلومات. وتتمثل هذه المخاطر في الاختراقات، البرمجيات الخبيثة، الهجمات على الشبكات، سرقة البيانات، تعطيل الخدمات، وكذلك تسريب المعلومات الحساسة وغيرها.

وحسب (Stallings, 2016) فإن أمن المعلومات يقوم على ثلاثة مبادئ أساسية: التوافر، السرية، والسلامة. فالتوافر يعني ضمان إمكانية الوصول إلى الأنظمة والمعلومات عند الحاجة. في حين السلامة تعني حماية المعلومات من أي تغيير غير المشروع، أما السرية فتعني منع الوصول غير المصرح به إلى المعلومات،

وتتم حماية المعلومات وفقا لمجموعة من الإجراءات، تتمثل في: استخدام كلمات المرور القوية، تشفير البيانات، تحديث الأنظمة، النسخ الاحتياطي، مراقبة الشبكات، تحديد صلاحيات الوصول، تكوين المستخدمين، وخطط الاستجابة للحوادث.

ولا يمكن اختزال الأمن السيبراني في الجانب التقني فقط وأهمل العنصر لأن الثقافة الأمنية داخل المؤسسة عنصرا أساسيا في حماية المعلومات.

11. الحوكمة الرقمية وحوكمة تكنولوجيا المعلومات

تتمثل حوكمة تكنولوجيا المعلومات في الإطار الذي يضمن أن استخدام التكنولوجيا داخل المؤسسة يدعم الأهداف الاستراتيجية، يسمح بخلق القيمة، بإدارة المخاطر، واستخدام الموارد بكفاءة.

وحسب (Weill, Ross, 2004) فإن حوكمة تكنولوجيا المعلومات تحدد من يمتلك حق اتخاذ القرار في القضايا التقنية، وكيف تتم مساءلته عن النتائج. وعليه فإن تكنولوجيا المعلومات لا ينبغي أن تترك فقط للتقنيين والمهندسين بل يجب أن تكون جزءا من حوكمة المؤسسة واستراتيجيتها.

وتشمل حوكمة تكنولوجيا المعلومات في العديد من القرارات مثل: اختيار الأنظمة، الاستثمار في البنية التحتية، حماية البيانات، إدارة المشاريع التقنية، تحديد الأولويات الرقمية، قياس العائد على الاستثمار، والامتثال للقوانين والمعايير.

12. الآثار التنظيمية لتكنولوجيا المعلومات

تؤثر تكنولوجيا المعلومات في بنية المؤسسة وثقافتها وكذلك طريقة عملها. فهي تسمح بتقليل المستويات الهرمية، تسريع الاتصال، دعم العمل عن بعد، تحسين التنسيق، وتمكين اللامركزية في القرار.

حيث يرى (Mintzberg, 1982) أن تكنولوجيا المعلومات تؤثر في آليات التنسيق داخل التنظيم، لأنها تسمح بتبادل المعلومات بسرعة وتدعم الرقابة والتحليل. كما تؤثر تكنولوجيا المعلومات في طبيعة العمل والمهارات المطلوبة، لأن المؤسسات أصبحت بحاجة إلى كفاءات رقمية، قدرة على تحليل البيانات، فهم الأمن السيبراني، وكذلك إتقان أدوات التعاون الرقمي.

لكن في نفس الوقت تكنولوجيا المعلومات تواجه تحديات عديدة مثل مقاومة العاملين إذا لم ترافق بالتكوين، الاتصال، المشاركة. لذلك نجاح مشاريع تكنولوجيا المعلومات لا يعتمد على التقنية وحدها، بل على الثقافة الرقمية، التنظيم، وإدارة التغيير.

13. تكنولوجيا المعلومات والأخلاقيات

تطرح تكنولوجيا المعلومات العديد من القضايا الأخلاقية، خاصة فيما يتعلق بالخصوصية، مراقبة العاملين، استخدام البيانات الشخصية، الخوارزميات، الذكاء الاصطناعي، والتمييز الرقمي.

وقد أكد (Laudon, Laudon, 2022) أن يجب على المؤسسات التي تستخدم تكنولوجيا المعلومات أن توازن بين الفعالية الاقتصادية، احترام الحقوق الفردية، خصوصاً حق الأفراد في الخصوصية وحماية بياناتهم.

وتشمل القضايا الأخلاقية الأساسية من له الحق في الوصول إلى البيانات، هل تم الحصول على موافقة أصحابها؟ وما حدود مراقبة العاملين رقمياً؟ وغيرها. وهذا ما جعل من الأخلاقيات الرقمية جزءاً من الإدارة الحديثة لتكنولوجيا المعلومات.

14. تحديات تكنولوجيا المعلومات في المؤسسات

رغم الأهمية الكبيرة لتكنولوجيا المعلومات، إلى أن المؤسسات تواجه عدة تحديات عند تبنيها، نذكر منها:

- ارتفاع تكاليف الاستثمار.
- سرعة تقادم التكنولوجيا.
- صعوبة التكامل بين الأنظمة.
- مقاومة التغيير.
- نقص الكفاءات الرقمية.
- مخاطر الأمن السيبراني.
- ضعف جودة البيانات والاعتماد المفرط على الموردين الخارجيين.

ويؤكد (Ross et al., 2006) أن القيمة الحقيقية لتكنولوجيا المعلومات لا تتحقق من خلال امتلاك التكنولوجيا فقط، بل من خلال بناء بنية رقمية واضحة، قابلة للتكامل، ومرتبطة بالاستراتيجية. وعليه فإن نجاح تكنولوجيا المعلومات يتطلب رؤية استراتيجية، تكوين مستمر، قيادة رقمية، حوكمة فعالة، وكذلك ثقافة تنظيمية داعمة للابتكار والتغيير.

15. خصائص تكنولوجيا المعلومات

تتميز تكنولوجيا المعلومات عن غيرها من التكنولوجيات بخصائص، أهمها:

- **تقليص الوقت والمكان:** وذلك من خلال عملية التخزين المتمثلة في حفظ البيانات والمعلومات إلى غاية استعمالها وكذلك عملية الاسترجاع المتمثلة في استعادة البيانات والمعلومات المخزنة من أجل إعادة استعمالها وهذا في وقت وجيز بالإضافة إلى أنها تستوعب حجم هائل من المعلومات المخزنة في نفس المكان وكذلك جعل الأماكن متقاربة إلكترونياً.
- **تكوين شبكات الاتصال:** وذلك من خلال نقل وتبادل المعلومات بين المستخدمين باستخدام خدمات الإنترنت مثل البريد الإلكتروني، تقنية الملفات الإلكترونية المحمولة، وكذلك المحادثات في الزمن الحقيقي.
- **الذكاء الاصطناعي:** تتميز تكنولوجيا المعلومات بسرعة خافقة في تنفيذ وأداء العمليات مما يمكن من الحصول على كم هائل من المعلومات في زمن وجيز مقارنة بالجهد البشري، بالإضافة إلى الدقة في تنفيذ العمليات وكذلك في النتائج المتحصل عليها (محمد فتحي عبد الهادي، 2000).

16. فوائد استخدام تكنولوجيا المعلومات

إن استخدام تكنولوجيا المعلومات يسمح بتحقيق مزايا متعددة للمؤسسة انطلاقاً من سهولة الحصول على المعلومة بأشكالها المختلفة كتابية وشفهية، وكذلك القدرة على تخزين كم هائل من المعلومات، مما يسمح بتخفيض التكاليف التخزين وكذلك نقل المعلومات. بالإضافة إلى رفع الإنتاجية وكفاءة المؤسسة وتطوير منتجاتها وتحقيق ميزة تنافسية في السوق المحلي والعالمي (Meziane Mohamed, 1999).

وعليه فإن تكنولوجيا المعلومات، عن طريق الحاسوب وقدرتها على المعالجات الإلكترونية، مكنت المؤسسة من تقليص العمالة في المؤسسة من جهة ومن جهة أخرى فإن المعلومات الدقيقة متحصل عليها تزيد من فعالية العملية الإدارية وتسهل عملية اتخاذ القرار من خلال توفير البدائل المتاحة أمام متخذ القرار في التوقيت المناسب وتقليل تكلفة الخطأ اتخاذ القرار. بالإضافة إلى إعادة هندسة الإدارة من خلال تكنولوجيا المعلومات حيث يرى Muller إعادة هندسة الإدارة تتمثل في كل التعديلات الجوهرية والرئيسية في عمليات المؤسسة التي تسمح بتحقيق وفورات أكبر وكفاءة أعلى.

17. تطور دور تكنولوجيا المعلومات من التشغيلية الى الاستراتيجية

شهدت تكنولوجيا المعلومات تحولا جذريا خلال العقود الأخيرة، فعندما كانت تستعمل كأداة دعم تشغيلية، تستعمل لتنفيذ المهام الروتينية، ومعالجة البيانات أصبحت اليوم محركا استراتيجيا للتغيير داخل المؤسسة وخلق القيمة وذلك مع ازدياد الاعتماد على النظم الرقمية. وهذا يعني أن القرارات التكنولوجية لم تعد شأنا فنيا بحث بل أصبحت جزءا من استراتيجية العمل مثل: الاعتماد على التحليلات الضخمة، الذكاء الاصطناعي لتطوير المنتجات، والاعتماد على بنية تحتية سحابية لابتكار نماذج عمل جديدة وغيرها.

ومع بروز مفهوم التحول الرقمي أصبحت تكنولوجيا المعلومات ... في نماذج الأعمال حيث سعت المؤسسات للاستفادة من التقنيات الحديثة لتحويل عملياتها وأنشطتها التقليدية إلى عمليات أخرى رقمية تكون أكثر كفاءة وابتكارا، مثل: تحويل الخدمات المصرفية إلى منصات إلكترونية و انتقال التسويق إلى القنوات الرقمية وكذلك ظهور شركات أعمالها كلها قائمة على التقنيات الحديثة، وهذا ما يجعل من تكنولوجيا المعلومات عنصرا استراتيجيا وتحاولا يحدد الميزة التنافسية للمؤسسات، كما يؤثر مباشرة على نموها وابتكارها. لكن هذا التحول الاستراتيجي رافقه كذلك تحديات جديدة مثل مخاطر الهجمات السيبرانية ، فشل المشاريع التقنية الضخمة وذلك في غياب حوكمة تكنولوجيا المعلومات، وهذا ما يجعل من الاستعمالات التقنية تذهب هدرًا.

18. مساهمة تكنولوجيا المعلومات في تحسين العمل الاداري

أحدثت تكنولوجيا المعلومات تحولاً جوهرياً في وظائف الإدارة، لأنها لم تغير أدوات العمل فقط ولكن ساهمت في تغيير طريقة التفكير الإداري نفسه (فريد كورتل، أمال يوب، 2016). ولقد ساهمت تكنولوجيا المعلومات في تحسين العمل الإداري من خلال إعادة تشكيل وظائف الإدارة التقليدية خاصة الرقابة والتخطيط، ففي مجال التخطيط، توفر تكنولوجيا المعلومات تدفقاً مستمراً للبيانات الداخلية والخارجية وهذا ما يسمح للإدارة بتحديد الأهداف، صياغة السياسات، وإعداد البرامج التنفيذية على أساس معلومات دقيقة وحديثة. كما تجعل التخطيط أكثر مرونة واستجابة للتغيرات البيئية، من خلال ربط المؤسسة بالسوق، الزبائن، والمنافسين. وتمكينها من تعديل خططها بسرعة وفقاً للمستجدات.

أما في مجال الرقابة، فلقد ساهمت تكنولوجيا المعلومات في الانتقال من الرقابة التقليدية إلى الرقابة الإلكترونية المستمرة وأصبح بالإمكان متابعة الأداء أثناء التنفيذ واكتشاف الانحرافات في الوقت المناسب ومنه اتخاذ الإجراءات التصحيحية بسرعة. كما أدت الرقمة إلى تقليل الرعاية المباشرة والصارمة وتعزيز الرقابة القائمة على الثقة والتمكين والمسؤولية الذاتية خاصة مع تزايد أهمية المعامل المعرفي.

خاتمة

تمثل تكنولوجيا المعلومات أحد الركائز الأساسية للمؤسسة الحديثة، لأنها تساعد في جمع البيانات، معالجتها، تحويلها إلى معلومات ومعرفة تدعم التسيير واتخاذ القرار. وقد تطورت تكنولوجيا المعلومات من كونها مجرد أداة لحوسبة العمليات إلى بنية استراتيجية مرتبطة بالتحول الرقمي، الابتكار، الحوكمة، الأمن السيبراني، وكذلك الميزة التنافسية.

إن فهم تكنولوجيا المعلومات ضروري من الناحية التقنية، الإدارية والاستراتيجية. فالقيمة لا تكمن فقط في الأجهزة والبرمجيات، ولكن قدرة المؤسسة على دمج التكنولوجيا في عملياتها وثقافتها واستراتيجيتها. ولذلك، فإن دراسة تكنولوجيا المعلومات تعتبر كمدخل أساسي لفهم الإدارة الحديثة، الاقتصاد الرقمي، وكذلك التحولات التنظيمية المعاصرة.

أسئلة المناقشة:

- ما الفرق بين البيانات، المعلومات والمعرفة؟
- لماذا لا تعتبر تكنولوجيا المعلومات مرادفا كاملا لنظم المعلومات؟
- كيف تساهم تكنولوجيا المعلومات في خلق الميزة التنافسية؟
- ما الفرق بين الرقمنة والتحول الرقمي؟
- لماذا يعد الأمن السيبراني قضية إدارية وليس تقنية فقط؟
- كيف تؤثر تكنولوجيا المعلومات في بنية المؤسسة وثقافتها؟
- ما أهمية حوكمة تكنولوجيا المعلومات في المؤسسات الحديثة؟

المحور الثاني

مخاطر تكنولوجيا المعلومات

تمهيد

تعد تكنولوجيا المعلومات أحد الأعمدة الأساسية في المؤسسات الحديثة، غير أن هذا التزايد في الاعتماد على الأنظمة الرقمية، قواعد البيانات، الشبكات، المنصات السحابية، والذكاء الاصطناعي، جعل المؤسسة أكثر عرضة لأنواع جديدة من المخاطر. بالإضافة إلى المخاطر التنظيمية مرتبطة فقط بالسوق، التمويل، الإنتاج، المنافسة، الموارد البشرية وغيرها. وأصبحت المخاطر الجديدة مرتبطة بفقدان البيانات، اختراق الأنظمة، ضعف جودة المعلومات، توقف الخدمات، سوء استخدام التكنولوجيا، وكذلك الاعتماد المفرد على مزودي الخدمات الرقمية.

وعلى هذا الأساس، أصبحت دراسة مخاطر تكنولوجيا المعلومات موضوعاً استراتيجياً، إدارياً وحوكيمياً بالإضافة إلى كونه تقني، لأنها تمس استمرارية المؤسسة، حماية أصولها، احترام التزاماتها القانونية، ضمان جودة قراراتها، وكذلك الحفاظ على ثقة زبائنها.

وقد أكد (Laudon, Laudon, 2022) أن نظم المعلومات، رغم دورها في تحسين الأداء داخل المؤسسة ودعم القرار، قد تصبح مصدراً للمخاطر إذا لم تدار ضمن إطار واضح للرقابة، الحوكمة والأمن.

وحسب المعايير الدولية الحديثة (ISO/IEC, 27001:2022) فإن أمن المعلومات لم يعد مقتصرًا على حماية الحاسوب أو الشبكة، بل يقوم على إدارة شاملة للمخاطر تشمل التكنولوجيا، الأشخاص، العمليات والسياسات. وعليه فإن هذا المعيار يقدم إطاراً لإنشاء نظام إدارة أمن المعلومات وتحسينه المستمر، ويربط ذلك بإدارة مخاطر السرية، التوافر والسلامة.

1. مفهوم مخاطر تكنولوجيا المعلومات

تعرف مخاطر تكنولوجيا المعلومات على أنها مجموعة التهديدات والاحتمالات التي قد تؤدي إلى نتائج سلبية على أهداف المؤسسة، ووفقاً لمعيار ISO فإن المخاطر تعرف على أنها تأثير عدم اليقين على الأهداف. وعليه يمكن تلخيص مخاطر تكنولوجيا المعلومات على أنها احتمال وقوع حذف أو خلل أو تهديد مرتبط باستخدام الأنظمة الرقمية ويؤدي إلى آثار

سلبية على المعلومات، العمليات، الأصول، السمعة، وكذلك استمرارية المؤسسة. وتظهر هذه المخاطر عندما تتوفر العناصر الآتية: أصول معلوماتية ذات قيمة، تهديدات، نقاط ضعف يمكن استغلالها، وكذلك آثار تترتب على تحقيق الخطر. كما يمكن التعبير عن الخطر المعلوماتي من خلال العلاقة بين هذه العناصر الأربعة الأساسية:

- الأصل المعلوماتي: وهو مورد غير مادي له قيمة بالنسبة للمؤسسة، مثل البيانات، التطبيقات، الخوادم، كلمات المرور، الشبكات، الوثائق، معرفة العاملين، والملكية الفكرية.
 - التهديد: كل عامل قد يصيب ضرراً للأصل المعلوماتي، مثل الهجمات الإلكترونية، الأخطاء البشرية، الكوارث الطبيعية، سوء الاستخدام، أو الأعطال التقنية.
 - نقطة الضعف: هو كل خلل أو نقص في النظام أو السلوك أو الإجراء قد يحقق تهديد.
 - الأثر: هو النتيجة السلبية التي تتحملها المؤسسة، مثل الخسارة المالية، فقدان الثقة، توقف الخدمة، تسرب البيانات، والعقوبات القانونية.
- وحسب (Stallings, 2016) فإن أمن المعلومات يقوم على حماية ثلاثة أبعاد رئيسية: السرية، السلامة والتوافر، وهي ما يعرف بـ: (CIA: Confidentiality, Integrity, Availability). وعليه فإن خطر تكنولوجيا المعلومات لا يتمثل فقط في سرقة البيانات، ولكن كذلك في تغييرها، إتلافها، تعطيل الوصول إليها، حتى استخدامها بطريقة غير مشروعة.

2. الفرق بين الخطر، التهديد، نقطة الضعف، والحادث

- الخطر: هو احتمال وقوع حدث سلبي مع وجود أثر محتمل على المؤسسة. كاحتمال توقف نظام المحاسبة بسبب خلل في الخادم.
- التهديد: هو مصدر الضرر المحتمل. مثلاً: برمجيات خبيثة، مهاجم إلكتروني، موظف مهمل، انقطاع كهربائي أو مزود خدمة غير موثوق.

- نقطة الضعف: هي القابلية التي تسمح بتحقيق التهديد. مثلا: عدم تحديث النظام، ضعف كلمة المرور، غياب النسخ الاحتياطي أو سوء توزيع الصلاحيات.
 - الحادث: هو تحقق الخطر فعليا. مثلا: اختراق قاعدة بيانات الزبائن، توقف الخادم، تلف الملفات أو تسرب معلومات سرية.
- وقد أشار (Whitman, Mattord, 2021) أنه على المؤسسة بفهم العلاقة بين هذه المفاهيم، لأنها لا تستطيع حماية نفسها بطريقة فعالة إذا لم تميز بين ما تملكه، وما يهددها، وما يجعلها عرضة للخطر، وكذلك ما يمكن أن يحدث عند فشل الضوابط الرقابية.

3. خصائص مخاطر تكنولوجيا المعلومات

تتميز مخاطر تكنولوجيا المعلومات بمجموعة خصائص التي تجعلها مختلفة عن الكثير من المخاطر التقليدية.

فهي مخاطر سريعة التغير وديناميكية، لأن التكنولوجيا نفسها تتطور بسرعة. فما يعد آمنا اليوم قد يصبح ضعيفا خلال فترة قصيرة، وذلك بسبب ظهور ثغرات جديدة أو أساليب هجوم أكثر تعقيدا.

هي مخاطر غير مرئية وغير ملموسة مقارنة بالمخاطر المادية، فمثلا قد يحدث اختراق أو تسرب معلومات دون أن تكتشفه المؤسسة فورا.

ترتبط ارتباطا وثيقاً بدرجة اعتماد المؤسسة على الأنظمة الرقمية، الشبكات، وقواعد البيانات، فهي لا تقتصر على الأعطال التقنية أو فقدان الأجهزة والبرمجيات بل تمتد لتشمل مخاطر أمن المعلومات مثل اختراق الأنظمة، تسريب البيانات، فقدان السرية، المساس بسلامة المعلومات وغيرها.

تتميز هذه المخاطر بطابعها المتداخل إذ أن خلا تقنيا محدودا قد يتحول الى اضطراب واسع يمكن أن يؤثر في العمليات التشغيلية، العلاقة مع الزبائن، سمعة المؤسسة وكذلك القرار الإداري.

تزداد خطورة هذه المخاطر بسبب اعتماد المؤسسات الحديثة على الترابط الشبكي، التعاملات الالكترونية، الحوسبة السحابية وكذلك العمل عن بعد. وهذا ما يجعل حدود الخطر تتجاوز الاطار الداخلي للمؤسسة لتشمل كل من الزبائن ، الموردين، الشركاء ومختلف الفاعلين في البيئة الرقمية. فهي بذلك مخاطر مترابطة لأن أي خلل في نظام واحد قد يؤثر في عدة أنظمة أخرى بسبب التكامل بين التطبيقات، قواعد البيانات، الشبكات والخدمات السحابية.

سرعة انتشارها، صعوبة التنبؤ بها، قابلية اثارها للتضاعف بسرعة وارتباطها المباشر بعناصر استراتيجية حساسة مثل استمرارية النشاط، القدرة التنافسية، الثقة الرقمية، حماية البيانات.

هي مخاطر عابرة للحدود لأن الهجوم او الخلل يمكن ان يأتي من خارج الدولة او بنية تحتية رقمية عالمية.

ويرى (Baskerville, Siponen, 2002) أن خصوصية المخاطر المعلوماتية تكمن في كونها تجمع بين البعد التقني والبعد السلوكي والتنظيمي، لذلك لا بد من التعامل معها باعتبارها مشكلة حوكمة وإدارة وثقافة مؤسسية.

4. تصنيف مخاطر تكنولوجيا المعلومات

يمكن تصنيف مخاطر تكنولوجيا المعلومات إلى عدة فئات رئيسية، نذكر منها ما يلي:

- **المخاطر التقنية (التكنولوجية):** تشمل التهديدات والمخاطر المتعلقة بالجانب الفني والتقني للأنظمة والنتيجة عن الأعطال، الثغرات أو سوء تصميم البنية التقنية. وتشمل على سبيل المثال: الهجمات الالكترونية (التصيد، البرمجيات الضارة).

وقد بين (Tanenbaum, Wetherall, 2010) أن البنى الشبكية، رغم أهميتها في ربط الأنظمة، قد تصبح مصدرا لمخاطر متعددة إذا لم تصمم وفق مبادئ الأمان، مراقبة الأداء، وإدارة الازدحام.

- **مخاطر أمن المعلومات :** تشمل هذه الفئة من المخاطر كل ما يهدد سرية المعلومات وسلامتها وتوافرها. مثل الوصول غير المصرح به، سرقة البيانات، البرمجيات الخبيثة، التلاعب بالمعلومات، التصيد الإلكتروني، تسريب المعطيات الحساسة. تعطيل الخدمة. اذ يؤكد (Stallings, 2016) أن أمن المعلومات يجب أن يبنى على ضوابط متعددة، تشمل التشفير، التحكم في الوصول، أمن الشبكات، المصادقة، النسخ الاحتياطي، وخطط الاستجابة للحوادث.
- **المخاطر البشرية :** يعد العنصر البشري أهم مصادر مخاطر تكنولوجيا المعلومات. لأن المخاطر يمكن أن تنتج عن الإهمال، ضعف التكوين، سوء استخدام النظام، مشاركة كلمات المرور، فتح رسائل مشبوهة، أو تجاوز الإجراءات الرسمية. وقد أشار (Peltier, 2016) إلى أن برامج أمن المعلومات الناجحة لا تقوم على الأدوات التقنية فحسب، بل تحتاج إلى وعي المستخدمين، سياسات واضحة، تدريب مستمر وثقافة أمنية داخل المؤسسة.
- **المخاطر التنظيمية والإدارية:** تنشأ هذه المخاطر من ضعف الهياكل والعمليات الإدارية وكذلك عندما تفتقر المؤسسة إلى سياسات واضحة لإدارة التكنولوجيا، أو عندما تكون المسؤوليات غير محددة، أو غياب الرقابة الداخلية على المشاريع الرقمية. ومن أمثلة أخطاء في اتخاذ القرار أو في سير الاجراءات، ضعف حوكمة تكنولوجيا المعلومات، غياب خطة أمنية، ضعف إدارة الصلاحيات، سوء اختيار الموردين، وفشل مشاريع نظم المعلومات وغيرها. تؤدي هذه المخاطر التنظيمية الى فوضى في العمل وانخفاض الكفاءة التشغيلية.
- وقد أوضح (Weill, Ross, 2004) أن حوكمة تكنولوجيا المعلومات تحدد من يمتلك حق اتخاذ القرار التقني ومن يتحمل المسؤولية عن نتائجه، مما يجعلها عنصرا أساسيا في الحد من المخاطر الرقمية.
- **المخاطر القانونية:** تتمثل في المخاطر المرتبطة بعدم الالتزام للمعايير والقوانين المحلية والدولية في سياق تكنولوجيا المعلومات وتشمل مثلا: خرق قوانين

حماية البيانات، أو عدم تطبيق اشتراطات الأمن السيبراني، أو عدم احترام معايير المتعلقة الملكية الفكرية، التوقيع الإلكتروني، الجرائم الإلكترونية، الأرشفة الرقمية، والخصوصية. وقد يؤدي ضعف الامتثال إلى هذه القوانين إلى عقوبات مالية، دعاوى قضائية، فقدان الثقة، منع المؤسسة من ممارسة بعض الأنشطة.

- **مخاطر الاستمرارية:** تشمل هذه الفئة المخاطر التي تؤدي إلى توقف الخدمات أو عدم قدرة المؤسسة على استعادة نشاطها بعد حادث تقني أو أمني. ومن أمثلتها: فقدان البيانات، غياب النسخ الاحتياطي، ضعف خطط التعافي من الكوارث، الاعتماد على خادم وحيد أو مزود خدمة وحيد. فقد أكد (Snedaker, 2013) أن استمرارية الأعمال والتعافي من الكوارث لا يتعلقان فقط باسترجاع الأنظمة، بل بضمان قدرة المؤسسة على مواصلة وظائفها الحرجة في ظل الأزمات.

- **مخاطر الموردين والخدمات السحابية:** ظهرت هذه المخاطر نتيجة توسع استخدام الحوسبة السحابية، حيث أصبحت المؤسسات تعتمد على مزودين خارجيين لتخزين البيانات وتشغيل التطبيقات. هذا الاعتماد كما أنه يوفر مزايا عديدة، فإنه يخلق مخاطر جديدة مثل فقدان السيطرة المباشرة على البيانات، صعوبة الانتقال من مزود إلى آخر، انقطاع الخدمة، ومخاطر الامتثال عبر الحدود. حيث أشار (Mahmood, et al. 2013) أن الحوسبة السحابية تتطلب نمطا خاصا من إدارة المخاطر، لأنها تنقل جزء من البنية التحتية والبيانات إلى بيئات لا تتحكم فيها المؤسسة بالكامل.

- **المخاطر الاستراتيجية:** ترتبط هذه المخاطر بالرؤية والاهداف طويلة المدى للمؤسسة. وتشمل المخاطر التي تنجم عن تحولات السوق، أو المنافسة الشديدة، أو أخطاء في رسم الاستراتيجية مثال اذا اتبعت مؤسسة استراتيجية تسويق خاطئة وتكلفت عن متابعة اتجاهات السوق التكنولوجية السريعة، قد تفقد مركزها التنافسي أو تحقق خسائر مالية كبيرة ولذلك تركز ادارة

المخاطر الاستراتيجية على توقع هذه السيناريوهات وضمان توافق القرارات الحالية مع الأهداف المستقبلية.

5. مصادر مخاطر تكنولوجيا المعلومات

تنشأ مخاطر تكنولوجيا المعلومات من تفاعل عدة مصادر داخلية وخارجية.

- المصادر الداخلية: يقصد بالمصادر الداخلية هي تلك المخاطر التي تنشأ من داخل المؤسسة نفسها، نتيجة خلل في مواردها البشرية أو أنظمتها التقنية أو سياستها التنظيمية أو إجراءات الرقابية. وتشمل هذه المخاطر ما يلي:
 - الأخطاء البشرية غير المقصودة أثناء ادخال البيانات ومعالجتها.
 - ضعف تكوين العاملين في استخدام الأنظمة المعلوماتية.
 - سوء استخدام كلمات المرور أو مشاركتها بين الموظفين.
 - غياب سياسات واضحة لأمن المعلومات.
 - ضعف الرقابة الداخلية على صلاحيات الدخول الى الأنظمة.
 - الأعطال التقنية في الأجهزة، الخوادم، البرمجيات، أو قواعد البيانات.
 - ضعف النسخ الاحتياطي للبيانات.
 - عدم وجود خطة لاستمرارية النشاط واسترجاع معلومات عند وقوع الأزمات.
 - اتخاذ الادارة لقرارات تقنية دون تقييم كاف للتكلفة، الأثر، الأمن والمواءمة الاستراتيجية، مقاومة بعض العاملين للتغيير الرقمي وعدم احترام الاجراءات.
 - سوء تنظيم المسؤوليات والصلاحيات داخل النظام المعلوماتي.

- تتميز هذه المخاطر بأنها ترتبط مباشرة بطريقة ادارة المؤسسة لمواردها الرقمية والبشرية، لذلك فان التحكم فيها يتطلب تحسين الحوكمة الداخلية، تكوين العاملين، تطوير السياسات الأمنية، وتحديد المسؤوليات بدقة.
- المصادر الخارجية: المخاطر التي تأتي من خارج المؤسسة حيث لا تكون ناتجة مباشرة عن العاملين أو الأنظمة الداخلية، بل تنشأ عن ظروف و أطراف خارجية يمكنها أن تهدد امن المعلومات واستمرارية النشاط ومن أهم هذه المخاطر:

- الهجمات السيبرانية.
- اختراق الأنظمة والشبكات، فشل شبكات الاتصال.
- الفيروسات والبرمجيات الخبيثة.
- محاولات التصيد الإلكتروني.
- سرقة البيانات من طرف قراصنة أو جهات منافسة.
- تعطيل الخدمات الإلكترونية أو انقطاع الكهرباء.
- الكوارث الطبيعية التي قد تؤثر في مراكز البيانات.
- المخاطر المرتبطة بالمنصات الرقمية.
- التغيرات القانونية.

تتميز هذه المخاطر بصعوبة التحكم فيها بشكل كامل لأن مصدرها يكون خارج حدود المؤسسة. لذلك تحتاج المؤسسة إلى أنظمة حماية متطورة وبقظة
تكنولوجية مستمرة، وآليات رقابة خارجية، بالإضافة إلى استراتيجيات
استجابة سريعة للأزمة الرقمية.

- المصادر المختلطة: تعد المخاطر المختلطة أكثر تعقيدا لأنه تنتج عن تفاعل عوامل داخلية وخارجية في نفس الوقت، فهي لا ترجع إلى خلل داخلي أو تهديد خارجي مستقل، ولكن تظهر عندما يلتقي ضعف داخلي مع تهديد خارجي.

ومن أمثلتها:

- تعرض المؤسسة لاختراق خارجي بسبب ضعف كلمات المرور الداخلية.
 - تسريب البيانات نتيجة خطأ موظف واستغلاله من طرف جهة خارجية.
 - توقف الخدمة بسبب اعتماد المؤسسة على مورد خارجي دون وجود خطة بديلة داخلية.
 - فشل نظام الحوسبة السحابية بسبب ضعف إدارة العلاقة مع مقدم الخدمة.
 - حدوث هجوم إلكتروني بسبب عدم تحديث البرامج من طرف المؤسسة.
 - ضعف حماية العمل عن بعد، مما يسمح للأطراف الخارجية بالدخول إلى النظام.
 - استخدام موظف لجهازه الشخصي غير مؤمن، مما يفتح المجال لاختراق الشبكة الداخلية.
 - تسرب البيانات بسبب ضعف سياسة الصلاحيات داخل المؤسسة مع وجود طرف خارجي غير موثوق.
- هذه المخاطر أكثر خطورة لأنها تجمع بين الضعف الداخلي والتهديد الخارجي، وهذا ما يجعل آثارها أكثر اتساعاً وصعوبة في معالجتها. وتتطلب إدارة هذا النوع من المخاطر مقارنة شاملة تجمع بين أمن المعلومات، الحوكمة الرقمية، إدارة الموردين، تكوين العاملين، والرقابة المستمرة للأنظمة.

6. أثر مخاطر تكنولوجيا المعلومات على المؤسسة

تترتب عن مخاطر تكنولوجيا المعلومات آثار عديدة تمس عدة مستويات:

- **الأثر المالي:** قد يترتب عن مخاطر تكنولوجيا المعلومات خسائر مباشرة بالنسبة للمؤسسة مثل تكاليف إصلاح الأنظمة، دفع تعويضات، استعادة البيانات، أو شراء حلول أمنية طارئة. كما قد يترتب عنها خسائر غير مباشرة بسبب توقف النشاط، مثل فقدان الزبائن أو تراجع الإيرادات ، أو تعويض الزبائن المتضررين.
- **الأثر التشغيلي:** أصبحت نظم المعلومات جزءا من الوظائف التشغيلية للمؤسسة، وليست فقط وظائف مساعدة. وعليه فان توقف نظم المعلومات يمكن أن يؤدي إلى تعطيل عمليات البيع، الإنتاج، المحاسبة، الموارد البشرية أو سلسلة التوريد، ضعف التنسيق بين المصالح، انخفاض جودة الخدمة، وتهديد استمرارية الأنشطة التشغيلية.
- **الأثر القانوني:** تظهر الآثار القانونية لمخاطر تكنولوجيا المعلومات عندما يؤدي الخل الرقعي إلى انتهاك القوانين المتعلقة بحماية البيانات، سرية المعلومات، الأمن السيبراني ، أو حقوق المتعاملين. وقد ينتج عن ذلك تعرض للمؤسسة لغرامات مالية ، دعوى قضائية، مساءلة تنظيمية، أو فقدان تراخيص واعتمادات ضرورية لممارسة النشاط.
- **آثار على السمعة:** تؤثر مخاطر تكنولوجيا المعلومات على سمعة المؤسسة من خلال إضعاف ثقة الزبائن ، الشركاء، الموردين، في قدرتها على حماية البيانات وضمان استمرارية الخدمات. وتعد من أخطر الآثار لأن استعادة الثقة المؤسسية بعد حدوث اختراق أو تسريب معلوماتي قد يتطلب وقتا طويلا وجهودا مالية واتصالية كبيرة. ويرى (Solove, 2013) أن الخصوصية وحماية البيانات ليستا مجرد التزام قانوني، بل هما عنصرا مرتبطان بالكرامة والثقة، والعلاقة بين الفرد والمؤسسة.
- **الأثر الاستراتيجي:** على المستوى الاستراتيجي، فيكمن لمخاطر التكنولوجيا المعلومات أن تؤدي إلى إضعاف القدرة التنافسية للمؤسسة، تعطيل المشاريع التحول الرقمي، الحد من الابتكار، وفقدان فرص النمو. كما أن المساس بالأصول المعلوماتية للمؤسسة يمكن أن يؤثر في جودة القرارات الاستراتيجية وفي قدرها على التكيف مع بيئة الأعمال الرقمية.

7. إدارة مخاطر تكنولوجيا المعلومات

إدارة مخاطر تكنولوجيا المعلومات هي عملية منهجية تهدف إلى تحديد المخاطر، تحليلها، تقييمها، معالجتها، مراقبتها، والتواصل بشأنها. فهي ليست عملية تقنية مؤقتة، بل دورة مستمرة مرتبطة بحوكمة المؤسسة.

ويعتبر نظام ISO/IEC 27005:2022 المرجع الأكثر تخصصاً في مجال تكنولوجيا المعلومات وأمن المعلومات، لأنه يوجه المؤسسات في كيفية إدارة مخاطر أمن المعلومات بطريقة منسجمة مع متطلبات نظام إدارة أمن المعلومات ISO/IEC 27001. وعليه فإن معيار ISO يقدم مقاربة منظمة لتحديد وتقييم ومعالجة مخاطر أمن المعلومات داخل مختلف أنواع المؤسسات.

وتشمل إدارة المخاطر المراحل الرئيسية الآتية:

- **تحديد المخاطر Identification:** تتمثل هذه المرحلة في جمع معلومات شاملة عن جميع التهديدات المحتملة التي قد تؤثر على الأنظمة التقنية، ويشمل ذلك تحليل البنية التحتية، الأصول التقنية، ومكونات البرمجية، والبيانات، بالإضافة إلى مراجعة الخبرات السابقة والاستعانة بآراء الخبراء لتكوين قائمة بالمخاطر التي يمكن أن تؤثر في هذه الأصول التقنية مثل: الهجمات السيبرانية، الأعطال التقنية، الأخطاء البشرية، ضعف كلمات المرور، سوء إدارة الصلاحيات.
- **تحليل المخاطر Analysis:** بعد تحديد المخاطر، يتم تقدير احتمال وقوع الخطر، وحجم أثره المحتمل على المؤسسة (سواء كان مالياً، تشغيلياً، تنظيمياً، أو سمعته). فقد يكون الخطر منخفضاً إذا كان أثره محدوداً واحتمال حدوثه ضعيفاً، وقد يكون مرتفعاً إذا كان من المحتمل أن يؤدي إلى توقف النشاط، فقدان البيانات، تسريب معلومات حساسة، أو إلحاق ضرر مالي وسمعي بالمؤسسة.
- **تقييم المخاطر Evaluation:** بناءً على تحليل المخاطر، يتم ترتيب المخاطر حسب أولويتها أو مستوى نضجها، وذلك عن طريق دمج قيم الاحتمال والتأثير

وكذلك تحديد المخاطر الحرجة التي يجب التركيز عليها أي مقارنة مستوى الخطر بمعايير القبول التي حددتها المؤسسة، بهدف معرفة ما إذا كان الخطر مقبولا أو يحتاج إلى معالجة مباشرة أو يمكن تجاهله.

● **معالجة المخاطر Treatment:** في هذه المرحلة يتم وضع استراتيجيات مناسبة للتعامل مع كل مخاطر مصنفة حسب أولويتها. تتضمن استراتيجيات المعالجة:

- اما تخفيف المخاطر عن طريق الإجراءات الوقائية أو الرقابة الإضافية.
- أو تحويل المخاطر إلى جهة أخرى عن طريق التأمين والتعاقد مع مزود متخصص.
- أو قبول أو تحمل المخاطر وذلك ضمن الحدود المقبولة.
- أو تجنب المخاطر بتغيير خطة العمل حيث يطور لكل مخاطر خطة عمل تفصيلية تشمل الإجراءات التدابير الفنية، والتنظيمية المطلوبة للحد من تأثيرها.

وتشمل الضوابط الممكنة: التشفير، النسخة الاحتياطي، إدارة الصلاحيات، المصادقة المتعددة، تحديث الأنظمة، مراقبة الشبكات، تدريب العاملين، وكذلك خطط استمرارية النشاط واسترجاع البيانات.

● **المراقبة والمراجعة: Monitoring and Review:** إدارة المخاطر ليست عملية مؤقتة عند التنفيذ، بل هي تشمل مراقبة دائمة وتعلم مستمر لمستجدات المخاطر وكذا التغيرات في بيئة العمل. ويشمل ذلك اختيار الضوابط الأمنية بانتظام وتحديث تحليل المخاطر عند ظهور تكنولوجيا جديدة وضبط الاستراتيجيات في ضوء الدروس المكتسبة، وبهذا الأسلوب الدوري، تبقى إدارة المخاطر قائمة على الحيطة والحذر ومواكبة المستجدات في بيئة رقمية...

8. مصفوفة المخاطر Risk Matrix

تعد مصفوفة المخاطر أداة تحليل وتعلم مرئية تستخدم في إدارة المخاطر وذلك من أجل تحديد مستوى الخطر وترتيب به حسب درجة احتمال وقوعه وحجم أثره على المؤسسة. وتقوم هذه المصفوفة عن الجمع بين بعدين أساسيين هما: احتمالية حدوث الخطر وشدة

تأثيره على المؤسسة، وبناء على تقاطع هذين البعدين ، يتم تصنيف المخاطر إلى مستويات مختلفة مثل: مخاطر ضعيفة، متوسطة، مرتفعة أو حرجية. فمثلا إذا اعتبر خطر ما احتماليته عالية وتأثيره كبير، في يصنف في أعلى درجات الخطورة، ومن ثم يتم تخصيص جهود أكبر للتعامل معه، وعليه فإن هذه المصفوفة تساعد في ترتيب أولويات التدخل بحيث تعالج أولا المخاطر ذات الاحتمال العالي والأثر الكبير خاصة تلك التي قد تؤثر في استمرارية النشاط، أمن المعلومات، الأداء المالي، السمعة أو الامتثال القانوني.

جدول 2: شكل مبسط لمصفوفة المخاطر

التأثير/الاحتمالية	منخفضة (1)	متوسطة (2)	عالية (3)
عالية (3)	متوسط (1X3)	عالي (2X3)	عالي جدا (3X3)
متوسطة (2)	منخفض (1X2)	متوسط (2X2)	عالي (3X2)
منخفضة (1)	منخفض (1X1)	منخفض (2X1)	متوسط (3X1)

تهدف مصفوفة المخاطر إلى مساعدة المؤسسة على الانتقال من التعامل العشوائي مع المخاطر إلى التعامل المنهجي والمنظم. فهي تسمح بتحديد المخاطر الأكثر خطورة، ترتيبها حسب الأولوية، اختيار إجراءات المعالجة المناسبة، وتخصيص الموارد المالية والتقنية والبشرية بطريقة عقلانية، كما تساعد الإدارة العليا على اتخاذ القرارات المناسبة.

9. الأمن السيبراني كمدخل التحكم في المخاطر

الأمن السيبراني هو مجموعة السياسات، التقنيات، الممارسات والضوابط الهادفة إلى حماية الأنظمة والشبكات والبيانات من الاستخدام غير المشروع أو التعطيل أو التغيير أو التدمير. وهو يمثل أحد المكونات الأساسية في إدارة مخاطر تكنولوجيا المعلومات.

وقد يعد NIST Cybersecurity Framework أحد أهم الأطر المرجعية العالمية في مجال الأمن السيبراني وإدارة المخاطر التقنية، وقد طوره المعهد الوطني الأمريكي للمعايير والتكنولوجيا NIST وذلك لمساعدة المؤسسات على فهم مخاطر الأمن السيبراني، تنظيمها، قياسها، تقليلها بطريقة منهجية. ويتميز هذا الإطار بأنه لا يقتصر على نوع من المؤسسات بل يمكن استعماله في مختلف أنواع المؤسسات مهما كان حجمها، أو قطاع نشاطها لأنه يقوم على مبادئ مرنة قابلة للتكيف مع طبيعة منظمة. وقد أصبحت النسخة الجديدة NIST CSF 2.0 منظمة حول ستة وظائف أساسية هي الحوكمة، التحديد، الحماية، الكشف، الاستجابة، الاسترداد والتعافي.

- **الحوكمة السيبرانية:** وهي تعني تحديد سياسات الأمن السيبراني، توزيع المسؤوليات، تحديد مستوى تقبل المخاطر وربط الأمن السيبراني بالاستراتيجية العامة للمؤسسة.
- **التحديد:** تهدف هذه الوظيفة إلى معرفة ما يجب حمايته داخل المؤسسة. وتشمل تحديد الأصول الرقمية، قواعد البيانات، تطبيقات الشبكات، المستخدمين الموردين، العمليات الحيوية والتهديدات المحتملة.
- **الحماية:** تركز وظيفة الحماية على وضع الضوابط والإجراءات التي تمنع وقوع الحوادث السيبرانية أو تقلل احتمال حدوثها ومن أمثلتها: إدارة كلمات المرور، المصادقة المتعددة العوامل، التشفير، النسخ الاحتياطي، تحديث الأنظمة، التكوين المستمر للعاملين.
- **الكشف:** تتمثل هذه الوظيفة في اكتشاف الحوادث أو الأنشطة غير العادية في الوقت المناسب، وتشمل مراقبة الشبكات، تتبع محاولات الدخول، تحليل السجلات، استعمال أنظمة كشف الاختراقات، مراقبة السلوك غير الطبيعي داخل الأنظمة الرقمية.
- **الاستجابة:** تتركز هذه الوظيفة على كيفية تعامل المؤسسة مع الحادث السيبراني عند وقوعه، وتشمل تحديد المسؤوليات، احتواء الحادث، الاتصال بالأطراف المعنية، تحليل سبب الخلل، تقليل الضرر واتخاذ الإجراءات التصحيحية.

- الاسترداد أو التعافي: تهدف وظيفة التعافي إلى استرجاع الأنظمة والخدمات والبيانات بعد وقوع الحادث وتشمل خطط استمرارية النشاط، خطة استرجاع البيانات، إعادة تشغيل الأنظمة، تعليم الدروس المستفادة، وتحسين الإجراءات المستقبلية.

ومن هفإن NIST لا ينظر إلى الأمن السيبراني باعتباره مجرد أدوات تقنية ، بل باعتباره نظام متكامل لإدارة المخاطر، حماية الأصول المعلوماتية، دعم استمرارية النشاط وتعزيز الثقة الرقمية داخل المؤسسة.

10. الرقابة الداخلية على تكنولوجيا المعلومات

تعد الرقابة الداخلية على تكنولوجيا المعلومات من أهم أدوات الحد من المخاطر. وهي تشمل السياسات والإجراءات والأنشطة التي تضمن أن الأنظمة تعمل بطريقة موثوقة وأمنة ومتوافقة مع أهداف المؤسسة.

وتنقسم الضوابط الرقابية إلى:

- ضوابط وقائية: مثل التحكم في الوصول، التشفير، الفصل بين المهام، والتكوين الأمني.
- ضوابط كاشفة: مثل أنظمة المراقبة، التدقيق الدوري، سجلات الأحداث، والتنبيهات الأمنية.
- ضوابط تصحيحية: مثل خطط الاستجابة للحوادث، النسخ الاحتياطي، واستعادة البيانات.

وقد أكد (Romney, Steinbart, 2017) أن الرقابة على نظم المعلومات المحاسبية والإدارية ضرورية لضمان جودة البيانات، منع الغش، حماية الأصول، ودعم صدقية التقارير.

11. مخاطر جودة البيانات

لا تقتصر مخاطر تكنولوجيا المعلومات على الاختراقات والهجمات، بل تشمل كذلك مخاطر جودة البيانات. حيث أن البيانات يمكن أن تكون ناقصة، مكررة، غير دقيقة، قديمة، وغير ملائمة لعملية اتخاذ القرار.

ومنه تعد جودة البيانات شرطا أساسيا لجودة القرار، فإذا كانت البيانات خاطئة، فإن التقارير ولوحات القيادة والتحليلات ستكون مضللة، حتى لو كانت الأدوات التقنية متطورة. وقد أكد (Davenport, Prusak, 1998) أن المعرفة التنظيمية لا تتكون بمجرد امتلاك البيانات، بل من خلال تنظيمها، تفسيرها، تداولها واستخدامها بطريقة صحيحة.

ويزداد هذا النوع من المخاطر مع انتشار الذكاء الاصطناعي والتحليلات المتقدمة، لأن الخوارزميات تعتمد على البيانات، وإذا كانت هذه الأخيرة خاطئة أو منحازة فقد ينتج عنها قرارات غير فعالة وغير عادلة. ولذلك تعد حوكمة البيانات عنصرا أساسيا في التقليل من هذه المخاطر.

12. مخاطر التحول الرقمي

التحول الرقمي لا يعني اقتناء برامج حديثة أو رقمنة الوثائق فقط، ولكن يمتد إلى إعادة تصميم العمليات، ونماذج العمل والعلاقة مع الزبائن. وعليه فإنه يحمل مخاطر استراتيجية وتنظيمية هامة.

ومن أبرز مخاطر التحول الرقمي:

- فشل المشاريع الرقمية بسبب غياب الرؤية.
- مقاومة العاملين للتغيير.
- ضعف التكوين.
- عدم تكامل الأنظمة.
- تضخم التكاليف دون عائد واضح.
- الاعتماد على حلول غير ملائمة.
- التركيز على التكنولوجيا بدلا من القيمة التنظيمية.
- نقص الكفاءات الرقمية.

وقد أوضح (Westerman, et al., 2014) أن التحول الرقمي الناجح يتطلب الجمع بين القدرات التقنية والقيادة التحويلية، لأن التقنية وحدها لا تنتج تحولا إذا ما لم ترافق بتغيير في الثقافة والعمليات ونموذج الأعمال.

وعليه، فإن المخاطر الرقمية لا تدار من طرف مهندسين تقنيين فقط، بل تحتاج إلى مشاركة الإدارة العليا، الموارد البشرية، المالية، القانونية، التدقيق الداخلي، وإدارة الجودة.

ومنه فإن التحكم في هذا النوع من المخاطر يتطلب مقاربة حوكمية شاملة تقوم على وضوح الرؤية الاستراتيجية، تطوير البنية التحتية، حماية البيانات، تأهيل الموارد البشرية، إدارة التغيير، تقييم المخاطر، ومراقبة الأداء الرقمي بصورة مستمرة.

13. مخاطر الذكاء الاصطناعي والأنظمة الخوارزمية

مع اتساع استخدام الذكاء الاصطناعي في المؤسسات، ظهرت مخاطر جديدة تتعلق بالتحيز الخوارزمي، غياب الشفافية، صعوبة تفسير القرارات الآلية، انتهاك الخصوصية، الاعتماد المفرط على النماذج، وضعف التحكم في مخرجاتها.

ويظهر هذا النوع من المخاطر أن التقنية لا تكون دائما محايدة، فالخوارزمية تتعلم من بيانات قد تكون ناقصة أو منحازة، وتستخدم في قرارات حساسة مثل التوظيف، منح القروض، تقييم الأداء، التسعير. ويؤكد (Russell, Norvig, 2020) أن حوكمة الذكاء الاصطناعي يجب أن تقوم على الشفافية، العدالة، القابلية للتفسير، المسؤولية البشرية، وحماية البيانات.

وعليه لا يجب التعامل مع الذكاء الاصطناعي بوصفه بديلا كاملا عن القرار البشري، بل بوصفه أداة دعم تحتاج إلى إشراف ورقابة وتقييم مستمر. ومنه فإن إدارة مخاطر الذكاء الاصطناعي تتطلب مقاربة حوكمية شاملة تقوم على الشفافية، المساءلة، الرقابة البشرية، جودة البيانات، الامتثال القانوني، وأخلاقيات الاستخدام. بما يضمن توظيف الذكاء الاصطناعي كأداة لتعزيز الأداء، والابتكار دون الاضرار بحقوق الأفراد أو استقرار المؤسسة.

14. مخاطر الخصوصية وحماية البيانات

تعتبر الخصوصية من أهم القضايا المرتبطة بتكنولوجيا المعلومات. فالمؤسسات تجمع كميات كبيرة من البيانات عن الزبائن، العمال، الموردين والمستخدمين، وهذا ما يخلق مسؤولية قانونية وأخلاقية في كيفية جمع هذه البيانات وتخزينها ومعالجتها ومشاركتها.

ويرى (Solove, 2013) أن الخصوصية لا تتمثل فقط في إخفاء المعلومات، ولكن تتعلق بالتحكم في كيفية استخدام المعلومات الشخصية وبحماية الأفراد من إساءة استغلال بياناتهم.

وتظهر مخاطر الخصوصية في المؤسسة عندما تقوم بجمع بيانات أكثر مما تحتاج، أو تحتفظ بها لمدة غير مبررة، أو تشاركها مع أطراف أخرى دون أساس قانوني، أو تفشل في تأمينها ضد التسرب والاختراق.

15. مخاطر الاستعانة بالمصادر الخارجية

قد تلجأ المؤسسات إلى التعاقد مع مزودين خارجيين لتطوير التطبيقات، استضافة البيانات، إدارة الشبكات، توفير الخدمات السحابية أو الدعم التقني. ورغم أن هذا الخيار قد يقلل التكاليف ويزيد الكفاءة، إلا أنه يخلق العديد من المخاطر مثل فقدان السيطرة، ضعف مراقبة المورد، تسرب البيانات، عدم وضوح المسؤوليات، وصعوبة إنهاء التعاقد.

ويؤكد (Willcocks, Lacity, 2012) أن الاستعانة بالمصادر الخارجية في مجال تكنولوجيا المعلومات لا ينبغي أن تدار من زاوية التكلفة فقط، بل يجب أن تخضع لتحليل استراتيجي وقانوني ورقابي دقيق.

وعليه يجب أن تتضمن العقود الرقمية بنوداً واضحة حول السرية، مستوى الخدمة، حماية البيانات، حق التدقيق، مكان تخزين البيانات، خطط التعافي، والمسؤولية عند وقوع الحوادث.

16. إدارة الحوادث المعلوماتية

تعد إدارة الحوادث عنصراً أساسياً h في إدارة مخاطر تكنولوجيا المعلومات، لأنظمة وجود وسائل الوقاية، إلا أن المؤسسة لا يمكنها أن تضمن انعدام الحوادث بشكل مطلق. وتتم إدارة الحوادث بعدة مراحل هي:

- الاستعداد من خلال وضع السياسات، تشكيل فريق الاستجابة، إعداد أدوات المراقبة، وتدريب المستخدمين.
- الاكتشاف والتحليل وذلك من خلال التعرف على الحادث وتحديد طبيعته ونطاقه وأثره.
- الاحتواء وذلك من أجل منع انتشار الضرر إلى أنظمة أخرى.
- الإزالة والمعالجة لإزالة سبب الحادث وغلق الثغرة.
- التعافي من خلال إعادة الأنظمة إلى العمل الطبيعي.
- التعلم من خلال تحليل الحادث وتحديث الإجراءات والضوابط.

وقد أكد (Kral, 2012) أن فعالية الاستجابة للحوادث تعتمد على التحضير المسبق، وضوح الأدوار، سرعة الاتصال، وتوثيق الإجراءات.

17. استمرارية الأعمال والتعافي من الحوادث

تعني استمرارية الأعمال قدرة المؤسسة على مواصلة وظائفها الأساسية أثناء الأزمات، في حين التعافي من الكوارث فيركز على استعادة الأنظمة والبيانات بعد وقوع حادث.

ومن أدوات الاستمرارية: النسخ الاحتياطي، مواقع العمل البديلة، تكرار الخوادم، خطط التعافي، اختبارات دورية، تحديد الوظائف الحرجة، وتحديد الزمن المقبول للتوقف.

ويؤكد (Snedaker, 2013) أن خطة التعافي التي لا تختبر دوريا قد تمنح المؤسسة إحساسا زائفا بالأمان، لأن فعاليتها لا تظهر إلا عند التطبيق الفعلي أو المحاكاة المنظمة. وعليه لا يجب على خطط الاستمرارية أن تكون وثائق جامدة، بل أنظمة حية تراجع باستمرار وفق تغير الأنظمة والعمليات والمخاطر.

18. الثقافة الامنية داخل المؤسسة

لا يمكن بناء أمن معلومات قوي دون ثقافة أمنية تنظيمية داعمة. لأن الموظف الذي لا يقدر قيمة البيانات قد يتعامل معها بإهمال، رغم توفر المؤسسة على تقنيات متقدمة. لذلك تعتمد إدارة المخاطر الرقمية على بناء وعي جماعي بأن الأمن مسؤولية مشتركة.

وتشمل الثقافة الأمنية:

احترام سياسات الاستخدام، حماية كلمات المرور، التبليغ عن السلوكيات المشبوهة، عدم مشاركة المعلومات الحساسة، الالتزام بالصلاحيات، وكذلك فهم أثر الأخطاء الفردية على المؤسسة.

وقد أكد (Peltier, 2016) أن التدريب والتوعية يجب أن يكونا مستمرين ومتكيفين مع طبيعة المستخدمين، لأن التوعية العامة غير المنتظمة لا تكفي لتغيير السلوك الأمني.

19. منهجية مقترحة لتحليل مخاطر تكنولوجيا المعلومات في المؤسسة

يمكن تحليل مخاطر تكنولوجيا المعلومات داخل المؤسسة وفق الخطوات الآتية:

- تحديد نطاق الدراسة: نظام معين، قسم، مؤسسة كاملة أو مشروع رقمي.
- جرد الأصول المعلوماتية ذات القيمة.
- تصنيف الأصول حسب الحساسية والأهمية.
- تحديد التهديدات المحتملة.
- تحديد نقاط الضعف الموجودة.
- تقدير احتمال وقوع الخطر.
- تقدير أثر الخطر على السرية، السلامة والتوافر.
- ترتيب المخاطر حسب الأولوية.
- اقتراح الضوابط المناسبة.
- تحديد المسؤوليات ومؤشرات المتابعة.
- مراجعة النتائج دورياً.

وتتوافق هذه المنهجية مع منطق ISO/IEC 27005 الذي يربط إدارة المخاطر بالتحديد، التقييم، المعالجة، الاتصال والمراقبة.

خاتمة

تمثل مخاطر تكنولوجيا المعلومات إحدى القضايا المحورية في الإدارة الحديثة، لأنها تمس جوهر عمل المؤسسة الرقمية: البيانات، الأنظمة، الشبكات، التطبيقات... الخ. ولم تصبح هذه المخاطر شأنا تقنيا محصورا في قسم الإعلام الآلي، بل أصبحت قضية استراتيجية تتطلب تدخل الإدارة العليا، التدقيق الداخلي، الموارد البشرية، القانونية، المالية، والأمن السيبراني.

وتشمل مخاطر تكنولوجيا المعلومات تشمل أبعادا تقنية، بشرية، تنظيمية، قانونية، تشغيلية واستراتيجية. وللتحكم فيها يجب مقاربة شاملة تجمع بين إدارة المخاطر، الحوكمة، الرقابة الداخلية، الأمن السيبراني، جودة البيانات، استمرارية الأعمال والثقافة الأمنية. إن فهم هذه المخاطر يمثل شرطا أساسيا لتحليل المؤسسة الرقمية، تقييم مشاريع التحول الرقمي، وبناء قرارات إدارية قائمة على الوعي بالمخاطر بدل الاكتفاء بالحماس التقني.

أسئلة المناقشة:

- ما الفرق بين الخطر، التهديد، نقطة الضعف، والحادث المعلوماتي؟
- لماذا تعد مخاطر تكنولوجيا المعلومات قضية إدارية وليست تقنية فقط؟
- كيف تؤثر جودة البيانات في جودة القرار الإداري؟
- ما العلاقة بين الأمن السيبراني وحوكمة تكنولوجيا المعلومات؟
- لماذا أصبحت مخاطر الموردين والخدمات السحابية مهمة في المؤسسة الحديثة؟
- كيف يمكن للمؤسسة بناء ثقافة أمنية فعالة؟
- ما أهمية استمرارية الأعمال في تقليل أثر المخاطر الرقمية؟
- اشرح أهمية تقييم المخاطر التقنية في مؤسسة تعتمد على تكنولوجيا المعلومات مع إعطاء أمثلة.
- ناقش دور الثقافة التنظيمية في إدارة المخاطر في المجال التقني: كيف تؤثر الأخطاء البشرية وسوء التخطيط الإداري على فعالية إدارة المخاطر؟
- في دورة إدارة المخاطر: استخرج الفرق بين خطوة التحليل والتقييم في عملية تقييم المخاطر، مع توضيح كيف تتكامل مع خطوة المعالجة.
- اقترح إطار عمل لإدارة مخاطر تكنولوجيا المعلومات وشرح كيف يساهم في تنظيم مراحل إدارة المخاطر.
- بمساعدة مصفوفة المخاطر، صنف الآتي بناء على الاحتمالية والأثر:
 - ✓ وقوع هجوم فيروسات على شبكة الشركة.
 - ✓ انقطاع مؤقت للإنترنت.
 - ✓ تحديث تكنولوجي طارئ.

المحور الثالث

حوكمة تكنولوجيا المعلومات "الاطار المفاهيمي"

تمهيد

أصبحت تكنولوجيا المعلومات موردا استراتيجي ا داخل المؤسسة المعاصرة، بعد أن انتقلت من وظيفة تقنية داعمة إلى عنصر جوهري في صياغة الاستراتيجية، خلق القيمة، إدارة المخاطر، تحسين الأداء، دعم القرار، وكذلك تطوير نماذج الأعمال. الا أن هذا التحول جعل استخدام التكنولوجيا داخل المؤسسة يحتاج إلى إطار حوكمي واضح يضمن أن الاستثمارات الرقمية لا تنفذ بصورة عشوائية أو تقنية محضة، ولكن وفق منطق مؤسسي يربط التكنولوجيا باحتياجات أصحاب المصالح من جهة، وأهداف المؤسسة من جهة أخرى.

وعلى هذا الأساس، ظهرت حوكمة تكنولوجيا المعلومات باعتباره امتدادا لحوكمة المؤسسات، ولكنها أكثر تخصصا في مراقبة وتوجيه استخدام المعلومات والتقنيات الرقمية. لان المؤسسة لا تحتاج فقط إلى معلومات متقدمة وأنظمة تقنية، ولكن تحتاج أيضا إلى تحديد من يقرر في مجال التكنولوجيا، ومن يتحمل المسؤولية، كيف تقاس القيمة، وكيف تدار المخاطر، وكذلك كيف يضمن توافق التكنولوجيا مع الاستراتيجية العامة للمؤسسة.

فحسب (Weill, Ross, 2004) أن حوكمة تكنولوجيا المعلومات تعني تحديد حقوق القرار وأطر المساءلة التي تشجع السلوك المرغوب في استخدام تكنولوجيا المعلومات داخل المؤسسة.

وقد أكد (ياسين، 2005؛ السالمي، 2008؛ الطائي و العبادي، 2009) أن نجاح التكنولوجيا داخل المؤسسة لا يرتبط فقط باقتناء الأجهزة والبرمجيات، بل بمدى تكاملها مع التنظيم، الموارد البشرية، الثقافة الإدارية، إجراءات العمل، والرقابة المؤسسية. وعليه فإن حوكمة تكنولوجيا المعلومات تمثل حلقة وصل بين الإدارة العليا، ووظيفة تكنولوجيا المعلومات، المستخدمين، أصحاب المصالح، والمدققين.

1. مفهوم حوكمة تكنولوجيا المعلومات

نعرف حوكمة تكنولوجيا المعلومات إ على أنها الإطار الذي يضمن أن استخدام تكنولوجيا المعلومات داخل المؤسسة يتم بطريقة مسؤولة، وأن القرارات التقنية مرتبطة بالأهداف الاستراتيجية، وأن المخاطر الرقمية تتم إدارتها بوعي، وأن الموارد المعلوماتية تستخدم بكفاءة

كما يمكن تعريفها بأنها نظام من الهياكل والعمليات والآليات التي تسمح بتوجيه ومراقبة استخدام تكنولوجيا المعلومات داخل المؤسسة، بهدف تحقيق القيمة، إدارة المخاطر، ضمان الامتثال، تحسين الأداء، وحماية الأصول المعلوماتية.

وحسب (IT Governance Institute, 2003) فان حوكمة تكنولوجيا المعلومات هي جزء من حوكمة المؤسسة ككل ، وتتمثل في القيادة والهياكل التنظيمية والعمليات التي تضمن أن تكنولوجيا المعلومات تدعم استراتيجية المؤسسة وأهدافها . كما يرى (De Haes, Van Grembergen, 2015) أن حوكمة تكنولوجيا المعلومات تهدف إلى تحقيق المواءمة بين الأعمال والتكنولوجيا، وخلق القيمة من الاستثمارات الرقمية، مع ضبط المخاطر والأداء.

أما (ياسين، 2005)، فيرى أن فهم حوكمة تكنولوجيا المعلومات يتم من خلال تقاطع ثلاثة مجالات: نظم المعلومات الإدارية، الإدارة الإلكترونية، والرقابة على المعلومات . و أن نظم المعلومات لا تحقق فعاليتها إلا عندما ترتبط بالقرارات الإدارية وتدعم التخطيط والرقابة والتنسيق. في حين أكد (السالمي، 2008) أن إدارة المعلومات داخل المؤسسة تحتاج إلى تنظيم للموارد التقنية، البشرية، والإجرائية بما يخدم الأداء المؤسسي. وعليه فإن حوكمة تكنولوجيا المعلومات تمثل مرحلة أكثر تقدم لأنها لا تكتفي بإدارة التكنولوجيا، بل توجهها وتربطها بالأهداف العليا للمؤسسة.

2. الفرق بين ادارة تكنولوجيا المعلومات وحوكمة تكنولوجيا المعلومات

تختلف إدارة تكنولوجيا المعلومات عن حوكمة تكنولوجيا المعلومات، ففي أن الإدارة تهتم بالتشغيل اليومي للخدمات التقنية، من صيانة الأنظمة، إدارة الشبكات، معالجة الحوادث، تطوير التطبيقات، دعم المستخدمين، وتحديث البنية التحتية. أما الحوكمة فتهم بمن يملك حق القرار، وكيف تحدد الأولويات، كيف يتم تقييم الاستثمارات التقنية، وكيف تدار المخاطر، وكيف تقاس مساهمة التكنولوجيا في تحقيق أهداف المؤسسة.

وعليه فان إدارة تكنولوجيا المعلومات تجيب على السؤال: كيف نشغل التكنولوجيا بكفاءة؟ في حين أن حوكمة تكنولوجيا المعلومات فتجيب عن السؤال: كيف نضمن أن التكنولوجيا تستخدم بشكل صحيح وتحقق القيمة المطلوبة؟

وقد ميز معيار ISO/IEC 38500 الذي يعتبر من المراجع المهمة في حوكمة المؤسسة لتكنولوجيا المعلومات، بين الحوكمة والإدارة حيث أن القيادة العليا تكون مسؤولة عن تقييم استخدام تكنولوجيا المعلومات ، وتوجيهه ومراقبته، بينما تتولى الإدارة تنفيذ القرارات والسياسات وتحقيق الأهداف الموضوعية.

وهذا التمييز بين الحوكمة والإدارة في تكنولوجيا المعلومات مهم جدا، لأن ضعف الحوكمة قد يؤدي إلى وجود قسم تقني نشيط من الناحية التشغيلية لكنه غير مرتبط بالاستراتيجية ، وفي المقابل يمكن ان تكون المؤسسة ذات رؤية رقمية طموحة، لكنها تفشل في التنفيذ إذا كانت الإدارة التقنية ضعيفة. وعليه فالمؤسسة بحاجة إلى وجود تكامل بين الإدارة والحوكمة.

3. نشأة وتطور حوكمة تكنولوجيا المعلومات

ظهرت حوكمة تكنولوجيا المعلومات نتيجة عدة تحولات متراكمة. ففي البداية، كانت التكنولوجيا تستخدم داخل المؤسسات لأتمت العمليات الإدارية البسيطة، مثل الرواتب، المحاسبة، المخزون، والفوترة. وفي هذه المرحلة، كانت التكنولوجيا تعد وظيفة مساعدة وتركز أساسا على الكفاءة التشغيلية (Laudon, Laudon, 2022).

ومع انتشار نظم المعلومات الإدارية أصبحت التكنولوجيا تدعم التخطيط والرقابة واتخاذ القرار. وقد أوضح (ياسين، 2005؛ العبادي، 2009) أن نظم المعلومات الإدارية أصبحت وسيلة ضرورية لتحسين فعالية الإدارة الحديثة، لأنها توفر المعلومات المناسبة في الوقت المناسب وبالشكل المناسب.

ومع ظهور الإنترنت، التجارة الإلكترونية، قواعد البيانات المتقدمة، الحوسبة السحابية، والذكاء الاصطناعي، تحولت التكنولوجيا إلى مورد استراتيجي يؤثر في النموذج الاقتصادي للمؤسسة وعلاقتها بالسوق. و عليه، لم يعد السؤال هو: كيف نستخدم التكنولوجيا؟ بل أصبح: كيف نحكم التكنولوجيا؟ ومن يقرر بشأنها؟ وكيف نضمن أنها تخلق قيمة ولا تولد مخاطر؟

وقد تطورت الأطر المرجعية لحوكمة تكنولوجيا المعلومات استجابة لهذه الحاجة. فقد أصبح COBIT من أشهر الأطر الدولية لحوكمة وإدارة تكنولوجيا المعلومات، حيث يربط بين

أهداف المؤسسة، أهداف تكنولوجيا المعلومات، العمليات، الرقابة، الأداء، والمخاطر. حيث تطور اطار COBIT من إطار موجه للرقابة والتدقيق إلى إطار أوسع لحوكمة وإدارة معلومات وتكنولوجيا المؤسسة .

4. أهمية حوكمة تكنولوجيا المعلومات

تنبع حوكمة تكنولوجيا المعلومات من كونها تسمح للمؤسسة بتحويل التكنولوجيا من مركز تكلفة إلى مصدر قيمة. فالمؤسسة قد تنفق مبالغ كبيرة على البرمجيات، الشبكات، الأنظمة السحابية أو مشاريع التحول الرقمي، لكنها لا تحقق النتائج المتوقعة إذا غابت الحوكمة. وعليه فان حوكمة تكنولوجيا المعلومات تسعى الى ضمان أن الانشطة وقرارات قسم تقنية المعلومات تخدم مصلحة المؤسسة العليا. ويمكن تلخيص أهم الأهداف الجوهرية لحوكمة تكنولوجيا المعلومات فيما يلي:

- **التوافق الاستراتيجي:** التأكد من مواءمة استراتيجية تقنية المعلومات مع الاستراتيجية العامة للمؤسسة. يعني ذلك أن كل مشروع تقني أو نظام معلومات جديد ينبغي أن يرتبط مباشرة بأهداف العمل والمتطلبات التي تضعها الادارة العليا. فالحوكمة تساعد على ضمان أن مشاريع تكنولوجيا المعلومات لا تختار بناء على الانهار، بل بناء على الأهداف الاستراتيجية، وعليه فان (Henderson, Venkatraman, 1993) يرى أن المواءمة الاستراتيجية بين الأعمال وتكنولوجيا المعلومات تعد شرطاً أساسياً لتحقيق القيمة من التكنولوجيا. و يؤكد (ياسين، 2018) أن الإدارة الإلكترونية لا يمكن أن تنجح إذا بقيت منفصلة عن رؤية المؤسسة، لأن التكنولوجيا يجب أن تخدم إعادة تنظيم العمل وتحسين الخدمة وليس فقط تحويل الإجراءات الورقية إلى إجراءات إلكترونية.

- **تحقيق القيمة من الاستثمارات الرقمية:** تعتبر الاستثمارات الرقمية مكلفة ومعقدة، وقد تفشل إذا لم تخضع لدراسة جدوى، متابعة، تقييم، ومساءلة. فالحوكمة تساعد على تحديد الأولويات، اختيار المشاريع، مراقبة التنفيذ، وقياس العائد. كما تعمل على ضمان ان الاستثمارات تكنولوجيا المعلومات تحقق قيمة فعلية وتحسن أداء الأعمال، وذلك من خلال ادارة محفظة المشاريع التقنية، بحيث يتم التركيز على المشاريع ذات

العائد الأعلى وربط العائد على الاستثمار في تكنولوجيا المعلومات بالأهداف المالية المؤقتة والتوقف عن المشاريع التي لا تحقق جدوى.

وفي هذا السياق أوضح أحد أخصائيي الحوكمة (Ross, et al., 2006) أن المؤسسات التي تمتلك بنية رقمية واضحة وقدرات حوكمية أفضل تكون قادرة على تنفيذ استراتيجياتها وتحقيق نتائج مستقرة.

وعليه فإن تكنولوجيا المعلومات تنتقل من مجرد مركز تكلفة الى كونها أصل استراتيجي يجب تعظيم قيمته، فمثلا يمكن للمؤسسة من خلال الحوكمة تقييم مدى رضا العملاء أو كفاءة العمليات بعد تطبيق نظام تكنولوجي جديد وذلك لمعرفة ما اذا كانت القيمة المتوقعة تحققت أم لا.

- إدارة وتحليل المخاطر الرقمية: تسمح الحوكمة بإدماج مخاطر التكنولوجيا في نظام المخاطر الكلي للمؤسسة. حيث لا يكفي وجود أدوات أمنية، بل لا بد من وجود سياسات، مسؤوليات، لجان، تقارير، مؤشرات، وخطط استمرارية. وهذا ما يؤكد عليه (Stallings, 2016؛ أبو نصر، 2017) وذلك بربط حماية البيانات بالإدارة والرقابة والثقافة المؤسسية.

وتعني إدارة المخاطر وضع الضوابط لضمان تحديد ومعالجة المخاطر المرتبطة بتكنولوجيا المعلومات بشكل استباقي، مثل مخاطر انقطاع الخدمات التقنية، وفشل المشاريع والأمن السيبراني، وفقدان البيانات. وذلك من خلال تقييم المخاطر التقنية، ووضع خطط للتحقيق منها خطط الطوارئ والتعافي من الكوارث بالإضافة الى الامتثال الأمني وسياسات النسخ الاحتياطي وغيرها.

وعليه فإن وجود حوكمة فعالة يعني ان القيادة التنفيذية مدركة لمخاطر التكنولوجيا وتعمل على الحد منها وليس ترك الأمر لقسم تقنية المعلومات وحده، هذا ما يؤدي الى تقليل احتمال حدوث أزمات تقنية قد تؤثر سلبا على سير العمل.

- الامتثال والتنظيم: من خلال الحوكمة يتم التأكد من التزام النظم تكنولوجيا المعلومات باللوائح، القوانين والمعايير المتعلقة بحماية البيانات، الأمن السيبراني،

الملكية الفكرية، الأرشفة، التوقيع الإلكتروني، والخصوصية. وهذا ما يجعل المسؤولين واضحة بين الإدارة العليا، قسم تكنولوجيا المعلومات، المستخدمين، المدققين، والموردين.

ومع تزايد تشريعات التي تحكم الجوانب التقنية مثل قوانين حماية البيانات privacy laws، والمعايير الدولية لأمن المعلومات ISO 27001 ومتطلبات التدقيق المالي المتعلقة بأنظمة المعلومات، أصبح الامتثال إلى هذه القوانين هدف أساسي للمؤسسات وذلك من أجل حوكمة التكنولوجيا. حيث يضمن إطار الحوكمة وجود سياسات وضمان تحكم كيفية إدارة البيانات وكيفية تطوير البرمجيات واختيارها بشكل يرضى المعايير، بالإضافة إلى الامتثال لمتطلبات الجهات الرقابية.

هذا الامتثال من خلال الحوكمة يسمح بحماية المؤسسة من العقوبات والغرامات وترسخ الثقة لدى أصحاب المصالح (عملاء، شركاء) لأن تكنولوجيا المعلومات تدار بمسؤولية ووفقا لمعايير أخلاقية ومهنية.

- تحسين الاداء والشفافية: تعد حوكمة تكنولوجيا المعلومات أحد الركائز الأساسية لتعزيز الأداء داخل المؤسسة وترسيخ الشفافية. فهي تساهم في توجيه الموارد الرقمية بما ينسجم مع الاهداف الاستراتيجية ويضمن تحقيق القيمة المضافة من الاستثمارات التكنولوجية. وعليه من خلال وضع أطر واضحة للمسؤوليات وآليات دقيقة لاتخاذ القرارات، وأنظمة فعالة للرقابة والمتابعة. تساهم حوكمة تكنولوجيا المعلومات في تحسين كفاءة العمليات وتقليل المخاطر المرتبطة بالأنظمة الرقمية وضمان استمرارية الخدمات وجودة المعلومات داخل المؤسسة. كما تمكن من تعزيز الشفافية من خلال توفير البيانات الموثوقة والقابلة للتتبع وفي الوقت المناسب، هذا ما يدعم المساءلة الادارية ويرفع من جودة التقارير المالية التشغيلية. توفر حوكمة تكنولوجيا المعلومات مؤشرات لقياس الأداء، مثل الجودة، زمن توقف الأنظمة، تكلفة المشاريع، مستوى رضا المستخدمين، عدد الحوادث الأمنية، ومدى

تحقيق الأهداف الرقمية. وهذا ما يساعد الإدارة العليا على اتخاذ قرارات مبنية على معلومات دقيقة.

5. المبادئ الأساسية لحوكمة تكنولوجيا المعلومات

تقوم حوكمة تكنولوجيا المعلومات على مجموعة من المبادئ الأساسية التي تهدف الى ضمان الاستخدام الرشيد والفعال للموارد الرقمية داخل المؤسسة، بما يتلائم مع أهدافها الاستراتيجية ويعزز قدرتها على خلق القيمة. و من أهم هذه المبادئ:

- **مبدأ المسؤولية:** يعني هذا المبدأ أن المسؤوليات المرتبطة بحوكمة تكنولوجيا المعلومات تكون محددة بوضوح. حيث أن الإدارة العليا تتحمل مسؤولية التوجيه والرقابة، والإدارة التنفيذية تتحمل مسؤولية التنفيذ، وقسم تكنولوجيا المعلومات يتحمل مسؤولية التشغيل والدعم، والمستخدمون يتحملون مسؤولية الاستعمال السليم للأنظمة. و في هذا السياق يؤكد (Weill , Ross, 2004) أن تحديد حقوق القرار و المساءلة هو جوهر حوكمة تكنولوجيا المعلومات.
- **مبدأ الاستراتيجية:** يقضي مبدأ الاستراتيجية انسجام تكنولوجيا المعلومات مع استراتيجية المؤسسة، حيث لا ينبغي تنفيذ أي مشروع رقمي إلا إذا كان يخدم هدفا واضحا مثل تقليل التكلفة، تحسين الخدمة، دعم الابتكار، رفع جودة القرار، أو تعزيز الأمن. وعليه فقد أشار (السالمي، 2008) إلى أن نظم المعلومات ينبغي أن ترتبط بأهداف المؤسسة، وأن تبني وفق احتياجاتها الإدارية، وليس وفق منطق تقني منعزل.
- **مبدأ اقتناء التكنولوجيا وقت الحاجة:** تعني حوكمة تكنولوجيا المعلومات اقتناء التكنولوجيا الملائمة، وليس شراء أحدث التكنولوجيا، لأنه أحيانا تكون التكنولوجيا حديثة و لكنها غير مناسبة لحجم المؤسسة، مهارات العاملين، ميزانيتها، وكذلك بنيتها التنظيمية
- **مبدأ الأداء:** تحتاج حوكمة تكنولوجيا المعلومات الى مؤشرات مثل نسبة توفير الأنظمة، عدد الحوادث، زمن الاستجابة، تكلفة الخدمة، نسبة نجاح المشاريع، مستوى رضا المستخدمين ونسبة تحقيق الأهداف الرقمية. وفق هذا المبدأ، لا يتم

تقييم التكنولوجيا بوجودها فقط، بل بنتائجها وبمساهمتها في الأداء المؤسسي: هل حسنت الخدمة؟ هل خفضت التكاليف؟ هل رفعت جودة البيانات؟ هل دعمت الرقابة؟ هل حسنت سرعة القرار؟

وقد أكد (Kaplan, Norton, 1996) أن قياس الأداء المتوازن لا يقتصر على المؤشرات المالية بل يجب أن يشمل العمليات الداخلية، التعلم، الزبائن، القرارات التنظيمية. وذلك من خلال لوحات قيادة رقمية تربط التقنية بالأداء المؤسسي.

- مبدأ الامتثال: تعني الحوكمة وفق هذا المبدأ، أن استخدام التكنولوجيا يجب أن يكون منسجما مع القوانين، المعايير، والأخلاقيات. ويشمل ذلك حماية البيانات، السرية المهنية، الملكية الفكرية، حقوق المستخدمين، والتزامات الأمن السيبراني.
- مبدأ السلوك الانساني: تهتم حوكمة التكنولوجيا بالبعد الانساني، لأن الأنظمة لا تعمل في الفراغ، بل يستخدمها أفراد لهم مهارات ، توقعات كما لهم مقاومة ومخاوف. لذلك لا بد من الأخذ بعين الاعتبار التكوين، الاتصال، المشاركة، وكذلك إدارة التغيير.

6. أبعاد حوكمة تكنولوجيا المعلومات

يمكن فهم حوكمة تكنولوجيا المعلومات من خلال أربعة أبعاد رئيسية:

- البعد الاستراتيجي: يتعلق هذا البعد بضمان توافق استراتيجية تكنولوجيا المعلومات مع استراتيجية المؤسسة ككل ويشمل تحديد الأهداف الكبرى للمشاريع التكنولوجية، وتوجيه الاستثمارات فيها وذلك من أجل تعظيم الميزة التنافسية للمؤسسة. فمثلا إذا كانت استراتيجية المؤسسة تقوم على تحسين تجربة الزبون، فيجب أن توجه الاستثمارات الرقمية نحو أنظمة إدارة العلاقة مع الزبائن، القنوات الرقمية، تحليل البيانات وخدمة ما بعد البيع. ويرى (Henderson, Venkatraman, 1993) أن العلاقة بين الاستراتيجية والتكنولوجيا علاقة تبادلية، لأن التكنولوجيا لا تنفذ الاستراتيجية فحسب بل قد تفتح إمكانات استراتيجية جديدة. كما يبرز هذا البعد دور مجلس الإدارة وكذا الإدارة التنفيذية في صنع الرؤية التكنولوجية للمؤسسة وتحديد أولويات التمويل التكنولوجي وقياس أثره على أهداف العمل.

- **البعد التنظيمي:** يختص هذا البعد ببناء الهيكل التنظيمي والإجراءات اللازمة لتطبيق الحوكمة بفعالية ويتضمن ذلك تشكيل لجان لتكنولوجيا مثل لجنة الحوكمة، او لجنة مشاريع تكنولوجيا المعلومات. وتعيين مسؤولين للإشراف ووضع سياسات وإجراءات مناسبة كما يتضمن توزيع الأدوار والمسؤوليات داخل قسم تقنية المعلومات بحيث يعرف كل طرف دوره في الحوكمة. ويؤثر البعد التنظيمي في جاهزية المؤسسة للتغيير من خلال وجود فرق مديرية، وبنية تكنولوجيا مرنة بالإضافة إلى جداول زمنية واضحة للتحديثات التكنولوجية.
 - **البعد الرقابي والامتثال:** يركز هذا البعد على الضوابط وكذا السياسات التي تضمن الالتزام بالقوانين والمعايير التكنولوجية ويشمل إجراءات التدقيق الداخلي والرقابة الخارجية وإدارة المخاطر التكنولوجية مثل إعداد ضوابط أمنية وحوكمة كمراجعة أمن المعلومات أو تقييم المخاطر السيبرانية وذلك من أجل حماية البيانات والأنظمة من الاختراقات، كما يشمل الالتزام بالمعايير المعروفة عالمياً المعيار كـ ISO 27001 أو متطلبات الجهات التنظيمية وعليه فإن هذا البعد يضمن مراقبة الأداء وتقييمه بانتظام مثل مراجعة مؤشرات الأداء KPIs.
 - **البعد القيمي:** يهدف هذا البعد إلى ضمان تحقيق عائد return on investment من خلال تكنولوجيا المعلومات لأن الحوكمة الفعالة لا تكتفي بتمويل المشاريع التقنية، بل تحسن أثرها وقيمتها على المؤسسة، وعليه يتم وضع مؤشرات ومقاييس لقياس النتائج المحققة مثل تحسين الكفاءة التشغيلية أو رضا المستخدمين أو زيادات الإيرادات الناتجة عن تطبيقات تكنولوجيا المعلومات. فتكنولوجيا المعلومات تسعى إلى تحقيق أهداف ملموسة وغير ملموسة، مثل الفوائد المالية لتقليل التكاليف أو تشغيلية لتسريع المعالجة أو استراتيجية لدعم الابتكار أو معرفية مثل تحسين جودة القرار. وفي هذا السياق أشار (Davenport, Prusak, 1998) أن القيمة الحقيقية للمعلومات تظهر عندما تتحول إلى معرفة قابلة للاستخدام في القرار والعمل.
7. دور أصحاب المصلحة في حوكمة تكنولوجيا المعلومات

تشارك عدة أطراف في تحقيق الحوكمة الفعالة لتكنولوجيا المعلومات في المؤسسة.

- مجلس الإدارة: يتحمل مجلس الإدارة مسؤولية النهائية في حوكمة تكنولوجيا المعلومات، أي أن التكنولوجيا تخدم استراتيجية المؤسسة وأن مخاطرها مضبوطة، فهو يحدد السياسات والاستراتيجيات العليا، ويوجه اتخاذ القرارات الاستثمارية الكبرى في تكنولوجيا المعلومات. فهو بذلك لا يلعب دور الخبير التقني فحسب، بل يمتلك القدرة على طرح الأسئلة الصحيحة حول المخاطر، الامتثال، الأداء، الموارد، القيمة وغيرها.
- الإدارة التنفيذية: تعمل تحت إشراف مجلس الإدارة على ترجمة الأطر الحوكمية إلى خطط تنفيذية. فهي تقوم بإعداد استراتيجيات تكنولوجيا المعلومات التفصيلية وتنفيذها بما يتوافق مع الرؤية المدروسة مسبقا. ومن مهامها: توزيع الموارد التقنية، تعيين فريق العمل المختص، متابعة المشاريع الرقمية، وضمان تكامل القرارات التكنولوجية مع العمليات التشغيلية اليومية للمؤسسة.
- إدارة تكنولوجيا المعلومات: هي الذراع التنفيذي لحوكمة تكنولوجيا المعلومات حيث تقوم بتطبيق السياسات والإجراءات الواردة في إطار الحوكمة وتطوير وتنفيذ المشاريع التقنية وفقا للخطة الاستراتيجية. فهي تتولى تشغيل الأنظمة، حماية البنية التحتية، دعم المستخدمين، تطوير التطبيقات، وإدارة الخدمات التقنية. لكن لا ينبغي أن تكون وحدها صاحبة القرار في المشاريع الرقمية.
- المستخدمون: المستخدمون في حوكمة تكنولوجيا المعلومات، ليسوا مجرد مستهلكين للتكنولوجيا، بل جزء من نظام الحوكمة ككل. فهم المسؤولون عن احترام السياسات، حماية كلمات المرور، الإبلاغ عن الحوادث، واستعمال الأنظمة بطريقة سليمة.
- التدقيق الداخلي والخارجي: يلعب التدقيق دورا هاما في حوكمة تكنولوجيا المعلومات من خلال تقييم الضوابط، اختبار فعالية الأنظمة، مراجعة الامتثال، وتقديم توصيات للتحسين. وقد بين (Romney,Steinbart, 2017) أن الرقابة على نظم المعلومات ضرورية لضمان موثوقية البيانات وحماية الأصول ودعم جودة التقارير.
- الموردون والشركاء: يعتبر الموردون جزءا هاما من نظام حوكمة تكنولوجيا المعلومات خاصة بعد توسع الحوسبة السحابية والاستعانة بالمصادر الخارجية.

وعليه لا بد على المؤسسة ضبط العلاقة معهم من خلال عقود واضحة، بنود حماية البيانات، مؤشرات مستوى الخدمة، حق التدقيق، وخطط التعافي.

8. علاقة حوكمة تكنولوجيا المعلومات بحوكمة الشركات

تعمل حوكمة تكنولوجيا المعلومات ضمن الاطار الأوسع لحوكمة الشركات وبالتالي هنالك تداخل وثيق يجمع بينها. فإذا كانت حوكمة الشركات تهتم بوضع هيكلية شاملة للمؤسسة وبتوزيع السلطة والمسؤولية والرقابة داخل المؤسسة، بما يحقق أهداف المساهمين وأصحاب المصالح، ووضع القيم والسياسات العامة مثل سياسات ادارة المخاطر، قواعد الافصاح و الشفافية، فان حوكمة تكنولوجيا المعلومات تسعى لترجمة تلك السياسات والقيم العامة الى ممارسات محددة في مجال التكنولوجيا. فمثلا اذا تبنى مجلس الادارة سياسة صارمة لإدارة المخاطر ضمن حوكمة المؤسسة فان حوكمة تكنولوجيا المعلومات ستعمل على تنفيذ ذلك عبر آليات لضبط المخاطر التقنية مثل تعزيز أمن المعلومات أو ضمان استمرارية الأنظمة التقنية الحرجة، نفس الشيء اذا أكدت حوكمة المؤسسة على الشفافية، فحوكمة تكنولوجيا المعلومات تسعى الى تطبيق ذلك عبر تقارير دورية عن أداء المشاريع التقنية مع توضيح من يمتلك صلاحيات اتخاذ القرار التقني ومن يتحمل مسؤوليته.

وعليه فان حوكمة تكنولوجيا المعلومات هي امتداد .. لحوكمة المؤسسة في العصر الرقمي، حيث أن القرارات المتعلقة بتكنولوجيا المعلومات هي جزء لا يتجزأ من القرارات الاستراتيجية للمؤسسة ككل. وبالتالي لا يمكن الفصل بين الاستراتيجية العمل داخل المؤسسة واستراتيجية تكنولوجيا المعلومات فمثلا الابتكار في المنتجات والخدمات عامة ما يعتمد على الابتكار التقني وغالبية المخاطر التجارية حاليا هي مخاطر تقنية (مثل الهجمات الالكترونية).

وبصفة عامة، حوكمة الشركات توفر الاطار الشامل الذي تدار فيه المؤسسة بفعالية ونزاهة، وحوكمة تكنولوجيا المعلومات تطبق هذا الاطار على ميدان التكنولوجيا لضمان أن هذه التكنولوجيا تدعم أهداف المؤسسة ولا تخرج عن سيطرة ورقابة الادارة العليا. ويمكن تلخيص تداخل حوكمة تكنولوجيا المعلومات وحوكمة المؤسسة في النقاط الآتية:

- حوكمة المؤسسة تحدد التوجه الاستراتيجي العام، في حين حوكمة تكنولوجيا المعلومات تضمن أن التكنولوجيا تخدم هذا التوجه.

- حوكمة المؤسسة تهتم بإدارة المخاطر، وحوكمة تكنولوجيا المعلومات تضبط المخاطر الرقمية.
- حوكمة المؤسسة تهتم بالشفافية، وحوكمة تكنولوجيا المعلومات تضمن جودة البيانات والتقارير.
- حوكمة المؤسسة تهتم بالمساءلة، وحوكمة تكنولوجيا المعلومات تحدد المسؤوليات الرقمية.

9. حوكمة تكنولوجيا المعلومات والتحول الرقمي

التحول الرقمي هو أحد أسباب الاهتمام بحوكمة تكنولوجيا المعلومات. وقد أكد (Westerman, et al., 2014) أن التحول الرقمي الناجح يتطلب الجمع بين القدرات التقنية والقيادة الإدارية، لأن التكنولوجيا دون قيادة لا تنتج فعليا. وتسمح الحوكمة في المشاريع الرقمية بطرح العديد من الأسئلة:

- ما الهدف الاستراتيجي من المشروع الرقمي؟
 - من يملك القرار في المشروع؟
 - ما المخاطر المرتبطة بالبيانات والأمن والخصوصية؟
 - كيف يتم قياس النجاح في المشروع؟
 - ما أثر المشروع في العاملين والزبائن؟
 - كيف يتم ضمان الاستمرارية بعد التنفيذ؟
- ويشير (ياسين، 2018؛ أبو النصر، 2015) أن كثيرا من المشاريع الرقمنة تفشل أو تتعثر عندما يتم التركيز على البنية التقنية فقط، دون إصلاح الإجراءات، تدريب العاملين، إعادة تنظيم الخدمات، وتغيير الثقافة الإدارية.

10. حوكمة تكنولوجيا المعلومات وإدارة المخاطر

ترتبط حوكمة تكنولوجيا المعلومات ارتباطا مباشرا بإدارة المخاطر، لأن كل نظام تقني يحمل مخاطر محتملة مثل: الاختراقات، توقف الخدمات، ضعف جودة المعلومات، فقدان

البيانات، فشل المشاريع، عدم الامتثال، مخاطر الذكاء الاصطناعي، وكذلك الاعتماد على الموردين.

وفي ظل بيئة تتسم بالتحول الرقمي، وترابط الأنظمة والاعتماد المتزايد على البيانات، وتزايد التهديدات السيبرانية، أصبحت ادارة المخاطر مكونا محوريا في حوكمة تكنولوجيا المعلومات. وتهدف هذه الأداة الى تحديد هذه المخاطر التي قد تؤثر في سلامة المعلومات، وسريتها وتوافرها وموثوقيتها، بالاضافة الى تقييمها وترتيبها حسب الأولوية ومعالجتها وكذلك حماية استمرارية أنشطة المواءمة عن طريق التحسين المستمر لآليات التحكم في المخاطر وعليه فحوكمة تكنولوجيا المعلومات تسعى الى تحويل ادارة المخاطر الى رافعة الأداء والمرونة وخلق القيمة.

وقد أوضح (Stallings, 2016) أن أمن المعلومات يتوقف على حماية السرية، السلامة والتوافر في حين حوكمة تكنولوجيا المعلومات توسع هذا المنظور لتربط الأمن بالمؤسسة ككل، بحيث تصبح إدارة المخاطر مسؤولية مشتركة بين الإدارة العليا، قسم التكنولوجيا، التدقيق، القانون، الموارد البشرية، وحتى القانون. وعليه فوجود برامج مضادة للفيروسات أو جدار ناريا يكفي لتحقيق أمن المعلومات، بل لابد من وجود سياسات، مؤشرات، تقارير، تدريب، مراجعة دورية، مساءلة واضحة، وكذلك خطط استمرارية.

11. آليات تطبيق حوكمة تكنولوجيا المعلومات

تتطلب حوكمة تكنولوجيا المعلومات تفعيل مجموعة من الآليات التنظيمية، والادارية، والتقنية التي تضمن الانتقال من المبادئ النظرية الى الممارسة الفعلية داخل المؤسسة.

- لجنة حوكمة تكنولوجيا المعلومات: تضم هذه اللجنة ممثلين عن الإدارة العليا، تكنولوجيا المعلومات، المالية، المخاطر، التدقيق، الموارد البشرية، و كل الوظائف الأساسية. وتتمثل مهمتها في تحديد الأولويات، متابعة المشاريع، تقييم المخاطر، وتقديم توصيات.
- محفظة المشاريع الرقمية: تساعد محفظة المشاريع الرقمية بترتيب المبادرات الرقمية وفقا لأهميتها، تكلفتها، مخاطرها، والعائد المتوقع منها. وهذا ما يسمح بتجنب تكرار المشاريع، التشتت، وضعف التنسيق.

- **سياسات تكنولوجيا المعلومات:** تتمثل سياسات تكنولوجيا المعلومات في مجموعة المبادئ والقواعد والإجراءات التي تحدد كيفية إدارة البنية التحتية المعلوماتية، وحماية البيانات، تنظيم صلاحيات الوصول، ضمان أمن الشبكات والأنظمة، ترشيد استخدام الأجهزة، البرمجيات والخدمات الرقمية. كما تساهم في تقليل المخاطر المرتبطة بالاختراقات السيبرانية، وفقدان البيانات وسوء استخدام المعلومات من خلال اعتماد آليات واضحة للمراقبة والتقييم والاستجابة للحوادث التقنية.
- **مؤشرات الأداء:** لا يمكن حوكمة ما لا يمكن قياسه، لذا يجب توفر مؤشرات لقياس جودة الخدمات الرقمية، إنجاز المشاريع، الحوادث، التكلفة، رضا المستخدمين، ومستوى المخاطر وغيرها.
- **التدقيق والمراقبة:** يسمح التدقيق الداخلي والخارجي من الكشف عن نقاط الضعف، تقييم فعالية الضوابط والتحقق من الامتثال إلى المعايير والقوانين. ويؤكد (Romney, Steinbart, 2017) أن الرقابة على الأنظمة ضرورية لضمان موثوقية المعلومات وحماية الأصول.
- **التكوين وبناء الثقة الرقمية:** لا يمكن نجاح الحوكمة إلا إذا تم تطبيقها على الواقع وليس بقائها على الورق فقط. لذلك تحتاج المؤسسة إلى تكوين العاملين، نشر الوعي الأمني، توضيح المسؤوليات، وتعزيز ثقافة الاستخدام المسؤول للتكنولوجيا.

12. مؤشرات نضج حوكمة تكنولوجيا المعلومات

يمكن تقييم نضج حوكمة تكنولوجيا المعلومات داخل المؤسسة من خلال عدة مستويات تدريبية بين درجة النضج التنظيمي والتقني.

- **المستوى الأول: غياب الحوكمة:** تكون الممارسات غير رسمية وتعتمد على الأفراد، إذ لا توجد سياسات أو إجراءات واضحة لإدارة تكنولوجيا المعلومات، وقد تكون القرارات التكنولوجية عشوائية وغير مرتبطة بالأهداف الاستراتيجية للمؤسسة.
- **المستوى الثاني: الحوكمة أولية وغير منظمة:** توجد بعض الإجراءات والممارسات ولكن غير موحدة وغير موثقة وتعتمد غالباً على ردود الفعل عند حدوث مشكلات.

- **المستوى الثالث: الحوكمة المتكررة:** تبدأ المؤسسة في تكرار بعض الإجراءات المتعلقة بالأمن، الصيانة، الدعم التقني وإدارة المخاطر لكن بدون وجود إطار رسمي شامل أو مؤشرات قياس دقيقة .
 - **المستوى الرابع: الحوكمة الموثقة والمنظمة:** في هذا المستوى تصبح السياسات والإجراءات التقنية مكتوبة وواضحة، كما يتم تحديد الصلاحيات والمسؤوليات مع وجود ارتباط أولي بين تكنولوجيا المعلومات وأهداف المؤسسة.
 - **المستوى الخامس: الحوكمة المقاسة والمراقبة:** يتم اعتماد مؤشرات أداء لقياس فعالية تكنولوجيا المعلومات داخل المؤسسة، م ثل مؤشرات جودة الخدمات الرقمية، مستوى الأمن، استمرارية الأعمال، سرعة معالجة الحوادث، ومدى الامتثال للمعايير.
 - **المستوى السادس: الحوكمة المستدامة:** خلال هذا المستوى تصبح المؤسسة في مرحلة متقدمة يتم فيها تحسين حوكمة تكنولوجيا المعلومات بصفة مستمرة، حيث تصبح التكنولوجيا أداة استراتيجية لرفع الأداء ، تعزيز الشفافية، تحقيق الميزة التنافسية ودعم الابتكار.
- إن انتقل إلى المؤسسة من مستوى حوكمة إلى آخر يعكس تطورها من استعمال عشوائي وتقليدي لتكنولوجيا المعلومات نحو نموذج حوكمة واضح يقوم على التخطيط، الرقابة، إدارة المخاطر، القياس المستمر و التحسين الدائم. وتساعد نماذج النضج مثل تلك المستخدمة في COBIT على تحديد وضع المؤسسة الحالي والفجوة بينها وبين الوضع المرغوب فيه. وعليه لا ينبغي استخدام النص كتصنيف شكل بل أداة تشخيص وتحسين مستمر.

13. تحديات حوكمة تكنولوجيا المعلومات في البلدان العربية

تواجه المؤسسات العربية عدة تحديات في تصنيف حوكمة تكنولوجيا المعلومات. من أبرزها ضعف الرقابة الرقمية، مركزية القرار، نقص الكفاءات المتخصصة، محدودية التكامل بين الإدارات، ضعف التوثيق، مقاومة التغيير، وتغليب شراء التكنولوجيا على إصلاح العمليات (ابراهيم الخلف الملاكوي، 2023).

وقد أشار (ياسين، 2018) أن تطبيق الإدارة الإلكترونية في البلدان العربية يواجه تحديات تنظيمية، ثقافية، وبشرية لا تقل أهمية عن التحديات التقنية. كما أكد (السالمي، 2008) أن نظم المعلومات تحتاج إلى إدارة واعية للبيانات والموارد والإجراءات حتى تحقق فعاليتها. ومن التحديات المهمة، أن قرار التكنولوجيا يترك في بعض الأحيان إلى القسم التقني فقط، ويتم استبعاد الإدارة العليا، والمستخدمون النهائيون. وهذا يؤدي إلى أنظمة غير متوافقة مع حاجات المؤسسة. كما قد يتم تنفيذ مشاريع رقمية دون مؤشرات واضحة لقياس المخاطر أو القيمة.

14. خصوصية حوكمة تكنولوجيا المعلومات في السياق الجزائري

تزداد أهمية حوكمة تكنولوجيا المعلومات، في السياق الجزائري مع توجه المؤسسات العمومية والخاصة نحو الرقمنة، الإدارة الإلكترونية، الخدمات عن بعد، الدفع الإلكتروني، والتحول الرقمي في القطاعات الاقتصادية. إلا أن هذا التحول يحتاج إلى حوكمة فعالة حتى لا تتحول الرقمنة إلى مجرد استثمار.

وتبرز الحاجة إلى الحوكمة في الجزائر من خلال عدة اعتبارات مثل ضرورة تحسين جودة الخدمة العمومية، دعم الشفافية، تقليل البيروقراطية، حماية البيانات، تحسين الرقابة، وكذلك تحديث نظم المعلومات في المؤسسات.

لكن تطبيق الحوكمة في الجزائر يواجه العديد من التحديات مثل نقص الكفاءات الرقمية، ضعف التكامل بين الأنظمة، ضعف التوثيق، محدودية قياس الأداء، مقاومة التغيير، وكذلك تفاوت البنية التحتية الرقمية بين المؤسسات والمناطق.

وحسب (ياسين، 2018) فإن نجاح حوكمة تكنولوجيا المعلومات في البيئة الجزائرية يتطلب ربط الرقمنة بإصلاح إداري شامل، تكوين الموارد البشرية، تطوير التشريعات، تعزيز الأمن السيبراني، وبناء ثقافة تنظيمية قائمة على الشفافية والمساءلة.

15. نموذج مفاهيمي مقترح لحوكمة تكنولوجيا المعلومات

يمكن اقتراح نموذج مبسط يقوم على ستة مكونات لحوكمة تكنولوجيا المعلومات:

- القيادة الرقمية: وتتمثل في التزام الإدارة العليا بتوجيه التكنولوجيا واعتبارها جزءا من الاستراتيجية.

- المواءمة الاستراتيجية: وتتمثل في ربط مشاريع التكنولوجيا بأهداف المؤسسة واحتياجات أصحاب المصالح.
- خلق القيمة: وتتمثل في قياس مساهمة التكنولوجيا في تحسين الأداء والخدمة والابتكار.
- ادارة المخاطر والامتثال: وتتمثل في حماية البيانات، التحكم في المخاطر، وكذلك احترام المعايير والقوانين.
- ادارة الموارد الرقمية: وتتمثل في الاستخدام الأمثل للبنية التحتية، التطبيقات، البيانات، الكفاءات وغيرها.
- قياس الاداء والتحسين المستمر: وتتمثل في استخدام مؤشرات دورية لتقييم النتائج وتصحيح الانحرافات.

خاتمة

تمثل حوكمة تكنولوجيا المعلومات إطاراً مفاهيمياً وعملياً يهدف إلى ضمان استخدام تكنولوجيا المعلومات بشكل رشيد ومسؤول. فهي لا تهتم فقط بكيفية تشغيل الأنظمة، ولكن تهتم كذلك بمن يقرر، من يراقب، كيف خلق القيمة، كيفية إدارة المخاطر، وكيفية قياس النتائج. ومن خلال هذا الفصل، تم ايضاح أن حوكمة تكنولوجيا المعلومات ترتبط بحوكمة المؤسسات ككل، وبنظم المعلومات، إدارة المخاطر، التحول الرقمي، حوكمة البيانات، الأمن السيبراني، وقياس الأداء. وتم التأكيد أن فهم الإطار المفاهيمي لحوكمة تكنولوجيا المعلومات يعد أساسياً لتحليل المؤسسات الرقمية، تقييم مشاريع التحول الرقمي، واقتراح أنظمة أكثر أماناً، فعالية وشفافية.

أسئلة المناقشة:

- ما الفرق بين إدارة تكنولوجيا المعلومات وحوكمة تكنولوجيا المعلومات؟
- لماذا تعد حوكمة تكنولوجيا المعلومات امتدادا لحوكمة المؤسسات؟
- كيف تساهم حوكمة تكنولوجيا المعلومات في خلق قيمة؟
- ما أهمية المواءمة بين الاستراتيجية وتكنولوجيا المعلومات؟
- لماذا تعد حوكمة البيانات جزءا من حوكمة تكنولوجيا المعلومات؟
- ما أهم التحديات التي تواجه تطبيق حوكمة تكنولوجيا المعلومات في المؤسسات العربية والجزائرية؟
- اشرح كيف يمكن أن تساهم حوكمة تكنولوجيا المعلومات في تحسين عملية اتخاذ القرار داخل قسم تكنولوجيا المعلومات؟

المحور الرابع

حوكمة تكنولوجيا المعلومات "الهكائن الأساسية"

تمهيد

أدى التطور المتسارع لتكنولوجيا المعلومات الى أحداث تطورات عميقة في ادارة المنظمات الحديثة واتخاذ القرارات الاستراتيجية فيها، ففي ظل بيئة اقتصادية تتميز بالتحول الرقمي المتسارع، العولمة، وزيادة تعقيد المخاطر التكنولوجية لم تعد تكنولوجيا المعلومات مجرد أدوات تشغيلية داعمة للأنشطة اليومية، بل أصبحت رافعة استراتيجية أساسية لخلق القيمة، تعزيز الابتكار وتحقيق الميزة التنافسية للمؤسسات.

وعليه فان فهم ركائز هذه الحوكمة يمثل مدخلا أساسيا لبناء نظام معلوماتي قادر على دعم الاستراتيجية، تقليل المخاطر، وتحسين الأداء المؤسسي وتنبع أهمية هذه الركائز من كون تكنولوجيا المعلومات أصبحت جزءا من بنية المؤسسة الحديثة، وليست وظيفة مساعدة فقط. فقد أكد (ياسين، 2005؛ السالحي، 2008) أن التكنولوجيا لا تحقق فعاليتها بمجرد اقتناء الأجهزة والبرمجيات، وإنما من خلال توظيفها داخل نظام إداري وتنظيمي قادر على تحويل البيانات إلى معلومات ومعرفة تدعم القرار. ويؤكد (أبو النصر، 2015) أن إدارة المعرفة وتكنولوجيا المعلومات تحتاجان إلى رؤية تنظيمية واضحة، وثقافة مؤسسية داعمة، وآليات للرقابة والتقييم.

كما أكد (Ross, 2004Weill) أن حوكمة تكنولوجيا المعلومات تقوم على تحديد حقوق القرار وأطر المساءلة التي تضمن استعمال التكنولوجيا بطريقة تخدم أهداف المؤسسة. ويوضح إطار COBIT 2019 أن حوكمة التكنولوجيا في المؤسسة تهدف إلى تحقيق قيمة مؤسسية من التكنولوجيا من خلال بنية حوكمية قابلة للتصميم وفق حاجات المؤسسة، مع ربط أهداف الحوكمة والإدارة بأهداف المؤسسة ككل وتوفير مؤشرات قابلة للتكيف حسب السياق المؤسسي.

1. الركيزة الأولى: المواءمة الاستراتيجية لتكنولوجيا المعلومات

- المفهوم والأسس النظرية: تعتبر المواءمة الاستراتيجية الركيزة الأولى في حوكمة تكنولوجيا المعلومات، وتعني أن تكون الاستثمارات ، القرارات، والأنظمة الرقمية منسجمة مع استراتيجية المؤسسة وأهدافها العامة. وعليه فان التكنولوجيا لا

ينبغي أن تدار كوظيفة تقنية مستقلة، ولكن كأداة استراتيجية تساعد المؤسسة على تحقيق رؤيتها، تحسين أدائها، تطوير خدماتها، وخدمة أصحاب المصالح.

وقد أشار (Henderson, Venkatraman, 1993) أن المواءمة بين استراتيجية الأعمال واستراتيجية تكنولوجيا المعلومات تمثل شرطا أساسيا لتحويل التكنولوجيا إلى عامل للتغيير التنظيمي والتميز التنافسي. كما يؤكد (ياسين، 2005) أن نظم المعلومات الإدارية ينبغي أن تبنى انطلاقا من حاجات التخطيط والرقابة واتخاذ القرار، ليس انطلاقا من من ظهور تقني وبمعزل عن أهداف المؤسسة.

وعليه، فإن المؤسسة التي تمتلك أنظمة معلومات متطورة لكنها لا تقوم بوظيفتها بأهدافها الاستراتيجية لا تستطيع تحقيق قيمة حقيقية من وراء هذه الاستثمارات. في حين المؤسسة التي تمتلك حوكمة فعالة فهي التي تهتم بمعرفة ما الهدف الإداري والاستراتيجي من التكنولوجيا قبل القيام بأي مشروع رقمي، وما القيمة التي ستضيفها والمخاطر التي يمكن أن تخلقها؟

وقد قدم (Venkatraman, Henderson, 1993) نموذجا نظريا يعرف باسم نموذج المواءمة الاستراتيجية يوضح العلاقة بين أربعة عناصر:

- استراتيجية المنظمة.
 - استراتيجية تكنولوجيا المعلومات.
 - البنية التنظيمية للمنظمة.
 - البنية التكنولوجية لنظام المعلومات.
- ويؤكد هذا النموذج أن تحقيق الأداء التنظيمي المرتفع يتطلب وجود تنسيق فعال بين هذه الأبعاد المختلفة.

● أهمية المواءمة الاستراتيجية: ان تحقق المواءمة الاستراتيجية بين تكنولوجيا

المعلومات والاستراتيجية المؤسسة يساهم في:

- تحسين الأداء التنظيمي.
- تعظيم العائد من الاستثمارات التكنولوجية.
- تعزيز الابتكار والتحول الرقمي.

- تحقيق ميزة تنافسية مستدامة.
 - آليات تحقيق المواءمة الاستراتيجية: من أهم الأدوات المستخدمة لتحقيق المواءمة الاستراتيجية نذكر:
 - المخطط التوجيهي لنظام المعلومات.
 - مشاركة الإدارة العليا في تحديد أولويات تكنولوجيا المعلومات.
 - هندسة المؤسسات.
 - ترجمة استراتيجية المؤسسة الى خارطة طريق رقمية.
 - اللجان الاستراتيجية لتكنولوجيا المعلومات.
 - اشتراك المستخدمين النهائيين في تصميم الأنظمة.
 - بطاقة الأداء المتوازن لنظم المعلومات.
 - ربط المشاريع التكنولوجية بمؤشرات أداء واضحة.
 - مراجعة الاستراتيجية الرقمية بصورة دورية.
 - مظاهر ضعف المواءمة الاستراتيجية: يظهر ضعف المواءمة بين التكنولوجيا والاستراتيجية في عدة حالات، نذكر منها:
 - تنفيذ مشاريع رقمية لا تخدم أهداف المؤسسة.
 - شراء برمجيات لا تتناسب مع احتياجات المستخدمين.
 - تعدد الأنظمة غير المتكاملة.
 - غياب الأولوية الرقمية.
 - ضعف مشاركة الإدارة العليا في القرارات التكنولوجية.
- وقد أشار (السالمي، 2008) أن نجاح نظم المعلومات يتوقف على مدى انسجامها مع البنية التنظيمية وحاجات الإدارة والمستخدمين. وعلمهم فان فشل النظام لا يكون دائما تقنيا، بل قد يكون نتيجة ضعف التحليل التنظيمي وسوء فهم احتياجات المؤسسة.

2. الركيزة الثانية: خلق القيمة من تكنولوجيا المعلومات

- مفهوم خلق القيمة التكنولوجية: لا يكفي أن تستثمر المؤسسة في التكنولوجيا، بل يجب أن تحقق هذه التكنولوجيا قيمة واضحة. وخلق القيمة التكنولوجية يعني قدرة تكنولوجيا المعلومات على خلق قيمة مضافة للمؤسسة و نتائج ملموسة مثل خفض التكاليف، تحسين جودة الخدمة، تسريع العمليات، رفع دقة المعلومات، دعم الابتكار، تحسين تجربة الزبون، أو تعزيز الرقابة.

وتحدد القيمة الناتجة عن تكنولوجيا المعلومات من خلال التفاعل بين العناصر وهي: الموارد التكنولوجية، العمليات التنظيمية، القدرات البشرية، والبيئة التنافسية.

وقد أوضح (Davenport, Prusak, 1998) أن القيمة الحقيقية لا تكمن في البيانات في حد ذاتها، بل في قدرة المؤسسة على تحويل البيانات إلى معرفة قابلة للاستخدام في القرار والعمل. وقد تتحول التكنولوجيا الى عبء اذا تم اعتمادها دون رؤية واضحة. فمثلا قد تشتري المؤسسة نظاما مكلفا لا يستخدمه الموظفون ، او تطبق منصة رقمية تزيد من التعقيد بدل تقليله، او تجمع بيانات ضخمة دون القدرة على تحليلها. لهذا تعد حوكمة القيمة من أهم ركائز حوكمة تكنولوجيا المعلومات.

- **ابعاد القيمة الناتجة عن تكنولوجيا المعلومات:**

يمكن أن تتجسد القيمة الناتجة عن تكنولوجيا المعلومات في عدة أشكال منها:

❖ **القيمة الاقتصادية:**

- تقليل التكاليف التشغيلية.
- تحسين كفاءة استخدام الموارد.
- زيادة الإيرادات.

— تحسين الإنتاجية.

❖ **القيمة الاستراتيجية:**

- دعم الابتكار التنظيمي.
- تعزيز التحول الرقمي.

❖ **القيمة التنظيمية:**

— تحسين التنسيق بين مختلف الوحدات التنظيمية.

— تعزيز التعلم التنظيمي.

❖ قيمة خدمة العمل:

— تحسين جودة الخدمات.

— تطوير تجربة المستخدم.

— تحسين رضا الزبائن.

وقد بين (Kaplan, Norton, 1996) أنقياس الأداء لا ينبغي أن يقتصر على المؤشرات المالية فحسب بل يجب أن يشمل الزبائن، العمليات الداخلية، التعلم والنمو، وعليه فإن تقييم قيمة تكنولوجيا المعلومات يجب أن يكون متعدد الأبعاد وغير محصور في العائد المالي المباشر.

- شروط خلق القيمة: لكي تخلق التكنولوجيا قيمة حقيقية داخل المؤسسة ، لابد من توفر الشروط الأساسية التالية:

— أن يكون المشروع الرقمي مرتبط بهدف واضح.

— أن تكون هناك دراسة جدوى تقنية ومالية وتنظيمية.

— أن تتوفر قيادة داعمة للتغيير.

— أن يتم تكوين المستخدمين.

— أن تقاس النتائج بعد التنفيذ.

— أن تكون البيانات دقيقة وموثوقة.

وهذا ما أكد عليه (العابدي، 2004) أن نظم المعلومات الإدارية لا تحقق فعاليتها إلا عندما تتكامل التكنولوجيا مع الموارد البشرية والإجراءات التنظيمية.

3. الركيزة الثالثة: إدارة المخاطر المرتبطة بتكنولوجيا المعلومات

- مفهوم المخاطر الرقمية: تشير مخاطر تكنولوجيا المعلومات إلى كل احتمال لوقوع حدث مرتبط بالأنظمة أو البيانات أو الشبكات أو المستخدمين، الذي من شأنه أن يؤدي إلى خسارة أو تعطيل أو ضرر للمؤسسة. وتشمل هذه المخاطر: الاختراقات، فقدان البيانات، توقف الأنظمة، ضعف جودة المعلومات، فشل المشاريع الرقمية،

تسرب البيانات الشخصية، الاعتماد المفرط على الموردين، ومخاطر الذكاء الاصطناعي. كما يمكن تصنيف هذه المخاطر الى مخاطر تقنية، أمنية، تنظيمية، وقانونية.

فقد أوضح (Whitman, Mattord, 2021) أن إدارة أمن المعلومات تحتاج إلى فهم العلاقة بين الأصول ، التهديدات ، نقاط الضعف ، والضوابط . كما يرى (ياسين، 2005 ؛ سالمي، 2008) أن ضعف الرقابة على البيانات والأنظمة يؤدي إلى تراجع جودة القرار وفقدان الثقة في المعلومات.

- أهمية ادارة المخاطر في الحوكمة: لا يمكن للمؤسسة أن تقوم بحوكمة تكنولوجيا المعلومات دون إدارة مخاطرها ، فمثلا اذا قامت المؤسسة باستثمار رقمي دون حماية بياناتها أو ضمان استمرارية خدماتها قد تتعرض لخسائر مالية ، قانونية، وسمعية، وعليه فإن إدارة المخاطر يجب أن تكون جزءا من القرار الرقمي، ولهست مرحلة لاحقة بعد وقوع الحادث فقط.

و يوفر اطار COBIT الإرشادات الخاصة بمخاطر المعلومات والتكنولوجيا، التي من شأنها ربط الممارسات والأنشطة بمؤشرات مخصصة للمخاطر، وهذا ما يجعل التحكم في المخاطر جزءا من نظام الحوكمة والإدارة. كما تسعى الحوكمة للحد من المخاطر من خلال آليات رقابية تساعد على:

- تحديد المخاطر التكنولوجية.
- تقييم احتمالية حدوثها.
- تقليل أثارها المحتملة.
- ومن أهم الأدوات المستخدمة في هذا المجال:
- التدقيق المعلوماتي.
- سياسات الأمن السيبراني.
- نظم ادارة المخاطر.
- خطط استمرارية العمل.

- أدوات إدارة المخاطر الرقمية: تتضمن إدارة المخاطر الرقمية عدة أدوات نذكر منها:

- جرد الأصول المعلوماتية.
 - تصنيف البيانات حسب الحساسية.
 - تحليل التهديدات ونقاط الضعف.
 - تقدير الاحتمال والأثر.
 - تحديد الضوابط الوقائية، الكاشفة، والتصحيحية.
 - إعداد خطط الاستمرارية والتعافي.
 - مراجعة المخاطر دورياً.
- وقد أكد (Snedaker, 2013) أن استمرارية الأعمال والتعافي من الكوارث لا يرتبطان فقط بالأنظمة التقنية بل بقدرة المؤسسة على مواصلة وظائفها الحرجة أثناء الأزمات. كما لا ينبغي حصر إدارة المخاطر في قسم تكنولوجيا المعلومات ، لأن المخاطر الرقمية تمس الإدارة العليا، المالية، الموارد البشرية، القانون، التدقيق، التسويق والعمليات، وهذا ما يفرض وجود آلية تنسيقية تجعل من المخاطر الرقمية جزءاً من إدارة المخاطر للمؤسسة.
4. الركيزة الرابعة: إدارة موارد تكنولوجيا المعلومات

- مفهوم الموارد الرقمية: تشمل الموارد الرقمية كل الأصول التي تعتمد عليها المؤسسة في إنتاج المعلومات والخدمات الرقمية ومن بينها:

- البنية التحتية التكنولوجية.
- البرمجيات والتطبيقات.
- قواعد البيانات والمعلومات.
- الموارد البشرية المتخصصة في تكنولوجيا المعلومات.
- المعرفة التقنية.
- الخوادم.

حيث أوضح (Laudon, Laudon, 2022) أن تكنولوجيا المعلومات داخل المؤسسة لا تتكون فقط من أجهزة وبرمجيات، بل تشمل كذلك البيانات، الأشخاص، الإجراءات والعمليات التنظيمية. وهذا ما أشار إليه كذلك (ياسين، 2005؛ الطائي والعبادي، 2009) أي أن نظم المعلومات الإدارية تتشكل من تفاعل الأجهزة، البرمجيات، البيانات، الأفراد والإجراءات.

- إدارة البنية التحتية: تتطلب حوكمة تكنولوجيا المعلومات إدارة فعالة للبنية التحتية الرقمية. حيث أن البنية التحتية لا بد أن تكون آمنة، موثوقة، قابلة للتكامل والتوسع، ومتلائمة مع حاجات المؤسسة. وتشمل هذه البنية الخوادم، الشبكات، مراكز البيانات، الخدمات السحابية، أنظمة النسخ الاحتياطي، وأدوات الحماية.

وقد أشار (Ross et al. 2006) أن البنية الرقمية الواضحة تمثل أساساً لتنفيذ الاستراتيجية، لأنها تسمح بتوحيد العمليات وتحسين المرونة التنظيمية.

- إدارة الموارد البشرية الرقمية: يتوقف نجاح حوكمة تكنولوجيا المعلومات على كفاءات بشرية مؤهلة. لأن المؤسسة تحتاج إلى محلي نظم، مهندسي شبكات، مديري قواعد بيانات، محلي بيانات، مختصي أمن معلومات، و كذلك مديري مشاريع رقمية.

ويؤكد (أبو النصر، 2015) أن التكنولوجيا تصبح أكثر قيمة عندما تدمج مع رأس المال المعرفي والبشري للمؤسسة. وهذا يعبر عن أهمية أن الاستثمار في التكوين وأنها لا تقل عن أهمية الاستثمار في الأجهزة والبرمجيات.

- إدارة محفظة المشاريع الرقمية: يتوجب على المؤسسة إدارة محفظة مشاريع تكنولوجيا المعلومات، أي لا بد من ترتيب المشاريع حسب الأولوية والقيمة والمخاطر والموارد المتاحة، حيث لا ينبغي تنفيذ جميع المشاريع في الوقت نفسه ولا ينبغي اختيار المشاريع وفقاً للضغط الإداري أو جاذبية التكنولوجيا. وعليه فإن إدارة المحفظة تسمح بتوجيه الموارد نحو المشاريع التي تحقق أكبر مساهمة استراتيجية.

- **ترشيد الموارد ومنع التكرار:** تهدف حوكمة تكنولوجيا المعلومات إلى تحقيق الاستخدام الأمثل لهذه الموارد بما ساهم في تحسين الأداء التنظيمي. حيث تشمل إدارة الموارد التكنولوجية عدة جوانب منها:

- التخطيط الاستراتيجي للبنية التحتية الرقمية.
- إدارة الكفاءات والمهارات الرقمية.
- تطوير نظم المعلومات.
- إدارة البيانات التنظيمية.

ومن ومن مشكلات ضعف الحوكمة وجود أنظمة متكررة، قواعد بيانات غير متكاملة، عقود تقنية غير منسقة، أو شراء حلول لا يتم استخدامها فعلياً. وعليه فإن الحوكمة تساعد على ترشيد الموارد ومنع التبذير الرقمي.

5. الركيزة الخامسة: قياس أداء تكنولوجيا المعلومات والمساءلة

- **أهمية قياس الأداء في حوكمة تكنولوجيا المعلومات:** تتطلب حوكمة تكنولوجيا المعلومات وجود نظام فعال لقياس الأداء يسمح بتقييم مدى مساهمة التكنولوجيا في تحقيق أهداف المنظمة. فقياس الأداء يسمح للمؤسسة بمعرفة هل التكنولوجيا تحقق أهدافها أم لا، وهل المشاريع الرقمية تقدم قيمة فعلية، وهل الخدمات التقنية تلبى حاجات المستخدمين. وعليه فإن قياس الأداء يساعد على:

— تحسين عملية اتخاذ القرار.

— تعزيز الشفافية والمساءلة.

— تحسين كفاءات الاستثمارات التكنولوجية.

وقد أكد (Kaplan, Norton, 1996) أن ما لا يقاس يصعب إدارته وتحسينه، وأن الأداء يجب أن يفهم من خلال مؤشرات مالية وغير مالية.

- **مؤشرات أداء تكنولوجيا المعلومات:** يمكن استخدام مجموعة متنوعة من المؤشرات لتقييم أداء نظم المعلومات نذكر منها:

- ❖ المؤشرات المالية: العائد على الاستثمار في تكنولوجيا المعلومات ، التكلفة الإجمالية لامتلاك الأنظمة، مدى احترام الميزانية والآجال.
- ❖ المؤشرات التشغيلية: نسبة توفر الأنظمة المعلوماتية، سرعة استجابة التطبيقات، عدد الأعطال المتكررة، عدد الحوادث التقنية والأمنية.
- ❖ المؤشرات التنظيمية: رضا المستخدمين، مستوى الابتكار التكنولوجي، جودة البيانات، مستوى الالتزام بسياسات الأمن.
- وتستخدم المؤسسات لوحات القيادة الرقمية لمتابعة مؤشرات الأداء الخاصة بنظم المعلومات، بشكل دوري مما يساعد على تحسين عملية الحوكمة واتخاذ القرارات الاستراتيجية.

- المساءلة في حوكمة تكنولوجيا المعلومات: تعني المساءلة تحديد من يتحمل مسؤولية القرار، التنفيذ، الرقابة و كذلك النتائج. لذلك اذا حدث فشل مشروع رقمي، فعلى المؤسسة أن تدرك هذا الخلل في التحليل، التمويل، المستخدمين، المورد، القيادة أو إدارة المشروع. وقد أكد (Weill, Ross, 2004) على أن جوهر حوكمة تكنولوجيا المعلومات يتمثل في وضوح حقوق القرار وأطر ، وبدون هذه المساءلة، تتحول التكنولوجيا إلى مجال يصعب تقييم نتائجه.

6. الركيزة السادسة: الامتثال والرقابة الداخلية

- مفهوم الامتثال الرقمي: يعني الامتثال الرقمي التزام المؤسسة بالمعايير ، القوانين، والسياسات المتعلقة بتكنولوجيا المعلومات والبيانات. ويشمل الأمن السيبراني، الملكية الفكرية، حماية البيانات الشخصية ، التوقيع الإلكتروني، سرية المعلومات، والأرشفة الرقمية..

وقد أوضح (ياسين، 2018) أن الإدارة الإلكترونية تفرض على المؤسسات تحديات قانونية وتنظيمية جديدة، لأن التعامل الرقمي يتطلب قواعد واضحة للثقة، الإثبات، السرية، وحماية المعلومات.

- الرقابة الداخلية على نظم المعلومات: تشمل الرقابة الداخلية على تكنولوجيا المعلومات كل الضوابط التي تضمن سلامة البيانات، حماية الأصول الرقمية، منع الوصول غير المصرح به، و كذلك ضمان استمرارية العمليات. وقد أوضح (Romney, Steinbart, 2017) أهمية الرقابة على نظم المعلومات المحاسبية والإدارية وذلك من أجل حماية الأصول وضمان موثوقية التقارير.

وتنقسم هذه الضوابط إلى:

- ضوابط وقائية، مثل الصلاحيات والتشفير وكلمات المرور.
- ضوابط كاشفة، مثل سجلات الدخول والمراقبة والتدقيق.
- ضوابط تصحيحية، مثل النسخ الاحتياطي وخطط التعافي.

7. الركيزة السابعة: حوكمة البيانات والمعلومات

- مركزية البيانات في المؤسسة الرقمية: تعد البيانات أصلا استراتيجيا في المؤسسة الحديثة، فهي تستخدم في اتخاذ القرار، التسويق، تقييم الأداء، إدارة الزبائن، التخطيط، التنبؤ، والذكاء الاصطناعي. وعليه فحوكمة تكنولوجيا المعلومات لا يمكن أن تتم بدون حوكمة البيانات.

وقد أكد (Davenport, Prusak, 1998) أن المعرفة التنظيمية لا تنشأ من تراكم البيانات فقط، بل من تنظيمها وتفسيرها وتوظيفها في العمل. كما يوضح (أبو النصر، 2015) أن إدارة المعرفة تتطلب بنية معلوماتية وثقافة مؤسسية قادرة على تبادل المعرفة وحمايتها.

- عناصر حوكمة البيانات: تشمل حوكمة البيانات عدة عناصر نذكر منها:

- تحديد مالك البيانات.
- تحديد صلاحيات الوصول.
- ضمان جودة البيانات.
- تصنيف البيانات حسب الحساسية.

— حماية البيانات الشخصية.

— تحديد دورة حياة البيانات.

— تنظيم الأرشفة والحذف.

— ضمان قابلية تتبع البيانات.

بدون هذه العناصر، يمكن للبيانات أن تتحول من كونها مصدر قيمة إلى مصدر خطر على المؤسسة. كما يمكن أن تؤثر على القرار الإداري. فعند استعمال بيانات غير دقيقة، مكررة، ناقصة، قديمة أو غير متناسقة، وحتى ان استعملت المؤسسة أدوات تحليل جيدة ومتقدمة، فإن النتائج ستكون مضللة وغير سليمة. وقد أشار (ياسين، 2005) أن جودة المعلومات من حيث الدقة، الملاءمة، التوقيت والأعمال، تعد شرطاً أساسياً لفعالية نظم المعلومات الإدارية.

8. الركيزة الثامنة: القيادة الرقمية والثقافة التنظيمية

- القيادة الرقمية: يتطلب نجاح حوكمة تكنولوجيا المعلومات قيادة واعية، فالقيادة الرقمية تعني قدرة الإدارة العليا على فهم دور التكنولوجيا في خلق القيمة، وتوجيه الاستثمار الرقمي، وبناء ثقافة استعمال مسؤولة وابتكارية. وقد أكد (Westreman, 2014) أن التحول الرقمي الناجح يتطلب الجمع بين القدرات التقنية والقيادة الإدارية، لأن التكنولوجيا لوحدها لا تكفي لإحداث تغيير حقيقي.
- الثقافة التنظيمية: تتمثل الثقافة التنظيمية في تحدي طريقة تعامل الأفراد مع التكنولوجيا. فمع وجود ثقافة مقاومة للتغيير، ضعيفة في تبادل المعرفة، أو متساهلة مع أمن المعلومات، فإن الحوكمة ستكون ضعيفة بالرغم من وجود السياسات والإجراءات. وقد أشار (أبو النصر، 2015) إلى أن إدارة المعرفة وتكنولوجيا المعلومات تحتاجان إلى ثقافة تشجع التعلم، المشاركة، والالتزام المؤسسي. ومن أجل نجاح أي مشروع رقمي يجب أن ترافق حوكمة تكنولوجيا المعلومات، عمليات تكوين، اتصال، دعم للمستخدمين، مشاركة، وإدارة المقاومة. لأن الأنظمة لا تفشل فقط بسبب وجود أخطاء في البرمجة ولكن قد تفشل بسبب أن المستخدمين لا يفهمونها أو لا يثقون فيها.

9. التكامل بين الركائز

تعتبر ركائز حوكمة تكنولوجيا المعلومات متكاملة فيما بينها، ولا يمكن أن تعمل بشكل منفصل. فالمواءمة الاستراتيجية تحدد الاتجاه، وخلق القيمة يبرر الاستثمار، وإدارة المخاطر تحمي المؤسسة، وإدارة الموارد تضمن الكفاءة، وقياس الأداء يوفر المساءلة، والامتثال يحمي الشرعية، وحوكمة البيانات تضمن جودة القرار، والقيادة الرقمية والثقافة التنظيمية تمنح النظام الحوكماتي قابلية التطبيق. وعليه فإن ضعف أي ركيزة من الركائز يؤثر في بقية الركائز الأخرى، فمثلا لا يمكن خلق قيمة من التكنولوجيا مع وجود بيانات رديئة، ولا يمكن إدارة المخاطر إذا كانت المسؤوليات غير واضحة، ولا يمكن تحقيق المواءمة في غياب الادارة الرقمية.

10. نموذج مقترح لركائز حوكمة تكنولوجيا المعلومات

يمكن تقديم ركائز حوكمة تكنولوجيا المعلومات في نموذج متكامل بفهم حوكمة تكنولوجيا المعلومات:

- المواءمة الاستراتيجية: هل تخدم التكنولوجيا استراتيجية المؤسسة؟
- خلق القيمة: هل تحقق التكنولوجيا قيمة مالية أو تنظيمية أو معرفية؟
- إدارة المخاطر: هل يتم التحكم في المخاطر الرقمية؟
- إدارة الموارد: هل تستخدم الموارد الرقمية بكفاءة؟
- قياس الأداء: هل توجد مؤشرات واضحة للأداء الرقمي؟
- الامتثال والرقابة: هل تحترم المؤسسة القوانين والمعايير والسياسات؟
- حوكمة البيانات: هل البيانات دقيقة وآمنة وقابلة للاستخدام؟
- القيادة والثقافة: هل توجد قيادة رقمية وثقافة داعمة للتغيير؟

خاتمة

تقوم حوكمة تكنولوجيا المعلومات على مجموعة من الركائز المتكاملة التي تسمح للمؤسسة بتوجيه التكنولوجيا، ومراقبتها، وتحويلها إلى مصدر قيمة. وقد بين هذا المحور أن أهم ركائز حوكمة تكنولوجيا المعلومات تتمثل في المواءمة الاستراتيجية، خلق القيمة، إدارة المخاطر، إدارة الموارد، قياس الأداء، الامتثال، حوكمة البيانات، والقيادة الرقمية.

تساهم هذه الركائز في ضمان الاستخدام الأمثل للتكنولوجيا داخل المؤسسات بما يحقق الأداء التنظيمي الفعال، ويعزز القدرة التنافسية والاستدامة للمؤسسة.

إن فهم هذه الركائز يمثل أساساً لتحليل المؤسسات الرقمية، تقييم مشاريع التحول الرقمي، بناء مؤشرات الأداء، وتشخيص نقاط القوة والضعف في حوكمة تكنولوجيا المعلومات.

أسئلة المناقشة:

- لماذا تعد المواءمة الاستراتيجية الركيزة الأولى في حوكمة تكنولوجيا المعلومات؟
- ما العلاقة بين إدارة المخاطر وحوكمة تكنولوجيا المعلومات؟
- لماذا تعد حوكمة البيانات جزءاً أساسياً من الحوكمة الرقمية؟
- كيف تؤثر الثقافة التنظيمية في نجاح أو فشل الحوكمة؟
- ما الفرق بين الامتثال الشكلي والحوكمة الفعلية؟
- كيف يمكن تطبيق نموذج ركائز حوكمة تكنولوجيا المعلومات في مؤسسة جزائرية؟
- كيف تساهم خلق القيمة من تكنولوجيا المعلومات في تحسين الأداء التنظيمي؟
- ما أهمية قياس أداء تكنولوجيا المعلومات في اتخاذ القرار الاستراتيجي؟

المحور الخامس

حوكمة تكنولوجيا المعلومات "القرارات المرتبطة بها"

تمهيد

تعتمد حوكمة تكنولوجيا المعلومات على وضع السياسات و تبني الأطر المرجعية، فهي تتجسد في نوعية القرارات التي تتخذها المؤسسة بشأن مواردها الرقمية، وأنظمتها المعلوماتية، مشاريعها التكنولوجية، بياناتها، وكذا مخاطرها. لان الحوكمة أساسا هي نظام لتوزيع سلطة القرار وتحديد المسؤوليات وكذا آليات المساءلة. وعليه، فما هي هذه القرارات التي يجب أن تتخذ في إطار هذه الحوكمة؟ ومن يملك حق اتخاذها؟ وعلى أي أساس يتم تقييمها؟

وقد أكد (Weill, Ross, 2004) أن حوكمة تكنولوجيا المعلومات تتمحور حول تحديد حقوق القرار وأطر المساءلة التي تشجع السلوك المرغوب في استعمال تكنولوجيا المعلومات داخل المؤسسة. وبالتالي فان جودة الحوكمة لا تظهر في وجود قسم المعلومات داخل المؤسسة فحسب، ولكن في وضوح من يقرر، من ينفذ، من يراقب، وكذلك من يتحمل نتائج القرار.

تمثل القرارات المرتبطة بحوكمة تكنولوجيا المعلومات نقطة التقاء بين البعد الاستراتيجي، البعد التنظيمي، البعد التقني، وكذلك البعد الرقابي، حيث يشير (ياسين، 2005) إلى أن نظم المعلومات الإدارية لا تحقق فعاليتها إلا عندما تكون مرتبطة بوظائف التخطيط، التنظيم، الرقابة، وكذا اتخاذ القرار. كما يؤكد (السالي، 2008) أن إدارة نظم المعلومات تتطلب تحديدا واضحا للموارد، المسؤوليات، الإجراءات، وتدفقات المعلومات داخل المؤسسة.

1. مفهوم القرار في حوكمة تكنولوجيا المعلومات

يمثل القرار في حوكمة تكنولوجيا المعلومات في أنه ذلك الاختيار المؤسسي المنظم المتعلق بتوجيه أو تخصيص أو مراقبة أو تقييم مورد رقمي أو نظام معلوماتي أو مشروع تكنولوجي معين. فالقرار لا يكون حوكماتيا بارتباطه بالتكنولوجيا فقط ، بل لابد منا رتبلمه بالاستراتيجية، المسؤولية، المخاطر، الأداء، وخلق القيمة كذلك. فمثلا قرار شراء حاسوب جديد هو قرار تشغيلي بسيط ، في حين قرار اعتماد نظام ERP ، أو الانتقال إلى الحوسبة

السحابية، أو إنشاء منصة رقمية للزبائن، فهو قرار حوكماتي لأنه يؤثر على المؤسسة ككل، ويمس الموارد، العمليات، المستخدمين، الأمن، وكذا الميزانية.

2. الفرق بين القرار التقني والقرار الحوكماتي

يجب التمييز بين نوعين من القرارات في مجال تكنولوجيا المعلومات:

- **القرار التقني:** يتمثل القرار التقني في كيفية تنفيذ الحلول مثل اختيار لغة البرمجة، إعداد الخادم، صيانة الشبكة، تحديث نظام التشغيل أو معالجة خلل تقني.
- **القرار الحوكماتي:** يتعلق هذا النوع من القرار بتوجيه التكنولوجيا وكذا ربطها بأهداف المؤسسة مثل تحديد أولويات الاستثمار الرقمي، اعتماد سياسة أمن المعلومات، توزيع الميزانية، اختيار نموذج الاستعانة بالمصادر الخارجية وكذلك تحديد ملكية البيانات.

وبناء عليه، فإن إدارة تكنولوجيا المعلومات تجيب عن سؤال: كيف يتمتنفيذ التكنولوجيا بكفاءة؟ أما حوكمة تكنولوجيا المعلومات فتجيب عن السؤال: لماذا نستخدم هذه التكنولوجيا؟ ومن يقرر؟ وما القيمة المتوقعة؟ وما المخاطر المقبولة؟ وكيف نحاسب المسؤولين عن النتائج؟

ويؤكد (Reix, Rowe, 2016) أن نظم المعلومات ليست مجرد أدوات تقنية، بل هي أنظمة اجتماعية تقنية تتفاعل فيها التكنولوجيا مع الأفراد والهيكل والإجراءات.

3. القرارات المرتبطة بحوكمة تكنولوجيا المعلومات

- **القرار المتعلق بتكنولوجيا المعلومات:**

❖ **طبيعة القرار الاستراتيجي الرقمي:** يعد قرار تحديد الاستراتيجية الرقمية للمؤسسة من أهملقرارات في حوكمة تكنولوجيا المعلومات. ويقصد بذلك تحديد الدور الذي ستؤديته التكنولوجيا في تحقيق أهداف المؤسسة: هل ستكون التكنولوجيا أداة لدعم العمليات؟ أم وسيلة لتحسين الخدمة؟ أم تكون عاملاً للابتكار؟ أم أساساً لنموذج أعمال جديد؟ ويرى (Henderson, Venkatraman, 1993) أن المواءمة بين استراتيجية المؤسسة واستراتيجية تكنولوجيا المعلومات

شرط أساسي لتحويل التكنولوجيا إلى أداة للتغيير التنظيمي والتميز التنافسي. كما يرى (ياسين، 2018) أن الإدارة الإلكترونية لا يتم فهمها باعتبارها مجرد ادخال الحاسوب في العمل الاداري بل إعادة تنظيم للعلاقات والإجراءات والخدمات باستعمال تكنولوجيا المعلومات.

❖ أسئلة القرار الاستراتيجي: يتطلب القرار الاستراتيجي في تكنولوجيا المعلومات الإجابة عن مجموعة من الأسئلة الجوهرية منها:

- ما موقع التكنولوجيا في استراتيجية المؤسسة؟
- ما الأولويات الرقمية خلال السنوات القادمة؟
- هل تهدف المؤسسة إلى الرقمنة الجزئية أم التحول الرقمي الشامل؟
- ما العمليات التي يجب رقمنتها أولاً؟
- ما القدرات الرقمية التي يجب بناؤها داخلياً؟
- ما المجالات التي يمكن تفويضها لموردين خارجيين؟
- كيف ستقاس مساهمة التكنولوجيا في الأداء المؤسسي؟
- ❖ خطورة غياب القرار الاستراتيجي: عند تغيب الرؤية الاستراتيجية، فإن التكنولوجيا تتحول إلى مجرد مشتريات متفرقة ومشاريع غير مترابطة. لأن المؤسسة قد تمتلك برامج عديدة ولكن غير متكاملة، أو قواعد بيانات متكررة، أو مواقع رقمية لكن لا تخدم المستخدمين. ولقد أشار (السالمي، 2008) أن فعالية نظم المعلومات تتوقف على مدى انسجامها مع حاجات المؤسسة وأهدافها الإدارية.

● القرار المتعلق بمعمارية تكنولوجيا المعلومات:

- ❖ مفهوم المعمارية الرقمية: يقصد بمعمارية تكنولوجيا المعلومات التصور العام الذي يحدد كيفية ترابط كل من البيانات، التطبيقات، الشبكات، المستخدمين، البنية التحتية، وكذا العمليات داخل المؤسسة. فهي بذلك تمثل الخريطة التقنية والتنظيمية التي تمنع الفوضى الرقمية وتسمح بتحقيق التكامل. وحسب (Ross, et al., 2006) فإن معمارية المؤسسة تعد أساساً

لتنفيذ الاستراتيجية، لأنها توفر قاعدة رقمية مشتركة تسمح بتوحيد العمليات وتحقيق المرونة.

❖ **طبيعة القرار المعماري الرقمي:** يشمل القرار المعماري أسئلة عديدة مثل:

- هل تعتمد المؤسسة على أنظمة مركزية أم موزعة؟
- هل تستخدم المؤسسة بنية محلية، سحابية، أم هجينة؟
- هل تعتمد قواعد بيانات موحدة أم قواعد متعددة؟
- كيف يتم ربط الأنظمة القديمة بالأنظمة الجديدة؟
- ما مستوى التكامل المطلوب بين الفروع والإدارات؟

❖ **أثر القرار المعماري:** للقرار المعماري أثر على المدالطويل، لأنه يحدد قدرة المؤسسة على التطور مستقبلاً. حيث أن الاختيارات المعمارية الضعيفة قد تؤدي إلى ارتفاع التكاليف، صعوبة التكامل، تضارب البيانات، ضعف الأمن، وتأخر تنفيذ المشاريع. في حين أن وضوح المعمارية يسمح بدعم المرونة، الاستجابة السريعة، وتوحيد الرؤية الرقمية للمؤسسة.

● **القرار المتعلق بالاستثمار في تكنولوجيا المعلومات:**

ويتمثل في تخصيص الميزانيات لمشاريع تقنية المعلومات الجديدة أو تحديث الأنظمة الحالية.

❖ **أهمية القرار الاستثماري:** يعتبر قرار الاستثمار الرقمي أحد القرارات الجوهرية في حوكمة تكنولوجيا المعلومات، لأن هذه التكنولوجيا تحتاج إلى موارد مالية معتبرة انطلاقاً من شراء البرمجيات، تجهيز الخوادم، الاشتراك في الخدمات السحابية، تكوين العاملين، تأمين البيانات وكذا صيانة الأنظمة.

وحسب (Laudon, Laudon, 2022) فإن نظم المعلومات الحديثة أصبحت ترتبط مباشرة بالأداء التنظيمي والقدرة التنافسية، لكنها تحتاج إلى إدارة واعية للاستثمار والتغيير التنظيمي. كما يؤكد (أبو النصر، 2015) أن الاستثمار في تكنولوجيا المعلومات لا يحقق قيمة إلا عندما يرتبط بإدارة المعرفة والمهارات البشرية وثقافة استخدام المعلومات.

❖ **معايير اتخاذ القرار الاستثماري:** يتوقف قرار الاستثمار في تكنولوجيا المعلومات على عدة معايير:

- العائد المالي المتوقع.
- القيمة التنظيمية غير المالية.
- درجة المخاطر.
- مدى توافق المشروع مع الاستراتيجية.
- قابلية التنفيذ.
- توفر الكفاءات.
- تكاليف الصيانة المستقبلية.
- أثر المشروع في المستخدمين والزبائن.
- مدى مساهمته في جودة البيانات والرقابة.

❖ **محفظة المشاريع الرقمية:** يجب دراسة كل مشروع رقمي ضمن محفظة المشاريع الورقية وليس بمعزل عن غيره . لأن المؤسسة يمكن أن تمتلك عدة مشاريع متنافسة على الموارد مثل مشروع أمن سيبراني، نظام محاسبي، مستودع بيانات، منصة زبائن، أو نظام موارد بشرية. و عليه فان إدارة المحفظة تسمح بتحديد الأولويات من جهة وترتيب المشاريع حسب القيمة ، المخاطر وكذا القدرة على التنفيذ.

وحسب (Kaplan, Norton, 1996) فان الأداء المؤسسي يجب أن يقاس بمنظور متوازن يتجاوز المؤشرات المالية إلى العمليات ، الزبائن وعليه فإن تقييم الاستثمار الرقمي يجب أن يراعي الأثر المالي وغير المالي معا.

● **القرار المتعلق بمصادر تكنولوجيا المعلومات:**

❖ **الاختيار بين التطوير الداخلي، الشراء أو الاستعانة الخارجية:** يعتبر قرار تحديد مصدر الحلول الرقمية المتمثل في : هل تطور المؤسسة النظام داخليا ؟ أم تشتري

برنامجاً جاهزاً؟ أو تعتمد على مزود خارجي؟ أم تلجأ إلى الحوسبة السحابية؟ أم تعتمد نموذجاً مختلطاً؟ من أهم القرارات في حوكمة تكنولوجيا المعلومات.

لكل قرار يحمل مزايا ومخاطر، حيث يمنح التطوير الداخلي المؤسسة تحكماً أكبر، لكن يحتاج إلى كفاءات كبيرة ووقت كاف، في حين الشراء من السوق يمكن من تقليل مدة التنفيذ، ولكن قد لا يتناسب تماماً مع خصوصيات المؤسسة. أما الاستعانة الخارجية فتسمح بالحصول على خبرة متخصصة، وفي نفس الوقت يمكن أن تخلق تبعية للموردين بالإضافة إلى المخاطر المتعلقة بالسرية والاستمرارية.

وفي نفس السياق، أوضح (Willcocks, Lacity, 2012) أن الاستعانة الخارجية في تكنولوجيا المعلومات لا ينبغي أن تبني على منطق تخفيض التكلفة فقط، بل يجب أن تدار كقرار استراتيجي يشمل المخاطر، العقود، الخدمة، التحكم والمعرفة.

❖ **القرار المتعلق بالموردين:** يستند قرار اختيار الموردين الرقميين إلى معايير دقيقة، نذكر منها:

- الكفاءة التقنية.
- الخبرة في القطاع.
- الاستقرار المالي للمورد.
- مستوى الخدمة.
- حماية البيانات.
- الالتزام القانوني.
- إمكانية نقل البيانات عند إنهاء العقد.
- قدرة الدعم والصيانة.
- حق التدقيق والمراجعة.

ويعتبر (ياسين، 2005؛ الطائي والعبادي، 2009) أن نجاح النظم المعلوماتية لا يرتبط فقط بالتقنية، بل كذلك بكفاءة الإدارة في اختيار الحلول وتنظيم العلاقة مع الأطراف المتدخلة.

• القرار المتعلق بحوكمة البيانات:

❖ البيانات كأصل استراتيجي: تعتبر البيانات من أهم أصول المؤسسة الرقمية. فهي أساس القرار، التخطيط، التسويق، الرقابة، تحسين الخدمات، و الذكاء الاصطناعي. ، وعليه فإن حوكمة البيانات تعد من أهم مجالات القرار في حوكمة تكنولوجيا المعلومات.

وحسب (Davenport, Prusak, 1998) فان البيانات لا تخلق قيمة إلا عندما يتم تنظيمها وتفسر ليها وتحويليها إلى معرفة قابلة للاستخدام. كما أكد (أبو النصر، 2015) أن إدارة المعرفة داخل المؤسسة تتطلب أنظمة معلومات فعالة، وثقافة شجع تبادل المعرفة، وآليات لحمايتها وتوظيفها.

❖ قرارات حوكمة البيانات: تشمل قرارات حوكمة البيانات ما يلي:

- من يملك البيانات داخل المؤسسة؟
- من يحق له الوصول إليها؟
- كيف تصنف البيانات حسب الحساسية؟
- ما قواعد إدخال البيانات وتحديثها؟
- كيف تضمن المؤسسة جودة البيانات؟
- ما مدة الاحتفاظ بالبيانات؟
- كيف يتم حذف البيانات أو أرشفتها؟
- ما الضوابط المتعلقة بالبيانات الشخصية؟
- كيف يتم تتبع مصدر البيانات وتاريخ تعديلها؟

❖ جودة البيانات والقرار الإداري: تؤثر جودة البيانات على القرار الإداري حيث يؤدي

ضعف جودة البيانات إلى قرارات إدارية ضعيفة ، فمثلا إذا كانت بيانات المبيعات غير دقيقة، أو بيانات الزبائن مكررة، أو بيانات المخزون قديمة، فهذا يؤدي إلى تقديم صورة مضللة للتقارير ولوحات القيادة. وهذا ما أشار اليه (ياسين، 2005)

أن جودة المعلومات من حيث الدقة، الملاءمة، التوقيت، والاكتمال شرط أساسي لفعالية القرار الإداري.

● القرار المتعلق بأمن المعلومات والمخاطر الرقمية:

❖ الأمن كقرار حوكمي: لا يعد الأمن السيبراني ليس قرارا تقنيا فحسب، بل هو قرار حوكمي يرتبط بمستوى المخاطر المقبول داخل المؤسسة. وعليه يتوجب على كل مؤسسة أن تحدد: ما المعلومات الأكثر حساسية؟ ما مستوى الحماية المطلوب؟ ما المخاطر المقبولة؟ ما الميزانية المخصصة للأمن؟ وكذلك من يتحمل مسؤولية الحوادث؟

ولقد أوضح (Stallings, 2016) أن أمن المعلومات يقوم على حماية السرية، السلامة، والتوافر. كما أكد (Whitman, Mattord, 2021) أن أمن المعلومات يتطلب سياسات وإجراءات ومسؤوليات واضحة، وليس مجرد أدوات تقنية.

❖ القرارات الأساسية في أمن المعلومات: تشمل قرارات الأمن المعلوماتي:

- اعتماد سياسة أمن معلومات.
- تحديد صلاحيات الوصول.
- اختيار آليات المصادقة.
- تحديد البيانات التي يجب تشفيرها.
- اعتماد خطط النسخ الاحتياطي.
- وضع خطة للاستجابة للحوادث.
- تحديد مسؤوليات المستخدمين.
- تقييم مزودي الخدمات السحابية.
- تنظيم التكوين والتوعية الأمنية.

ويجدر الذكر أن توسع استخدام الإنترنت والنشر الإلكتروني ، يفرض تحديات مرتبطة بحماية المعلومات والحقوق الرقمية والثقة في البيئة الإلكترونية.

❖ **علاقة القرار الأمني بالاستمرارية:** يرتبط قرار الأمن بـاستمرارية الأعمال، فالمؤسسة لا تسعى فقط إلى منع الحوادث، بل إلى ضمان القدرة على الاستمرار عند وقوعها. وعليه يجب الإدارة تحديد مستوى التوقف المقبول، مدة استعادة النظام، و كذا درجة فقدان البيانات التي يمكن تحملها.

وحسب (Snedaker, 2013) فإن التخطيط لاستمرارية الأعمال والتعافي من الكوارث يجب أن يرتبط بالوظائف الحرجة للمؤسسة، وليس فقط باستعادة الأجهزة والبرمجيات.

● القرار المتعلق بمستوى الخدمة الرقمية:

❖ **مفهوم الخدمة الرقمية:** تقدم تكنولوجيا المعلومات العديد منالخدمات الرقمية للمؤسسة، مثل البريد الإلكتروني، الشبكة، التطبيقات، قواعد البيانات، الدعم الفني، الأمن،الاتصال، التخزين، والتحليلات. وعليه يتوجبوجود قرارات واضحة بشأن مستوى الخدمة المتوقع.

❖ **اتفاقيات مستوى الخدمة:** تستخدم اتفاقيات مستوى الخدمة لتحديد ما يجب أن يقدمه قسم تكنولوجيا المعلومات أو المورد الخارجي من حيث التوفر، سرعة الاستجابة، زمن الإصلاح، الدعم، الجودة، والأمن. حيثتساعد هذه الاتفاقيات على تحويل العلاقة بين المستخدمين ومزودي الخدمة إلى علاقة قابلة للمساءلة والقياس، ومحددة بمؤشرات واضحة.

❖ **قرارات الخدمة:**تتضمن قرارات مستوى الخدمة:

- ما الخدمات الرقمية الحرجة؟
- ما ساعات التشغيل المطلوبة؟
- ما زمن الاستجابة المقبول؟
- ما مستوى الدعم للمستخدمين؟
- ما الأولوية عند وقوع أعطال؟
- كيف تقاس جودة الخدمة؟
- من يتابع الشكاوى والحوادث؟

وقد أشار (السالي، 2008) أن نظم المعلومات يجب أن توفر المعلومات والخدمات في الوقت المناسب وبالشكل الذي يخدم القرار الإداري.

● القرار المتعلق بالموارد البشرية والكفاءات الرقمية:

❖ أهمية الكفاءات الرقمية: يشترط تنفيذ حوكمة تكنولوجيا المعلومات وجود موارد بشرية مؤهلة. فالتكنولوجيا لا تخلق قيمة بذاتها، ولكن من خلال الأشخاص الذين يقومون بتصميمها، إدارتها، استخدامها، واستخراج المعلومات منها.

حيث أكد (أبو النصر، 2015) أن إدارة المعرفة وتكنولوجيا المعلومات ترتبط برأس المال البشري والثقافة التنظيمية، لأن المعرفة لا تتحقق بمجرد تخزين المعلومات بل بتبادلها واستثمارها.

❖ قرارات الموارد البشرية الرقمية: تشمل هذه القرارات:

- ما الكفاءات الرقمية المطلوبة؟
- هل يتم التوظيف أم التكوين الداخلي؟
- ما المهارات التي يجب تطويرها لدى المستخدمين؟
- كيف يتم تدريب العاملين على الأمن المعلوماتي؟
- هل تحتاج المؤسسة إلى مدير أمن معلومات؟
- هل تحتاج إلى محلي بيانات؟
- كيف يتم تقييم أداء فرق تكنولوجيا المعلومات؟

❖ إدارة التغيير: كل قرار تكنولوجي مهم ينتج عنه تغييرا في طريقة العمل ، وعليه يتوجب مرافقة القرارات الرقمية بخطة لإدارة التغيير، تشمل الاتصال، التكوين، الدعم، المشاركة، ومعالجة مقاومة المستخدمين. لأن الإدارة الإلكترونية تواجه تحديات بشرية وتنظيمية وثقافية لا تقل أهمية عن التحديات التقنية.

● القرار المتعلق بالامتثال القانوني والأخلاقي:

ان توسع استخدام تكنولوجيا المعلومات يؤدي الى زيادة أهمية الامتثال للمعايير و القوانين. فمثلا البيانات الشخصية، العقود الإلكترونية، التوقيع الرقمي، الملكية

الفكرية، حماية المستهلك، والأرشفة الإلكترونية كلها مجالات تحتاج إلى قرارات حوكمية واضحة. والقرار الرقمي لا يكفي أن يكون قانونيا، بل يجب أن يكون أخلاقيا كذلك. فيمكن للتكنولوجيا أن تسمح بمراقبة العاملين، تحليل سلوك الزبائن، جمع بيانات واسعة، أو استخدام خوارزميات لاتخاذ قرارات آلية. وهذا ما يسمح بطرح الأسئلة الأخلاقية الآتية: هل تم إعلام الأفراد؟ هل استخدام البيانات عادل؟ هل الخوارزميات قابلة للتفسير؟ هل توجد حماية من التمييز؟ وقد أشار (Laudon, Laudon, 2022) أن استخدام نظم المعلومات يطرح قضايا أخلاقية متعلقة بالخصوصية، الملكية، المسؤولية، والمساءلة. كما أن مسؤولية الامتثال والأخلاقيات الرقمية تقع على الإدارة العليا، وليس على القسم التقني وحده. لأن القسم التقني ينفذ الضوابط، في حين تحديد ما هو مقبول قانونيا وأخلاقيا هو قرار مؤسسي.

● القرار المتعلق بالتدقيق والرقابة على تكنولوجيا المعلومات:

❖ دور التدقيق في الحوكمة: يسمح التدقيق على تكنولوجيا المعلومات بتقييم مدى فعالية الضوابط، جودة البيانات، احترام السياسات، سلامة الأنظمة، وإدارة المخاطر. وعليه فإن قرار تنظيم التدقيق المعلوماتي يعد من القرارات الأساسية في الحوكمة.

وحسب (Romney, Steinbart, 2017) فإن الرقابة على نظم المعلومات ضرورية لحماية الأصول، ضمان موثوقية البيانات، دعم التقارير، وتقليل مخاطر الأخطاء والغش.

❖ أنواع التدقيق المرتبط بتكنولوجيا المعلومات وقراراته: يمكن التمييز بين أنواع عديدة من التدقيق في تكنولوجيا المعلومات:

- تدقيق أمن المعلومات.
- تدقيق التطبيقات.
- تدقيق قواعد البيانات.
- تدقيق الصلاحيات.

— تدقيق استمرارية الأعمال.

— تدقيق الموردين.

— تدقيق الامتثال.

— تدقيق المشاريع الرقمية.

وتتضمن قرارات التدقيق:

— ما المجالات التي يجب تدقيقها؟

— كم مرة يتم التدقيق؟

— هل يكون التدقيق داخليا أم خارجيا؟

— ما المعايير المعتمدة؟

— من يتابع تنفيذ التوصيات؟

— كيف يتم رفع التقارير الى الادارة العليا؟

● القرار المتعلق بالتحول الرقمي:

❖ التحول الرقمي كقرار حوكمي شامل: التحول الرقمي يعني تغييرا في العمليات، الثقافة، الهيكل، نموذج الأعمال، والعلاقة مع الزبائن وليس فقط ادخال أدوات جديدة. فهو بذلك قرار حوكمي من أعلى مستوى.

فحسب (Westerman, et al., 2014) فان التحول الرقمي الناجح يتطلب مزج القدرات التقنية بالقيادة الإدارية، لأن التقنية وحدها لا تصنع التحول. وأهمالقرارات المرتبطة بالتحول الرقمي:

— ما الرؤية الرقمية للمؤسسة؟

— ما العمليات التي ستعاد هندستها؟

— ما الخدمات التي ستقدم رقميا؟

— ما أثر التحول في العاملين؟

— ما البنية التحتية المطلوبة؟

- ما مخاطر التحول؟
- كيف تقاس نتائجه؟
- كيف يتم تمويله؟
- كيف تضمن المؤسسة عدم إقصاء بعض المستخدمين بسبب الفجوة الرقمية؟

وحسب(ي.سين، 2018) فإن نجاح الإدارة الإلكترونية يرتبط بضرورة إعادة تصميم الإجراءات وتطوير الثقافة الإدارية، وليس بمجرد استعمال الوسائل الإلكترونية.

4. المسؤولون عن القرارات في حوكمة تكنولوجيا المعلومات

تنسب المسؤولية في قرارات حوكمة تكنولوجيا المعلومات الى جهات مختلفة داخل هياكل الحوكمة، من الادارة العليا ومجلس الادارة الى التنفيذية والفرق الفنية، حسب نوع القرارات. فمثلا أغلبية الاستثمارات الاستراتيجية الكبيرة تقرر من قبل مجلس الادارة وذلك لتوافقها مع استراتيجية المؤسسة العامة، في حين القرارات التشغيلية المرتبطة ببيئة الانظمة وتنفيذ السياسات الأمنية وغيرها. فتميل الى ان تتخذها الادارة التنفيذية ولكن ضمن الأطر الذي يحددها مجلس الادارة.

- النموذج المركزي: من خلال هذا النموذج تتخذ الإدارة العليا أو الإدارة المركزية لتكنولوجيا المعلومات معظم القرارات. مما يسمح بتوحيد المعايير وخفض التكرار من جهة ، كما يمكن أن يكون بطيئاً وغير حساس لاحتياجات الوحدات المختلفة من جهة أخرى.
- النموذج اللامركزي: يسمح هذا النموذج ل لوحدات أو الفروع باتخاذ قراراتها التقنية بشكل مستقل. وهذا ما يسمح بمرونة عالية، ولكنه قد يؤدي إلى تضارب الأنظمة، تكرار التكاليف وضعف التكامل من جهة أخرى.
- النموذج الفدرالي: يمزج هذا النموذج بين المركزية واللامركزية في اتخاذ القرارات ، حيث تتخذ القرارات الاستراتيجية والمعمارية على المستوى المركزي، فيترك بعض القرارات التشغيلية للوحدات. وهذا ما يناسب المؤسسات الكبيرة والمعقدة.

5. مصفوفة مقترحة للقرارات المرتبطة بحوكمة تكنولوجيا المعلومات

يمكن تقديم مصفوفة كما يلي:

مجال القرار	السؤال الحوكماتي المركزي	الجهة المعنية
-------------	--------------------------	---------------

الاستراتيجية الرقمية	كيف تخدم التكنولوجيا أهداف المؤسسة؟	مجلس الإدارة والإدارة العليا
المعمارية الرقمية	كيف تتكامل الأنظمة والبيانات؟	إدارة تكنولوجيا المعلومات والإدارة العليا
الاستثمار الرقمي	أين تُخصص الميزانية الرقمية؟	الإدارة العليا والمالية وتكنولوجيا المعلومات
البيانات	من يملك البيانات ومن يستخدمها؟	الإدارة، تكنولوجيا المعلومات، مالكو البيانات
الأمن والمخاطر	ما مستوى الخطر المقبول؟	الإدارة، تكنولوجيا المعلومات، مالكو البيانات
الخدمات الرقمية	ما مستوى الخدمة المطلوب؟	الإدارة العليا، الأمن، المخاطر، التدقيق
الموردون	ما الذي يُنفذ داخليًا وما الذي يُفوض؟	تكنولوجيا المعلومات والمستخدمون
الكفاءات	ما المهارات الرقمية المطلوبة؟	الإدارة العليا، المشتريات، القانون، تكنولوجيا المعلومات
الامتثال	ما القوانين والمعايير الواجب احترامها؟	الموارد البشرية والإدارة العليا
التحول الرقمي	كيف نعيد تصميم العمل رقميًا؟	القانون، التدقيق، تكنولوجيا المعلومات
		الإدارة العليا وكل الوظائف

6. منهجية اتخاذ القرار في حوكمة تكنولوجيا المعلومات

لكي تكون القرارات المرتبطة بتكنولوجيا المعلومات رشيدة، يمكن اتباع منهجية مكونة من عدة مراحل:

- تحديد الحاجة الرقمية أو المشكلة: ما المشكلة التي نريد حلها؟
- ربط القرار بالاستراتيجية: هل يخدم القرار أهداف المؤسسة؟
- تحليل البدائل: ما الخيارات المتاحة؟
- تقدير القيمة والتكلفة: ما الكلفة وما العائد المتوقع؟
- تحليل المخاطر: ما المخاطر التقنية، القانونية، والتنظيمية؟
- تحديد أصحاب المصلحة: من سيتأثر بالقرار؟
- تحديد المسؤوليات: من يقرر؟ من ينفذ؟ من يراقب؟
- اعتماد القرار: ويكون وفق آلية موثقة ورسمية.
- تنفيذ القرار: وفق مؤشرات خاصة وخطة معينة.

— تقييم النتائج: هل تحقق الهدف؟ ما الدروس المستفادة؟

ان اتباع هذه المنهجية في اتخاذ القرار، تجعل من القرار الرقمي قرارا مؤسسيا قابلا للتبرير والمساءلة، بدلا أن يكون قرارا ارتجاليا أو تقنيا محضا.

خاتمة

تعتبر القرارات المرتبطة بحوكمة تكنولوجيا المعلومات جوهر الحوكمة الرقمية، فهي تحدد كيفية توجيه التكنولوجيا، تخصيص الموارد، إدارة المخاطر، خلق القيمة، وضمان المساءلة. ومن خلال هذا المحور نبين أن هذه القرارات تشمل الاستراتيجية الرقمية، المعمارية، الاستثمار، البيانات، الأمن، الخدمات، الموردين، الموارد البشرية، الامتثال، التدقيق، والتحول الرقمي.

وتشير الأدبيات أن التكنولوجيا لا تحقق قيمتها بمجرد وجودها، بل من خلال قرارات رشيدة تربطها بالأهداف المؤسسية وتخضعها للرقابة والقياس (ياسين، 2005؛ السالمي، 2008؛ Weill, Ross, 2004). و أن فهم هذه القرارات يسمح بتحليل كيفية بناء حوكمة تكنولوجيا المعلومات فعالة داخل المؤسسات، خصوصا في بيئة تسعى إلى تطوير الرقمنة والتحول الرقمي.

أسئلة المناقشة:

- ما الفرق بين القرار التقني والقرار الحوكماتي في تكنولوجيا المعلومات؟
- لماذا يعتبر تحديد حقوق القرار مهما في حوكمة تكنولوجيا المعلومات؟
- كيف تؤثر استراتيجية المؤسسة في القرارات الرقمية؟
- ما هي أهم المعايير التي يجب اعتمادها عند تقييم الاستثمار في تكنولوجيا المعلومات؟
- لماذا تعتبر حوكمة البيانات قرارا استراتيجيا وليس تقنيا فقط؟
- كيف يمكن توزيع قرارات تكنولوجيا المعلومات بين المركزية واللامركزية؟
- ما دور التدقيق الداخلي في تحسين قرارات حوكمة تكنولوجيا المعلومات؟
- اشرح باختصار المجالات الخمسة لقرارات تقنية المعلومات حسب نموذج Ross and Weill، مع ذكر مثال عملي لكل مجال.
- ما هي الجهة المسؤولة عادة عن قرار الاستثمار في المشاريع الرقمية في المؤسسات الكبرى ولماذا؟
- بين الفروق الأساسية بين قرارات البنية التحتية وقرارات الاستثمار ضمن حوكمة تقنية المعلومات.

المحور السادس

حوكمة تكنولوجيا المعلومات "نظام COBIT"

تمهيد

تعتبر حوكمة تكنولوجيا المعلومات من أهم متطلبات المؤسسات الحديثة، خاصة في ظل التحول الرقمي، وتزايد الاعتماد على البيانات، انتشار الخدمات السحابية، وتنامي المخاطر السيبرانية. لكن الحوكمة لا تتحقق بمجرد وضع سياسات عامة أو إنشاء قسم للإعلام الآلي، بل تحتاج إلى أطر مرجعية منظمة تساعد المؤسسة على تحديد أهدافها، توزيع المسؤوليات، إدارة المخاطر، قياس الأداء، وكذلك ضمان خلق القيمة من تكنولوجيا المعلومات.

ويعتبر COBIT أحد أشهر الأطر الدولية في مجال حوكمة وإدارة معلومات وتكنولوجيا المؤسسة. وكذلك ضمان نجاح الأعمال والتحول الرقمي والابتكار. فهو بذلك إطار حوكمي شامل يربط تكنولوجيا المعلومات بأهداف المؤسسة، ويحدد كيفية خلق القيمة، وإدارة المخاطر، وتنظيم الموارد، وقياس الأداء.

1. مفهوم COBIT ونشأته

إطار COBIT هو مختصر لعبارة: Control Objectives for Information and Related Technology وتعني أهداف الرقابة تقنية المعلومات والتقنيات ذات صلة.

ظهر إطار COBIT في البداية كإطار للرقابة والتدقيق على نظم المعلومات، ثم تطور تدريجياً ليصبح إطاراً شاملاً لحوكمة وإدارة معلومات وتكنولوجيا المؤسسة. ويعني هذا التطور انتقال المؤسسات من النظر إلى التكنولوجيا كوظيفة تشغيلية إلى النظر إليها كأصل استراتيجي يرتبط بالقيمة، المخاطر، الأداء، والامتثال.

وقد طورت (ISACA, 2019) هذا الإطار ليكون إطاراً معتمداً دولياً لحوكمة وإدارة تقنية المعلومات، وواصلت تحديثه ليتوافق مع التحولات الحديثة في تكنولوجيا المعلومات. كما أكدت ISACA على أنه صمم ليساعد المؤسسات على دمج المعايير والممارسات والأطر المختلفة داخل حل حوكمي واحد قابل للتكيف مع خصوصية المؤسسة. حيث شهد هذا الإطار عدة تطورات منذ ظهوره الأول عام 1996 وصولاً إلى النسخة الأحدث 2019 التي تتميز بمرونة كبيرة وقدر عالي من التكاليف والاستثمارات.

وعليه، يمكن تعريف COBIT على أنه إطار مرجعي لحوكمة وإدارة المعلومات وتكنولوجيا المؤسسة، يهدف إلى مساعدة المؤسسات على تحقيق القيمة من تكنولوجيا المعلومات، وإدارة المخاطر المرتبطة بها، وضمان توافقها مع الأهداف الاستراتيجية، وذلك من خلال مجموعة من المبادئ، الأهداف، العمليات، الممارسات، ومؤشرات الأداء. وهذا التعريف يتوافق مع نظرة (DeHaes, Van Grembergen, 2015)، باعتبار أن حوكمة تكنولوجيا المعلومات تهدف إلى تحقيق المواءمة بين الأعمال والتكنولوجيا، خلق القيمة، إدارة المخاطر، وقياس الأداء.

2. أهمية COBIT في حوكمة تكنولوجيا المعلومات

يقدم إطار COBIT لغة مشتركة بين الإدارة العليا، إدارة تكنولوجيا المعلومات، مسؤولي المخاطر، المستخدمين، وأصحاب المصالح، فهو بذلك يعتبر كحل للعديد من المؤسسات التي تعاني من غياب إطار موحد يربط بين الأهداف الادارية والأنشطة التقنية اضافة الى ضعف التكنولوجيا.

وقد أشار (Weill, Ross, 2004) أن حوكمة تكنولوجيا المعلومات تقوم أساسا على تحديد حقوق القرار وأطر المساءلة التي تشجع السلوك المرغوب في استعمال تكنولوجيا المعلومات، وهذا ما ترجمه إطار COBIT من خلال بنية عملية تساعد على تحديد: من يقرر؟ ماذا يجب أن يدار؟ ما المخاطر؟ ما المؤشرات؟ وما النتائج المنتظرة؟ فهو بذلك يتجاوز النظرة التقنية الضيقة إلى التكنولوجيا، ويضعها داخل نظام إداري وحوكمي متكامل. في هذا السياق تظهر أهمية COBIT في الجوانب الآتية:

- تحقيق المواءمة بين أهداف تكنولوجيا المعلومات واستراتيجية المؤسسة ككل، من خلال توفير الأدوات والموارد والارشادات اللازمة لتحديد مسؤوليات ادارة تقنية المعلومات وربطها بأولويات العمل الاستراتيجية.
- سد الفجوة بين نظم المعلومات والاحتياجات التقنية من جهة واحتياجات الأعمال الأساسية من جهة أخرى. هذا ما يجعله أداة فعالة للموارد ومتخصصي تكنولوجيا المعلومات من أجل ضمان جودة موثوقية أنظمة المعلومات في المؤسسة.
- دعم خلق القيمة من الاستثمارات الرقمية.

- ضبط المخاطر السيبرانية والتشغيلية والتنظيمية.
- تحسين الرقابة الداخلية والتدقيق على نظم المعلومات.
- قياس أداء تكنولوجيا المعلومات من خلال مؤشرات واضحة.
- تحسين الامتثال للمعايير والقوانين والسياسات.
- دعم التحول الرقمي بطريقة منظمة وقابلة للتقييم.

3. الفرق بين الحوكمة والادارة في COBIT

يميز COBIT بين مفهومين أساسيين هما الحوكمة والإدارة، فالحوكمة حسب اطار COBIT تعني أن تقوم الإدارة العليا أو الهيئة الحاكمة بتقييم احتياجات أصحاب المصالح، وتحديد الاتجاهات، ومراقبة الأداء. فهي ترتبط بأسئلة كبرى مثل:

- هل تكنولوجيا المعلومات تخدم أهداف المؤسسة؟
- هل المخاطر الرقمية مقبولة أو تم مراقبتها؟
- هل الاستثمارات الرقمية تحقق قيمة؟
- هل الأداء يقاس بوضوح؟
- هل الموارد تستعمل بكفاءة؟

في حين الإدارة في اطار COBIT فهي تتعلق بعملية التخطيط وبناء وتشغيل ومراقبة الأنشطة اليومية لتكنولوجيا المعلومات. فهي تهتم بتنفيذ التوجيهات التي تحددها الحوكمة من خلال المشاريع، الخدمات، التطبيقات، البنية التحتية، الأمن، الدعم، والتشغيل.

ويعتبر التمييز بين الحوكمة والادارة مهم جدا داخل المؤسسة، حتى يتجنب الخلط بين تشغيل النظام وحوكمته. لأنه من الممكن وجود قسم آلي يهتم بأعمال الصيانة والدعم، لكنه لا يمتلك حوكمة حقيقية إذا كانت القرارات الرقمية غير مرتبطة بالاستراتيجية، وإذا لم يتم تقييم المخاطر، حتى إذا النتائج لا تكون قابلة للمساءلة.

وعليه فقد أكد (IT Governance Institute, 2003) أن حوكمة تكنولوجيا المعلومات جزء من حوكمة المؤسسة، وهدفها ضمان أن التكنولوجيا تدعم أهداف المؤسسة واستراتيجيتها.

4. المبادئ العامة لنظام COBIT

يقوم اطار COBIT 2019 على أساس حوكمي، يرى أن لكل مؤسسة نظام حوكمة خاصا بها، وأن هذا النظام يجب أن يصمم وفق احتياجات المؤسسة، أهدافها، مخاطرها، وبيئتها. حيث يقدم هذا الاطار توجيهات عملية وموارد تساعد المؤسسات على تكييف حل الحوكمة وفق حجمها واحتياجاتها. فهو قابل للتكامل مع الممارسات والمعايير الأخرى. وأهم المبادئ العامة لهذا الاطار هي كالآتي:

- **تلبية احتياجات أصحاب المصالح:** تعمل حوكمة تكنولوجيا المعلومات على تلبية احتياجات أصحاب المصالح داخل المؤسسة ، مثل المساهمين، الإدارة، الزبائن، المستخدمين، الموردين، الجهات الرقابية، والمجتمع. لأن كل هؤلاء ينتظرون من المؤسسة الاستخدام الفعال، الأمن، والمسؤول لتكنولوجيا المعلومات.
- وفي هذا السياق، أكد (ياسين ، 2005) أن يجب أن توفر المعلومات الدقيقة واللائمة وفي الوقت المناسب لمختلف مستويات القرار داخل بالإضافة الى توفير خدمات فعالة ومخاطر مضبوطة.
- **تغطية المؤسسة ككل:** لا ينظر إلى تكنولوجيا المعلومات حسب اطار COBIT، على أنها خاصة بقسم الإعلام الآلي فقط، بل يعتبرها موردا مؤسسيا يشمل كل الوحدات والوظائف مثل المحاسبة، الموارد البشرية، التسويق، المشتريات، الإنتاج، والرقابة التي تعتمد على البيانات والأنظمة الرقمية.
- **اعتماد اطار موحد ومتكامل:** يسمح اطار COBIT بدمج العديد من الأطر مثل: ISO 27001، ITIL، ISO 38500، وكذلك إدارة المخاطر ، فهو يجمع بين الحوكمة، الأمن، التدقيق، إدارة الخدمات، ومعمارية المؤسسة ، وإدارة المخاطر كلها في نظام واحد متكامل. وصمم ليعمل بسهولة مع التوجيهات والمعايير والأنظمة والممارسات المختلفة التي تحتاجها المؤسسة داخل حل حوكمي موحد.
- **اعتماد مقارنة شمولية:** يتبنى اطار COBIT مقارنة شمولية تسمح بفهم التكنولوجيا ضمن منظومة مؤسسية كاملة ، فحوكمة تكنولوجيا المعلومات وفق هذا النظام لا

تعتمد على العمليات فقط، بل تشمل الهياكل التنظيمية، المعلومات، الثقافة، السلوك، المهارات، السياسات، والخدمات.

وحسب(أبو النصر، 2015)فان تكنولوجيا المعلومات لا تحقق قيمة دون ثقافة تنظيمية ومعرفة بشرية قادرة على توظيف المعلومات وتحويلها إلى قرارات وممارسات.

- الفصل بين الحوكمة والادارة: يسمح اطار COBIT بفصل واضح بين التوجيه والمراقبة من جهة، والتنفيذ والتسيير من جهة أخرى. مما يساعد على بناء مساءلة واضحة، بحيث لا تختلط مسؤولية التنفيذ بسلطة اتخاذ القرار.

5. مكونات نظام الحوكمة وفق اطار COBIT

يعمل اطار COBIT على فكرة أن نظام الحوكمة يتكون من مكونات متعددة يجب أن تعمل معا. ويمكن تلخيصها فيما يلي:

- العمليات: تتمثل العمليات في مجموعة الأنشطة التي تنفذها المؤسسة لتحقيق أهداف الحوكمة والادارة مثل: ادارة الخدمات، ادارة الأمن، ادارة المخاطر، ادارة الموارد، ادارة المشاريع، ادارة البيانات، ومراقبة الأداء.
- الهياكل التنظيمية: تتمثل الهياكل التنظيمية في مجموع المجالس واللجان والوحدات المسؤولة عن اتخاذ القرار و عن الرقابة، مثل مجلس الإدارة، لجنة تكنولوجيا المعلومات، إدارة الأمن المعلوماتي، إدارة نظم المعلومات، والتدقيق الداخلي.
- المبادئ والسياسات والاجراءات: تحتاج الحوكمة داخل المؤسسة إلى سياسات واضحة مثل سياسة أمن المعلومات، سياسة استخدام الأنظمة، سياسة النسخ الاحتياطي، سياسة إدارة البيانات، وسياسة الاستعانة بالموردين.
- المعلومات: تعبر المعلومات من الأصول الجوهرية في نظام COBIT، لأن كل من القرارات، الرقابة، والأداء تعتمد على معلومات دقيقة، ملائمة، آمنة، وفي الوقت المناسب. وهذا ما أكد عليه(Davenport , Prusak, 1998) حيث يعتبر أن البيانات لا تصبح معرفة إلا من خلال التنظيم ، التفسير وكذلك الاستخدام داخل سياق إداري واضح.

- الثقافة، الاخلاقيات والسلوك: تحتاج الحوكمة إلى ثقافة تنظيمية تشجع الالتزام، الشفافية، حماية البيانات، واحترام الصلاحيات، وكذلك الإبلاغ عن المخاطر وليس فقط الاجراءات والوثائق.
- الأشخاص، المهارات، الكفاءات: تحتاج حوكمة تكنولوجيا المعلومات إلى كفاءات متنوعة مثل: محللو البيانات، خبراء في نظم المعلومات، مختصو الأمن السيبراني، مدققو نظم المعلومات، مديرو مشاريع، وكذلك المهتخدمون المهربون. ولقد أكد (أبو النصر، 2015) على أن العنصر البشري والمعرفي يمثل شرطاً أساسياً لنجاح إدارة المعرفة وتكنولوجيا المعلومات.
- الخدمات والبنية التحتية والتطبيقات: وتتمثل في مجموع الموارد التقنية التي تعتمد عليها المؤسسة: الخوادم، الشبكات، قواعد البيانات، التطبيقات، الخدمات السحابية، أدوات الحماية، ومنصات التحليل. ويجب على كل هذه الموارد يجب أن تخضع لقرارات حوكمة تكنولوجيا واضحة من حيث الاستثمار، المخاطر، القيمة، والتكامل.

6. مجالات COBIT الأساسية

ينظم COBIT أهداف الحوكمة والادارة ضمن مجالات عديدة نذكر منها:

- مجال الحوكمة: **EDM: Evaluate, Direct and Monitor** التقييم، التوجيه، والمراقبة. يمثل هذا المجال مستوى الحوكمة العليا. حيث تركز عملياته على أن الإدارة العليا تعمل على تقييم حاجات المؤسسة، توجيه الإدارة التنفيذية، ومراقبة الأداء والامتثال والمخاطر.

- ❖ **التقييم Evaluate**: يتمثل تحليل الوضع الحالي والمستقبلي لتكنولوجيا المعلومات: أي ما قيمة التكنولوجيا؟ ما مخاطرها؟ هل تخدم استراتيجيات المؤسسة؟ هل الموارد كافية؟ هل أصحاب المصالح راضون؟
- ❖ **التوجيه Direct**: يتمثل في تحديد التوجهات والسياسات والأولويات. حيث تقوم الإدارة العليا بتقري ما يجب تحقيقه، وما المخاطر المقبولة، وما الموارد المخصصة، وكذلك المعايير المعتمدة.

❖ **المراقبة Monitor:** يعني بالمراقبة متابعة النتائج، قياس الأداء، التأكد من الالتزام، وكذلك مدى تحقيق الأهداف.

وهذا ما يتوافق مع ما ذهب إليه (Weill, Ross, 2004) اللذان يعتبران أن الحوكمة تتمحور حول حقوق القرار والمساءلة في تكنولوجيا المعلومات.

- **مجال التخطيط والتنظيم APO Align, Plan and Organize:** أيالمواءمة، التخطيط، والتنظيم. يهتم هذا المجال بترجمة توجهات الحوكمة إلى استراتيجيات وخطط وموارد وسياسات. ويشمل العديد منالقضايا مثل استراتيجية تكنولوجيا المعلومات، معمارية المؤسسة، الابتكار، الميزانية، الموارد البشرية، إدارة الموردين، المخاطر، والأمن.

❖ **المواءمة الاستراتيجية:** يجب أن تكون خطط تكنولوجيا المعلومات منسجمة مع استراتيجية المؤسسة. وقد أشار (Henderson,Venkatraman, 1993) إلى أن المواءمة بين الأعمال والتكنولوجيا شرط أساسي لتحقيق التحول التنظيمي.

❖ **التخطيط الرقمي:** يتضمن تحديد المشاريع، الأولويات، الميزانيات، الموارد، والبرامج الرقمية.

❖ **التنظيم:** يشمل التنظيم تحديد الهياكل ، المسؤوليات، المهارات والسياسات التي تسمح بتنفيذ الخطة. وحسب(الطائي والعبادي ، 2009) فان نجاح نظم المعلومات الإدارية يتطلب توافقا بين التكنولوجيا والهيكل التنظيمي و كذلك الموارد البشرية.

- **مجال البناء، الاقتناء، والتنفيذ BAI : Build, Acquire and Implement :** يركز هذا المجال على تحويل الخطط إلى حلول رقمية فعلية. ويشمل إدارة البرامج والمشاريع، تحديد المتطلبات، بناء الحلول، اقتناء البرمجيات، إدارة التغيير، اختبار الأنظمة، ونقلها إلى بيئة التشغيل.

❖ **إدارة المشاريع الرقمية:** يؤكد اطار COBIT على أهمية إدارة المشاريع وفق أهداف واضحة ومخاطر مضبوطة و كذلك مؤشرات متابعة ومدروسة. ولهذا

العديد من مشاريع تكنولوجيا المعلومات تفشل نتيجة ضعف الحوكمة، غياب متطلبات واضحة ، سوء إدارة التغيير، وكذلك ضعف مشاركة المستخدمين.

- ❖ اختيار الحلول: يساعد القرار الحوكمي على تحديد ما اذا كان الحل سيتم تطويره داخلياً، شراءه، أو الحصول عليه من مزود خارجي.
- ❖ ادارة التغيير: يتطلب التحول نحو الإدارة الإلكترونية تغييراً تنظيمياً وثقافياً، وليس مجرد استعمال الأدوات الرقمية، لذا لا بد من تحضير المستخدمين، تدريبهم، وتعديل الإجراءات. وهذا ما أشار اليه (ياسين، 2018).

- مجال التسليم والخدمة والدعم: DSS : Deliver, Service and Support: يهتم هذا المجال بالتشغيل اليومي للخدمات الرقمية. حيث يشمل إدارة العمليات، إدارة الحوادث، إدارة المشكلات، الأمن، استمرارية الخدمة، ودعم المستخدمين.

- ❖ استمرارية الخدمة: وتتمثل في ضمان أن الأنظمة الحرجة متوفرة دائماً أو تسترجع بسرعة عند حدوث خلل.
- ❖ ادارة الحوادث: وتتمثل في وجود إجراءات واضحة للتبليغ عن الحوادث، تصنيفها، معالجتها، وتحليل أسبابها.
- ❖ أمن المعلومات: يعتبر أمن المعلومات أهم أبعاد هذا المجال ، وهو يقوم على السرية، السلامة والتوافر. وهذا ما أكد عليه (Stallings, 2016).
- ❖ دعم المستخدمين: حتى تكتمل الخدمة الرقمية لابد من دعم المستخدمين ومساعدتهم على استغلال الأنظمة بطريقة فعالة.

- مجال المراقبة والتقييم: MAE Montitor, Evaluate and Assess: يهتم هذا المجال بمتابعة الأداء والامتثال والرقابة الداخلية. فهو يجيب عن أسئلة مثل:

- هل تحقق تكنولوجيا المعلومات أهدافها؟
- هل الضوابط فعالة؟
- هل المؤسسة ملتزمة بالقوانين والمعايير؟
- هل الأداء يتحسن؟

— هل المخاطر تحت السيطرة؟

وقد أكد كلمن (Romney, Steinbart, 2017) أن الرقابة على نظم المعلومات ضرورية لضمان موثوقية البيانات، حماية الأصول، ودعم جودة التقارير.

7. أهداف الحوكمة والادارة في COBIT

يقترح نظام COBIT مجموعة من أهداف الحوكمة والإدارة التي تساعد المؤسسة على تنظيم أعمالها الرقمية. ويمكن فهمها من خلال التمييز بين:

❖ **أهداف الحوكمة:** وهي جميع الأهداف المرتبطة بالتقييم، التوجيه، والمراقبة على مستوى الإدارة العليا.

❖ **أهداف الإدارة:** وهي الأهداف المرتبطة بالتخطيط، البناء، التشغيل، والمراقبة على مستوى الإدارة التنفيذية.

يمنع هذا التقسيم الخلط بين من يحدد الاتجاه ومن ينفذ. ف مثلاً الإدارة العليا لا تقوم بتفاصيل تشغيل الشبكة، لكنها مسؤولة عن التأكد من أن الشبكة آمنة وتخدم أهداف المؤسسة، في حين إدارة تكنولوجيا المعلومات مسؤولة عن التنفيذ والتشغيل والتحسين. وهذا يتوافق مع ما طرحه (Georgel, 2009) أن حوكمة نظم المعلومات يجب أن تضمن التحكم في نظام المعلومات من حيث الأداء، المخاطر، التكاليف، والقيمة.

8. عوامل تصميم نظام الحوكمة في COBIT

يدعو نظام COBIT 2019، إلى تصميم نظام الحوكمة وفق خصوصية كل مؤسسة، وليس نموذجاً واحداً لجميع المؤسسات. فهو يوفر مرونة في التنفيذ، يسمح بتكييف حل الحوكمة حسب احتياجات المؤسسة. وأهم عوامل تصميم الحوكمة:

- **استراتيجية المؤسسة:** تختلف حوكمة تكنولوجيا المعلومات في المؤسسة، حسب ما إذا كانت هذه المؤسسة تبحث عن النمو، الابتكار، الاستقرار، تخفيض التكلفة، أو تحسين الخدمة.

- أهداف المؤسسة: ترتبط أهداف تكنولوجيا المعلومات بأهداف المؤسسة ككل ، مثل رضا الزبائن، تحسين الكفاءة، دعم الامتثال، تقليل المخاطر، أو تعزيز الابتكار.
- ملف المخاطر: حيث تختلف الحوكمة في الم مؤسسة على حسب درجة المخاطرة، فمؤسسة مالية مثلا تحتاج إلى مستوى أعلى من التحكم الأمني والامتثال ، مقارنة بمؤسسة صغيرة ذات نشاط محدود.
- حجم المؤسسة: فلما زاد حجم المؤسسة، زادت الحاجة إلى هيكل حوكم يرسى من لجان، مؤشرات، عمليات موثقة، وتدقيق دوري.
- دور تكنولوجيا المعلومات داخل المؤسسة: إذا كانت التكنولوجيا مجرد أداة دعم داخلي في المؤسسة ، فإن متطلبات الحوكمة تختلف عن مؤسسة يكون نموذج أعمالها قائما على التجارة الإلكترونية أو المنصات الرقمية.
- نموذج التوريد: تختلف الحوكمة من مؤسسة الى أخرى حسب اعتمادها على التطوير الداخلي أو الموردين أو الحوسبة السحابية أو الاستعانة الخارجية.
- المتطلبات القانونية والتنظيمية: حيث تحتاج المؤسسات الخاضعة لتنظيمات صارمة إلى مستوى أعلى من الامتثال والرقابة.

9. نموذج النضج والقدرة في نظام COBIT

يساعد نظام COBIT المؤسسات على تقييم مستوى قدرتها على تنفيذ العمليات وتحقيق أهداف الحوكمة. والهدف من ذلك ليس فقط التصنيف الشكلي للمؤسسات، ولكن معرفة الوضع الحالي للمؤسسة، تحديد الفجوة، وكذلك وضع خطة من أجل التحسين. و عليه يمكن تقسيم مستويات النضج في نظام COBIT كما يلي:

- المستوى الأول: يتمثل في الممارسات غير الرسمية التي تعتمد على الأفراد.
- المستوى الثاني: يتميز بوجود إجراءات جزئية وغير موحدة.
- المستوى الثالث: يتميز بعمليات موثقة ومطبقة.
- المستوى الرابع: يتميز بعمليات مقاسة ومراقبة.
- المستوى الخامس: يتمثل في التحسين المستمر وابتكار.

يساعد هذا النموذج على فهم أن الحوكمة لا تطبق دفعة واحدة، بل تتطور تدريجيا من ممارسات بسيطة إلى نظام متكامل قائم على القياس والتحسين.

10. COBIT وعلاقته بالأطر والمعايير الأخرى

يتميز نظام COBIT بقدرته على التكامل مع الأطر والمعايير الأخرى، فهو لا يعمل بمعزل عنها. فنجد أن COBIT 2019 صمم ليكون قابلا للاندماج مع المعايير، التوجيهات، الأنظمة والممارسات التي تحتاجها المؤسسة.

- **COBIT و ISO 38500:** يركز ISO 38500 على نظام إدارة أمن المعلومات، بينما يساعد COBIT على ادماج الأمن ضمن حوكمة تكنولوجيا المعلومات ككل. فنجد أن نظام ISO 38500 يحدد توجه سلوك الهيئة الحاكمة في حين أن COBIT يحول هذا المبدأ مؤسسي قابل للتصميم، التنفيذ، وكذلك التقييم. وبذلك يوفر ISO المرجعية المعيارية العليا في حين نظام COBIT يقدم البنية الرقابية والتنفيذية لتجسيده.
- **COBIT و ITIL:** يركز نظام ITIL على إدارة خدمات تكنولوجيا المعلومات خاصة الدعم والتشغيل، في حين COBIT يغطي كل من الإدارة والحوكمة ولكن من منظور أوسع. وعليه فإن COBIT يتميز باتساع نطاقه المؤسسي والرقابي، بينما يتميز ITIL بعمق تطبيقي في مجال إدارة الخدمات فنظام COBIT يحدد ما ينبغي حوكمته وإدارته وقياسه، في حين ITIL يقدم إرشادات حول كيفية تنظيم الممارسات والأنشطة اللازمة لإنشاء الخدمات الرقمية، تقديمها، دعمها، وتحسينها.
- **COBIT و COSO:** يسمح نظام COSO بمعالجة المخاطر والرقابة الداخلية على مستوى المؤسسة ككل من عمليات مالية وتشغيلية، وتقارير وغيرها. أما COBIT فيختصر في حوكمة وإدارة المعلومات وكذا التكنولوجيا والضوابط المرتبطة بها. وعليه فإن COBIT نظام يساعد على تطبيق مكونات COSO داخل البيئة الرقمية.

11. خطوات تصنيف COBIT داخل المؤسسة

يتم تطبيق نظام COBIT داخل المؤسسة وفقا لمنهجية تدريجية، خاصة اذا كانت المؤسسة في بداية بناء حوكمة تكنولوجيا المعلومات.

- تحديد الحاجات والدوافع: تتمثل هذه الخطوة في تحديد أسباب اعتماد نظام COBIT: هل الهدف من ذلك تحسين الأمن ، أم تقليل فشل المشاريع ؟ أم تحسين الامتثال ؟ أم دعم التحول الرقمي ؟ أم رفع جودة الخدمات ؟
- تحديد أصحاب المصالح: في هذه المرحلة يتعين على المؤسسة تحديد الأطراف المعنية: الإدارة العليا، المستخدمون، إدارة تكنولوجيا المعلومات، التدقيق، المخاطر، المالية، الموردون ، الزبائن، والجهات الرقابية.
- تقييم الوضع الحالي: يتم في هذه المرحلة تحليل الوضع القائم داخل المؤسسة: ما أهم العمليات الموجودة؟ ما هي نقاط الضعف؟ ما مستوى النضج؟ ما هي المخاطر الموجودة؟ وما المشاكل المتكررة؟
- تحديد الوضع المستهدف: يجب على المؤسسة تحديد المستوى المطلوب من النضج في عملياتها حسب الأهمية والمخاطر.
- تحليل الفجوة: يتم خلال هذه المرحلة مقارنة الوضع الحالي بالوضع المستهدف، وتحديد الفجوة بينهما، وذلك في السياسات، العمليات، الأدوات، المهارات، وكذلك الرقابة.
- وضع خطة تحسين: تشمل خطة التحسين تحديد الأولويات، الموارد، المسؤوليات، الآجال، وكذلك مؤشرات النجاح.
- التحسين والمتابعة: يتم تنفيذ التحسين تدريجياً وبصفة مستمرة مع مراقبة النتائج وتعديل الخطة عند الحاجة.

12. تطبيق نظام COBIT في المؤسسات الجزائرية

تواجه المؤسسات الجزائرية تحديات خاصة في تطبيق حوكمة تكنولوجيا المعلومات، أهمها ضعف الثقافة الرقمية، محدودية التوثيق، مقاومة التغيير، نقص الكفاءات المتخصصة، ضعف التكامل بين الأنظمة، وكذلك التركيز على شراء التكنولوجيا أكثر من حوكمتها.

وهذا ما أشار إليه (ياسين، 2018) أن الإدارة الإلكترونية في البلدان العربية تواجه تحديات تنظيمية، ثقافية، بشرية لا تقل أهمية عن التحديات التقنية.

وعليه فان نظام COBIT يمكن أن يساعد المؤسسات العمومية والخاصة في الكثير من النقاط:

- تنظيم مشاريعها الرقمية.
- تحسين جودة الخدمات الإلكترونية.
- ضبط مخاطر الأمن السيبراني.
- تحسين الرقابة على نظم المعلومات.
- دعم الشفافية والمساءلة.
- ترشيد الإنفاق على التكنولوجيا.
- تحسين جودة البيانات والقرارات.
- تعزيز الثقة في الخدمات الرقمية.

وبناء على ما سبق فان تطبيق COBIT في الجزائر يحتاج إلى تكييف مع المؤسسات المحلية، خاصة من حيث الحجم، مستوى النضج الرقمي، طبيعة النشاط، الكفاءات المتوفرة، البيئة التنظيمية والقانونية.

13. مزايا نظام COBIT

أهم المزايا التي يوفرها نظام COBIT للمؤسسة تتمثل في:

- توفير لغة مشتركة بين التقنيين والاداريين: حيث يساعد نظام COBIT على تقريب الرؤية بين قسم تكنولوجيا المعلومات والإدارة العليا، لأن كلاهما يتوفران على نفس الأهداف.
- تحسين المساءلة: يساعد هذا النظام على تحديد من يقرر، من ينفذ، من يراقب، ومن يتحمل النتائج.
- دعم خلق القيمة: يسمح نظام COBIT بربط تكنولوجيا المعلومات بأهداف المؤسسة ككل، وهذا ما يسمح بتقييم القيمة الناتجة عن الاستثمارات الرقمية.
- التحكم في المخاطر: يسمح هذا الإطار بتحديد المخاطر الرقمية، تقييمها، ومراقبتها. كما يعزز الضوابط على عملية تكنولوجيا المعلومات، مما يدعم الامتثال للمتطلبات التنظيمية والقوانين.

- التغطية الشاملة لحوكمة تكنولوجيا المعلومات: يوفر اطار COBIT تغطية شاملة لجميع جوانب حوكمة تكنولوجيا المعلومات وادارتها، فهو يشمل: ادارة المخاطر، ادارة الموارد، ادارة الأداء. وذلك لضمان تحقيق القيمة المرجوة.
- دعم التدقيق والرقابة: يساعد نظام COBIT المدققين، وذلك بتوفير مرجع لتقييم الضوابط والممارسات.
- قابلية التكامل مع الاطراف الاخرى: يمكن دمج نظام COBIT مع الأنظمة الأخرى ISO، ITIL، بهدف تبني منهجية حوكمة شاملة ومتكاملة تستفيد من الممارسات المتعددة وهذا التكامل يوفر رؤية شمولية للضبط.
- المرونة وقابلية التكيف: يتميز هذا الاطار بإمكانية تطبيقه في مختلف الصناعات والقطاعات وبين المؤسسات الكبيرة والصغيرة، مما يجعله خيارا قابلا للتخصص وفق بيئة كل مؤسسة.

14. حدود نظام COBIT

يكتسي اطار COBIT أهمية كبرى، لكنه لا يمثل حلا لجميع مشكلات تكنولوجيا المعلومات. لأن فعاليته تتوقف على طريقة تطبيقه، ومدى التزام الإدارة العليا، نضج المؤسسة وكذلك توفر الكفاءات. وأهم حدوده:

- يمكن أن يكون معقدا بالنسبة للمؤسسات الصغيرة ذات الموارد المحدودة والخبرات الفنية القليلة، خاصة إذا تم تطبيقه بشكل كامل وبدون تكييف. وكذلك نظرا لوثائقه التفصيلية وكثرة عملياته.
- يمكن لهذا الاطار أن يتحول إلى وثائق شكلية إذا لم يتم ربطه بالقرار الفعلي.
- يحتاج إلى فهم جيد تكوين في مجال الحوكمة.
- استخدام هذا النظام لا يغني عن الأطر المتخصصة في الخدمات، الأمن، أو المشاريع.
- كثافة استخدام الموارد أو فرق عمل، وقت، أنظمة متابعة، قد تكون تحديا بالنسبة للمؤسسات ذات اقسام تكنولوجيا المعلومات المحددة

— يتوقف هذا النظام على ثقافة تنظيمية تتوقف على المساءلة وعلى القياس. وهذا ما يصعب أحيانا تحقيقه وما يجعله يحد من الابداع والمرونة.

15. نموذج مقترح مبسط لنظام COBIT

يمكن تبسيط نظام COBIT حسب النموذج الآتي:

السؤال الحوكماتي	إجابة COBIT
لماذا نستخدم التكنولوجيا؟	لتحقيق أهداف المؤسسة وخلق القيمة
من يوجه التكنولوجيا؟	الإدارة العليا والهيئات الحاكمة
من يدير التكنولوجيا؟	الإدارة التنفيذية وإدارة تكنولوجيا المعلومات
كيف نضمن القيمة؟	من خلال أهداف الحوكمة والإدارة ومؤشرات الأداء
كيف نتحكم في المخاطر؟	من خلال عمليات إدارة المخاطر والأمن والرقابة
كيف نقيس النضج؟	من خلال مستويات القدرة والتحسين المستمر
كيف ندمج المعايير الأخرى؟	باستعمال COBIT كإطار شامل قابل للتكامل

خاتمة

يمثل COBIT إطارا مرجعيا مهما لحوكمة وإدارة تكنولوجيا المعلومات، فهو يساعد على تحويل التكنولوجيا من وظيفة تقنية إلى اعتبارها موردا استراتيجيا قابلا للتوجيه، القياس، والمساءلة. ولقد تطور هذا الإطار من نظام رقابة وتدقيق إلى إطار شامل لحوكمة وتكنولوجيا المؤسسة، يسمح بدعم المواءمة الاستراتيجية، خلق القيمة، إدارة الموارد، إدارة المخاطر، قياس الأداء، والامتثال.

فهو بذلك يقدم هيكلا من العمليات والأنشطة يمتد عبر دورة حياة خدمات تقنية المعلومات ككل، ابتداء من التخطيط الاستراتيجي، تنظيم موارد تقنية المعلومات، اكتساب الانظمة وتنفيذها، تشغيل الخدمات التقنية ودعمها، وكذلك مراقبة الأداء وتقييمه وبهذه

النظرة الشمولية فان اطار COBIT يضمن ان جميع عمليات تكنولوجيا المعلومات تصب في تحقيق أهداف المؤسسة وتدار بفعالية ضمن حدود المخاطر المقبولة.

وتؤكد العديد من الأدبيات مثل (ياسين، 2005؛ السالحي، 2008؛ أبو النصر، 2015؛ Weill, Ross, 2004 ; De Haes, Van Grembergen, 2015) أن نجاح تكنولوجيا المعلومات لا يعتمد فقط على اقتناء الأنظمة، ولكن على مدى إدماجها في الاستراتيجية، التنظيم، الثقافة، الرقابة. وعليه فان هذا الاطار يوفر إطارا تحليليا وتطبيقيا لفهم كيفية بناء حوكمة رقمية فعالة داخل المؤسسة، خاصة بالنسبة للمؤسسات التي تسعى إلى تطوير الرقمنة وتحسين جودة الخدمات والتحكم في المخاطر.

أسئلة المناقشة:

- ما المقصود بإطار COBIT؟ وما علاقته بحوكمة تكنولوجيا المعلومات؟
- ما الفرق بين الحوكمة والإدارة في COBIT؟
- كيف يساعد COBIT على تحقيق المواءمة بين تكنولوجيا المعلومات واستراتيجية المؤسسة ككل؟
- كيف يمكن استعمال COBIT في تقييم نضج حوكمة تكنولوجيا المعلومات؟
- ما أهمية مجال EDM في نظام COBIT؟
- كيف يمكن استعمال COBIT في تقييم نضج حوكمة تكنولوجيا المعلومات؟
- ما علاقة COBIT بالأطر الأخرى ISO وITIL؟
- ما أهم التحديات التي تواجه تطبيق COBIT في المؤسسات؟

المحور السابع

حوكمة تكنولوجيا المعلومات وفق معايير ISO

تمهيد

تعتبر معايير ISO من أهم المرجعيات الدولية المعتمدة التي تستند إليها المؤسسات في تنظيم أنشطتها، تحسين أدائها، ضبط عملياتها وكذلك إدارة مخاطر. كما تكتسب هذه المعايير أهمية خاصة في مجال تكنولوجيا المعلومات باعتبارها إطاراً منهجياً يساعد المؤسسة على توجيه التكنولوجيا، ضبط استخداماتها، إدارة الخدمات الرقمية، حماية المعلومات وكذا تقييم المخاطر المرتبطة بالبيئة الرقمية.

يعتبر تطبيق حوكمة تكنولوجيا المعلومات وفق معيار ISO منظومة مترابطة من المعايير بداية من معيار ISO 38500 المتعلق بحوكمة تكنولوجيا المعلومات في المؤسسة، بالإضافة إلى معيار ISO 27001 في مجال إدارة أمن المعلومات، ISO 27005 لإدارة مخاطر أمن المعلومات، ISO 20000 لإدارة خدمات تكنولوجيا المعلومات، و ISO 31000 لإدارة المخاطر ارتفاع عام.

باعتبار أن تكنولوجيا لا تحقق فعاليتها بمجرد اقتناء الأجهزة والبرمجيات بل تحتاج إلى نظام إداري، إجراءات واضحة، موارد بشرية مؤهلة و معلوماتية دقيقة تدعم القرار والرقابة. فإن معايير ISO تمنح المؤسسة لغة تنظيمية ومنهجية تساعد على الانتقال من الاستخدام العشوائي للتكنولوجيا إلى الاستخدام المحكوم، المقاس، والوجه نحو خلق خلق القيمة.

1. مفهوم حوكمة تكنولوجيا المعلومات وفق ISO

تعتبر حوكمة تكنولوجيا المعلومات حسب نظام ISO، ذلك النظام الذي تضعه المؤسسة من أجل تقييم استخدام تكنولوجيا المعلومات، توجيه ومراقبته. بما يضمن الاستخدام الكفء، المسؤول، الفعال والمضمون من الناحية التنظيمية، الأخلاقية والقانونية.

كما يعتبر معيار ISO 38500 المرجع الرئيسي في هذا المجال حيث يقدم المبادئ التوجيهية لأعضاء الهيئات الحاكمة داخل المؤسسة حول الاستخدام الفعال والمسؤول لتكنولوجيا المعلومات، وينطبق على جميع المؤسسات بمختلف أنواعها، وأحجامها وكذا استخداماتها للتكنولوجيا.

ويمكن معرفة حكم التكنولوجيا المعلومات وفق ISO بأنها مجموعة من المبادئ والمسؤوليات والعمليات التي تتضمن أن تكنولوجيا المعلومات تستخدم بطريقة تحزم أهداف المؤسسة وتحافظ على مواردها المعلوماتية، تدير مخاطرها وتحث قيمة لأصحاب المصالح. وهذا التعريف يتوافق مع نظرة (Weill, Ross, 2004) اللذان يعتبران أن حوكمة تكنولوجيا المعلومات تقوم على تحديد حقوق القرار وأطر المساءلة التي توجه السلوك المرغوب في استعمال التكنولوجيا داخل المؤسسة كما يتوافق مع (ياسين، 2005) الذي يؤكد أن نظم المعلومات الإدارية يجب أن ترتبط بالتخطيط والرقابة وكذلك اتخاذ القرار حتى تكون ذات قيمة فعلية للمؤسسة.

2. مكانة ISO 38500 في حوكمة تكنولوجيا المعلومات

يمثل معيار ISO 38500 أهم المراجع في حوكمة تكنولوجيا المعلومات وفق نظام ISO لأنه لا يركز على تشغيل الأنظمة أو إدارة الأمر فقط ولكنه موجه كذلك إلى الهيئات الحاكمة والإدارة داخل المؤسسة، المسؤولة عن الرقابة والتوجيه.

وصدرت النسخة الحديثة من المعيار بعنوان the governance of information technology (IT) for the organizations سنة 2024، وهي النسخة الثالثة بعد نسخة 2015، التي أظهرت أهمية في اعتبار أن حوكمة تكنولوجيا المعلومات ليست مسؤولية القيم الإعلامية فقط ولكن مسؤولية الهيئة الحاكمة، مجلس الإدارة وكذلك الإدارة العليا. وعليه فإن ISO 38500 استطاع أن يربط تكنولوجيا المعلومات بأبعاد أساسية وهي:

- البعد الاستراتيجي: هل تخدم التكنولوجيا أهداف المؤسسة؟
- البعد الرقابي: هل يتم تقييم ومراقبة الاستخدام الرقمي؟
- البعد التنظيمي الأخلاقي: هل يتم استخدام التكنولوجيا بطريقة مسؤولة مقبولة؟

وهذا ما أكد عليه (سالمي، 2008)؛ (الطائي والعبادي، 2009) باعتبار أن نظم المعلومات لا يمكن أن تكون فعالة إذا بقيت منفصلة عن التنظيم، الإدارة وكذلك الثقافة المؤسسية.

3. الفرق بين حوكمة تكنولوجيا المعلومات وإدارة تكنولوجيا المعلومات من منظور معيار ISO

يسمح هذا المعيار بالتمييز بين الح وكمة والإدارة في تكنولوجيا المعلومات، حيث تهتم الح وكمة بالتوجيه والمساءلة الرقابة في حين تهتم الإدارة بالتنفيذ والتشغيل. ح وكمة تكنولوجيا المعلومات تسمح بالإجابة عن الأسئلة التالية:

- هل تستخدم التكنولوجيا المناسبة؟
 - هل تخدم التكنولوجيا استراتيجية المؤسسة؟
 - من يتحمل مسؤولية القرار الرقمي؟
 - ما مستوى المخاطر المقبول؟
 - هل الاستثمارات الرقمية تحقق قيمة؟
 - هل يتم احترام المعايير والقوانين؟
- إدارة تكنولوجيا المعلومات تسمح بالإجابة عن الأسئلة التشغيلية مثل:

- كيف يتم تشغيل الشبكة؟
- كيف يتم صياغة النظام؟
- كيف ندير الحوادث؟
- كيف يتم تحديث البرمجيات؟
- كيف ندعم المستخدمين؟

ومن المهم التمييز بين الح وكمة والإدارة من حيث تكنولوجيا المعلومات داخل المؤسسة، لأن هذه الأخيرة قد تمتلك إدارة تقنية فعالة من حيث الدعم و الصياغة لكنها تفتقر إلى ح وكمة حقيقية إذا كانت قرارات الاستثمار الرقمي، الأمن، البيانات وكذا المخاطر غير مرتبطة بالإدارة العليا. وهذا ما أكد عليها (Reix, Rowe, 2016) باعتبار أن نظم المعلومات، أنظمة اجتماعية وتقنية تتداخل فيها التكنولوجيا مع البنية التنظيمية والممارسات الإدارية.

4. مبادئ حوكمة تكنولوجيا المعلومات وفق ISO 38500

يقوم معيار ISO 38500 على مجموعة من المبادئ الأساسية التي تساعد المؤسسة على مراقبة وتوجيه تكنولوجيا المعلومات بشكل رشيد.

- **مبدأ المسؤولية:** يعني هذا المبدأ أن مسؤوليات تكنولوجيا المعلومات يجب أن تكون واضحة ومحددة بحيث كل طرف داخل المؤسسة يعرف دوره في اتخاذ القرار، الرقابة، التنفيذ، الاستخدام والمساءلة. لقد اعتبر (ياسين، 2005) و(العبادي، 2009) أن ضعف تحديد المسؤوليات يؤدي إلى ضعف فعالية نظم المعلومات، لأن النظام المعلوماتي لا يقوم على الأجهزة فقط، ولكن يقوم كذلك على الأفراد، الإجراءات وتدفقات العمل.
- **مبدأ الاستراتيجية:** ينص هذا المبدأ على استخدام تكنولوجيا المعلومات يجب أن يكون منسجماً مع استراتيجية المؤسسة ككل لأن التكنولوجيا ليست غاية في حد ذاتها وإنما وسيلة لتحقيق أهداف محددة مثل تحسين الخدمة، دعم القرار، رفع الإنتاجية، تحسين العلاقة مع الزبائن، تعزيز الشفافية. وهذا ما أكد عليه (Hendreson, Venkartraman, 1993) اللذان اعتبراً أن الهوامة بين استراتيجية الأعمال واستراتيجية تكنولوجيا المعلومات شرط أساسي لتحقيق القيمة من التكنولوجيا.
- **مبدأ الاقتناء الرشيد:** إن الحوكمة وفق هذا المبدأ، لا تعني شراء أحدث الأنظمة ولكن اختيار التكنولوجيا التي تناسب احتياجات المؤسسة وقدراتها. فيمكن أن يكون النظام متقدماً وحديثاً ولكنه غير ملائم لنظم المؤسسة وكفاءاتها البشرية أو ثقافتها. وقد أكد (سالمي، 2008) أن نظم المعلومات يجب أن تبنى وفقاً لحاجات المؤسسة وليس وفقاً لمفهوم تقني منفصل عن الواقع التنظيمي لها.
- **مبدأ الأداء:** ينص هذا المبدأ على ضرورة قياس أداء تكنولوجيا المعلومات داخل المؤسسة، فهذه الأخيرة يجب أن تعرف هل حققت تكنولوجيا المعلومات الأهداف المرجوة منها مثل: تقليل التكاليف، تسريع الخدمة، تحسين جودة المعلومات، أو تقليل الأخطاء. وقد اعتبر (Kaplan, Norton, 1996) أن قياس الأداء لا يجب أن

يقتصر على المؤشرات المالية فقط، بل يجب أن يشمل العمليات الداخلية، الزبائن، التعلم، وكذا القرارات التنظيمية.

- مبدأ الامتثال: يقصد بالامتثال أن استخدام تكنولوجيا المعلومات يجب أن يكون وفقاً للقوانين، اللوائح، السياسات الداخلية والمعايير وكذا الالتزامات التعاقدية. ويشمل ذلك كل من سرية المعلومات، الملكية الفكرية، حماية البيانات، حقوق المستخدمين وأمن الأنظمة.

- مبدأ السلوك الانساني: يتم استخدام تكنولوجيا المعلومات من طرف مجموعة من الأفراد لهم مهارات، مقاومة، مخاوف وتوقعات. وعليه فوجب على الحوكمة مراعاة احتياجات المستخدمين، التواصل، التكوين، وإدارة التغيير.

5. نموذج التقييم، التوجيه، والمراقبة وفقاً لـ ISO 38500

يعتمد معيار ISO 38500 على ثلاثة عناصر: التقييم، التوجيه والمراقبة.

- التقييم Evaluate: ويقصد أن تقوم الإدارة العليا بتقييم الوضع الحالي والمستقبل لاستخدام تكنولوجيا المعلومات ويتضمن ذلك دراسة:

— مدى ملائمة الأنظمة الحالية.

— قيمة الاستثمارات الرقمية.

— المخاطر المرتبطة للتكنولوجيا.

— مدى رضا المستخدمين.

— مدى توافق التكنولوجيا مع الاستراتيجية.

— جاهزية الموارد البشرية.

يسمح هذا التقييم بمنع اتخاذ قرارات تقنية قائمة على الانطباع أو ضغط الموردين وبالتالي يتحول القرار الرقمي إلى قرار مبني على المعلومات والتحليل.

- التوجيه: بعد عملية التقييم تعمل الإدارة العليا على توجيه استعمال تكنولوجيا المعلومات وذلك من خلال السياسات، الأولويات، الميزانيات، الاستراتيجيات المعايير. وتشمل هذه العملية :

- اعتماد سياسة رقمية.
 - تحديد أولويات الاستثمار.
 - تحديد مستوى المخاطر المقبول.
 - المصادقة على سياسات الأمن.
 - تحديد مسؤوليات البيانات.
 - توجيه مشاريع التحول الرقمي.
- المراقبة: تتمثل المراقبة في متابعة مدى تنفيذ التوجيهات وتحقيق الأهداف وتشمل العديد من المؤشرات مثل:

- نسبة توفر الأنظمة.
- عدد الحوادث الأمنية.
- نسبة نجاح المشاريع الرقمية.
- مستوى رضا المستخدمين.
- جودة البيانات.
- مدى احترام الميزانية.
- مدى الالتزام بالسياسات و المعايير.

انطلاق مما سبق، فإن الح وكمة من منظور معيار ISO 38500 تمثل دورة مستمرة وليست فقط إجراء إداريا مؤقتا.

6. علاقة معيار ISO 38500 بباقي معايير ISO الداعمة

يمثل معيار ISO 38500 معيار وكمي علمي، وعليه فإن تطبيقه بمفرده لضبط كل جوانب تكنولوجيا المعلومات يكون غير كاف، هذا ما يستدعي الحاجة إلى معايير أخرى داعمة لتغطية المخاطر، الأمن، الخدمات، الجودة، والخصوصية.

- نظام ISO 27001 نظام ادارة أمن المعلومات: يعتبر هذا المعيار من أشهر معايير أمن المعلومات عالميا، حيث يحدد أفضل الممارسات في مجال إدارة أمن المعلومات

فهو يحدد متطلبات إنشاء وتنفيذ وصيانة وتحسين نظام إدارة أمن المعلومات. كما يقوم على إدارة المخاطر المرتبطة بأمن البيانات التي تمتلكها المؤسسة أو تعالجها.

وتتمثل العلاقة بين ISO 38500 و ISO 27001 في أن ISO 38500 يحدد مسؤولية الحوكمة العليا في مراقبة وتوجيه التكنولوجيا، في حين ISO 27001 يساعد على بناء نظام إداري لحماية المعلومات. وهذا ما يجعل من أمن المعلومات ليس فقط أداة تقنية، ولكن نظام مؤسسي يدعم كل من التكنولوجيا، السياسات والأشخاص.

- **نظام 2021 : ISO 27005 إدارة مخاطر أمن المعلومات:** يرتبط هذا المعيار بإدارة مخاطر أمن المعلومات، وهو بذلك معيار داعم لـ ISO 27001 حيث يقدم التوجيهات حول كيفية تحديد المخاطر وتحليلها، تقييمها ومعالجتها. وتتمثل أهميته في تحويل الأمن السيبراني من رد فعل بعد وقوع الحوادث إلى مراقبة استباقية لإدارة المخاطر.
 - **نظام 2018 : ISO 20000 إدارة خدمات تكنولوجيا المعلومات:** يركز هذا المعيار على نظام إدارة خدمات تكنولوجيا المعلومات، فهو يحدد متطلبات إنشاء، تنفيذ، صياغة وتحسين نظام إدارة الخدمة. كما يساعد المؤسسة في تنظيم الخدمات الرقمية بما يلي متطلبات المستخدمين والزبائن والمؤسسة. و تتمثل علاقة هذا النظام بالحوكمة في أن الإدارة العليا تحتاج إلى مراقبة جودة الخدمات الرقمية مثل: توفير الأنظمة، سرعة الإجابة، إدارة الحوادث، الدعم التقني، وإدارة التغيير.
 - **نظام 2018 : ISO 31000 إدارة المخاطر:** يقدم هذا المعيار المبادئ والتوجيهات العامة لإدارة المخاطر داخل المؤسسة، كما يوفر منهجية لتحديد المخاطر، تحليلها، تقييمها، معالجتها من مراقبتها. وتكمن أهمية هذا المعيار بالنسبة لحوكمة تكنولوجيا المعلومات في أنه يسمح بإدماج المخاطر الرقمية ضمن نظام خاطر المؤسسة ككل، بدل التعامل معها كقضية تقنية منعزلة.
7. تطبيق حوكمة تكنولوجيا المعلومات وفق نظام ISO داخل المؤسسة

يتم تطبيق حكم التكنولوجيا المعلومات وفق معيار ISO من خلال مجموعة من المراحل:

- **تحديد نطاق الحوكمة:** تبدأ المؤسسة في هذه المرحلة بتحديد نطاق الحوكمة وكمة من خلال: هل يشمل كل أنظمة المؤسسة هل يركز على الأمن فقط؟ هل يشمل الخدمات الرقمية؟ هل يتعلق بالتحول الرقمي؟ هل يشمل الموردين والخدمات السحابية؟
- تتسم هذه المرحلة بالأهمية لأنها تسمح بتوزيع المسؤوليات، تحديد الأولويات وتخفيض الموارد.
- **تحديد أصحاب المصالح:** تمس تكنولوجيا المعلومات ال عديد من الأطراف مثل: الادارة العليا، المستخدمين، الزبائن، الموردين، الجهات الرقابية، المدققين والمجتمع. وعليه يتوجب تحليل احتياجات جميع الأطراف. وهذا يتفق مع رؤية (Freeman, et al., 2010) في نظرية أصحاب المصالح، حيث يرى أن المؤسسة ليست مسؤولة أمام المساهمين فقط ولكن أمام جميع الأطراف التي تؤثر في نشاطها او تتأثر به.
- **بناء سياسة حوكمة تكنولوجيا المعلومات:** تعتمد المؤسسة في حوكمة تكنولوجيا المعلومات سياسة واضحة تحدد :
 - أهداف استخدام تكنولوجيا المعلومات.
 - مسؤوليات الإدارة العليا.
 - مسؤوليات إدارة تكنولوجيا المعلومات.
 - قواعد أمن المعلومات.
 - قواعد حوكمة البيانات.
 - مبادئ الاستثمار الرقمي.
 - مؤشرات الأداء.
 - آلية المراجعة و التحسين.
- **وضع الهياكل التنظيمية:** تحتاج حوكمة تكنولوجيا المعلومات إلى العديد من الهياكل التنظيمية مثل:

- لجنة تكنولوجيا المعلومات.
- لجنة الأمن السيبراني.
- مسؤول أمن المعلومات.
- مسؤول حماية البيانات.
- لجنة إدارة المخاطر.
- التدقيق الداخلي لنظم المعلومات.

● **ادارة المخاطر الرقمية:** يتوجب ربط ا لحوكمة بإدارة المخاطر في تكنولوجيا المعلومات، وذلك من خلال تحديد الأصول المعلوماتية، تحليل التهديدات، تقييم الاحتمال والأثر، اختيار الضوابط، ومراقبة النتائج.

وقد أكد (ياسين، 2005) أن نظم المعلومات يجب أن توفر معلومات دقيقة موثوقة تساعد الإدارة على الرقابة واتخاذ القرار وهذا لا يتحقق إذا كانت البيانات معروضة للمخاطر أو غير محمية .

● **قياس الأداء والتحسين المستمر:** تعمل معايير ISO على مبدأ التحسين المستمر وعليه فإن اعتماد السياسة لوحدها غير كافي، بل يجب قياس النتائج ومراجعة الأداء وكذلك تحديث الضوابط حسب تغيير البيئة الرقمية.

8. مؤشرات تقييم حوكمة تكنولوجيا المعلومات وفق نظام ISO

يتم تقييم ح وكمة تكنولوجيا المعلومات وفق نظام ISO من خلال مؤشرات كمية ونوعية منها:

- درجة توافق تكنولوجيا المعلومات مع استراتيجية المؤسسة.
- وضوح المسؤوليات والصلاحيات.
- وجود سياسة مكتوبة لح وكمة التكنولوجيا.
- نسبة توفر الأنظمة الحرجة.
- عدد الحوادث الأمنية.
- زمن استجابة الحوادث.

- درجة نضج إدارة المخاطر.
- نسبة المشاريع الرقمية المنجزة في الوقت و الميزانية.
- مستوى رضا المستخدمين.
- نسبة الالتزام بسياسات أمن المعلومات.
- جودة البيانات ودقتها.
- مدى انتظام التدقيق والمراجعة.

تساعد هذه المؤشرات على تحويل الح وكمة من خطاب عام إلى ممارسة قابلة لقياس والمساءلة.

9. مزايا حوكمة تكنولوجيا المعلومات وفق نظام ISO

توفير معايير ISO العديد من المزايا للمؤسسة أهمها:

- توحيد المفاهيم والممارسات: حيث تمنح هذه المعايير لغة مشتركة بين الإدارة، التقنيين، المدققين وكذا الجهات الرقابية هذا ما يسهل عملية التواصل ويسمح بتقليل الغموض.
- تعزيز الثقة: اعتماد المؤسسة على معايير دولية معروفة مثل ISO، يسمح بتعزيز ثقة الزبائن، المستثمرين وشركاء في قدرتها على حماية المعلومات وكذا إدارة الخدمات الرقمية.
- تحسن الرقابة والمساءلة: وذلك من خلال تحديد المسؤوليات، تو ثيق الإجراءات، متابعة الأداء و إثبات الامتثال.
- دعم ادارة المخاطر: حيث تسمح معايير ISO بإدماج المخاطر الرقمية ضمن منهجية منظمة خاصة إطار ISO 31000 و ISO27005.
- دعم التحول الرقمي: توفير معايير ISO إلى التحول الرقمي وإطار يضمن الأمن، الجودة، الاستمرارية و الامتثال وهذا بطريقة منهجية ومنظمة.

- تحسن جودة الخدمات الرقمية: تساعد معايير ISO على تنظيم خدمات تكنولوجيا المعلومات، تحسين الاستجابة للحوادث وضبط مستوى الخدمة وذلك من خلال ISO 20000.

10. حدود تطبيق معايير ISO في حوكمة تكنولوجيا المعلومات

تكتسي معايير ISO أهمية كبيرة بالنسبة للمؤسسات غير أنها لا تمثل حلاً جاهزاً ولا لائماً لكل المؤسسات. وعليه يمكن أن تتحول إلى وثائق شكلية إذا لم يتم تبنيها بجدية من طرف الإدارة العليا. ومن أهم حدود استعمالها:

- ارتفاع تكلفة التطبيق، التكوين والاستشارة.
- صعوبة فهم بعض المتطلبات في غياب خبرة متخصصة.
- خطر التركيز على الشهادة بدل التحسين الحقيقي.
- ضعف الثقافة التنظيمية قد يشكل عائق في فعالية التطبيق.
- عدم ملائمة التطبيق لبعض المؤسسات الصغيرة.
- الحاجة إلى تحديث مستمر بسبب تغيير المخاطر الرقمية.

وقد أشار (أبو ناصر، 2017) إلى أن نجاح تكنولوجيا المعلومات لا يتحقق بالأدوات وحدها، لكن يحتاج إلى ثقافة تنظيمية، معرفة بشرية وكذلك آلية تعلم مستمرة. لذلك فإن معايير ISO لا بد أن تستخدم كإطار التحسين المستمر وليس كإجراء شكلي للحصول على الشهادة.

11. حوكمة تكنولوجيا المعلومات وفق ISO في المؤسسات الجزائرية

في البيئة الجزائرية، تزايد أهمية معايير ISO بسبب توسع الوقمنة، تطور الخدمات الإلكترونية، تزايد الاعتماد على قواعد البيانات، وظهور مخاطر الأمن السيبراني والخصوصية. إلا أن تطبيق الحوكمة وفق ISO يواجه العديد من التحديات منها:

- ضعف الثقافة الرقمية في بعض المؤسسات.
- محدودية تكوين المتخصص.
- مقاومة التغيير.

- نقص التوثيق.
 - التركيز على اقتناء التكنولوجيا بدلا من حوكمتها.
 - محدودية التدقيق المعلوماتي.
 - ضعف مؤشرات الأداء الرقمي.
- وقد أكد (ياسين، 2018) أن الإدارة الإلكترونية في البيئة العربية تتطلب إصلاحا إداريا، تنظيميا، وثقافيا وليس فقط ادخال التكنولوجيا. كما يرى (سالي، 2008) أن نظم المعلومات تحتاج إلى إدارة واضحة للموارد والبيانات والإجراءات حتى تتحقق فعاليتها. وعليه يمكن أن تساهم حوكمة تكنولوجيا المعلومات وفق إطار ISO في الجزائر في:

- تحسين جودة الخدمات العمومية الرقمية.
- تعزيز أمن البيانات في المؤسسات العمومية والخاصة.
- دعم الشفافية و الرقابة.
- تحسين موثوقية نظم المعلومات.
- ترشيد الإنفاق الرقمي.
- تقوية ثقة المواطنين والزبائن في الخدمات الإلكترونية.
- دعم التحول الرقمي الوطني بطريقة منظمة.

12. نموذج مقترح لحوكمة تكنولوجيا المعلومات وفق نظام ISO

يمكن تقديم نموذج مبسط لحوكمة تكنولوجيا المعلومات يقوم على سبعة عناصر:

- القيادة والالتزام: الادارة العليا مسؤولة عن التوجيه والرقابة
- المواءمة الاستراتيجية: التكنولوجيا تخدم أهداف المؤسسة.
- المخاطر والأمن: حماية المعلومات وإدارة المخاطر الرقمية.
- الخدمات الرقمية: ضمان جودة الخدمات واستمراريتها.

البيانات والخصوصية: حماية البيانات وضمان جودتها.

الأداء الامتثال: قياس النتائج واحترام القوانين والمعايير.

التحسن المستمر: مراجعة النظام وتطويره باستمرار.

كما يمكن ربط كل عنصر بمعيار ISO المناسب كما هو موضح في الجدول الآتي:

جدول 3: ربط كل عنصر بمعيار ISO المناسب له

عنصر الحوكمة	المعيار الداعم
التوجيه والرقابة	ISO 38500
أمن المعلومات	ISO 27001
مخاطر المعلومات	ISO 27005
ادارة الخدمات الرقمية	ISO 200001
ادارة الخدمات العامة	ISO 31000
الخصوصية	ISO 27701

خاتمة

تقدم معايير ISO إطارا علميا ومنهجيا لحوكمة تكنولوجيا المعلومات، فهي تساعد المؤسسة على الانتقال من الاستخدام التقنية غير المنتظم إلى الاستخدام المؤسسي المحكوم بالإستراتيجية، الأداء، المسؤولية، المخاطر، الأمن والامتثال. ويمثل معيار ISO 38500 المرجع الأساسي في الحوكمة، في حين تمثل المعايير ISO 27001، ISO 27005، ISO 20001، ISO 31000 أدوات داعمة لضبط الأمن، الم خاطو، الخدمات وكذلك التحسين المستمر.

ولقد نصت العديد من الأدبيات (ياسين، 2005؛ السالحي، 2008؛ أبو نصر، 2007؛ Reix, Rowe, 2016; Weill, Ross, 2004) أن نجاح تكنولوجيا المعلومات لا يتحقق بمجرد توفير الأجهزة والبرمجيات ولكن من خلال إدماجها في نظام إداري وتنظي يمي واضح يدعم القرار والرقابة وخلق القيمة.

وعليه فإنه فهم ح وكمة التكنولوجيا المعلومات وفق معيار ISO يسمح بتحليل المؤسسات الرقمية بطريقة أكثر منهجية، وتقييم مدى نضجها واقتراح آليات عملية لتحسين الأداء الرقمي، حماية البيانات وإدارة المخاطر.

أسئلة المناقشة:

- ما المقصود بحوكمة تكنولوجيا المعلومات وفق ISO؟
- ما الفرق بين ISO 38500 و ISO 27001؟
- لماذا تعتبر الإدارة العليا مسؤولة عن حوكمة تكنولوجيا المعلومات؟
- ما أهمية ISO 31000 في إدارة المخاطر الرقمية؟
- كيف يمكن تطبيق ISO 20000-1 لتحسين جودة الخدمات الرقمية؟
- ما أهم التحديات لتطبيق معايير ISO في المؤسسات الجزائرية؟

المحور الثامن

حوكمة تكنولوجيا المعلومات وفق معايير ITIB

تمهيد

يعتبر ITIL من أهم الأطر المرجعية العالمية في مجال إدارة خدمات تكنولوجيا المعلومات، وهو يستعمل على نطاق واسع من طرف المؤسسات التي تسعى إلى تحسين خدماتها الرقمية، تنظيم الدعم التقني، إدارة الحوادث، رفع رضا المستخدمين والزبائن، وضمان استمرارية الخدمات.

ويعتبر ITIL إطاراً لأفضل ممارسات أكثر من كونه معياراً دولياً صارماً مثل ISO، فهو يقدم توجيهات عملية وممارسات مرنة تساعد المؤسسة على تصميم الخدمات، تسليمها وتحسينها باستمرار. كما يمكن وصف ITIL الإطار يساعد المؤسسة على تحويل تكنولوجيا المعلومات من وظيفة تقنية داخلية إلى منظومة خدماتية موجهة نحو القيمة، الجودة، الاستمرارية، ورضا أصحاب المصالح، فهو بذلك يربط كل من الاستراتيجية، التصميم، التسليم، والتحسين المستمر ضمن دورة متكاملة للخدمة الرقمية.

1. مفهوم ITIL ومكانته في حوكمة تكنولوجيا المعلومات

يشير مصطلح ITIL : Information Technology Infrastructure Library إلى مكتبة البنية التحتية لتكنولوجيا المعلومات، وقد ظهر في البداية على شكل مجموعة من الكتب التي تتضمن أفضل الممارسات المتعلقة بإدارة خدمات تكنولوجيا المعلومات، ثم تطور بعد ذلك ليهب إطاراً مرجعياً شاملاً يساعد المؤسسات على تقديم خدمات رقمية ذات جودة عالية.

يمكن تعريف ITIL على أنه إطار منظم لأفضل الممارسات في إدارة خدمات تكنولوجيا المعلومات، يهدف إلى مساعدة المؤسسات على تصميم الخدمات الرقمية، تشغيلها، دعمها، تحسينها، وربطها باحتياجات الأعمال والمستخدمين وأصحاب المصالح.

يختلف ITIL عن COBIT من حيث زاوية التركيز، حيث يركز COBIT على الحوكمة وإدارة تكنولوجيا المعلومات على مستوى المؤسسة ككل، من حيث الرقابة، المخاطر وخلق القيمة. أما ITIL فيتم بصورة أكبر بإدارة الخدمات الرقمية، أي كيف يتم تصميم الخدمة؟ كيفية دعمها؟ وكيف تقاس جودتها؟ وكيف تحسن باستمرار؟ وعليه يمكن القول أن ITIL

يدعم حوكمة تكنولوجيا المعلومات من خلال تنظيم البعد الخدماتي والتشغيلي للتكنولوجيا.

وفي نفس السياق نجد أن (السالمي، 2008) يوضح أن إدارة المعلومات تتطلب تنظيم الموارد التقنية، البشرية الإجرائية بما يخدم الأداء المؤسسي وهذا ما يتوافق مع فلسفة ITIL التي تنظر إلى التكنولوجيا ليس كأدوات فقط ولكن كخدمات موجهة نحو المستخدم والقيمة.

2. تطور ITIL من ادارة العمليات الى ادارة المنتجات والخدمات الرقمية

تم تطور ITIL عبر عدة مراحل انطلاقاً من الإصدارات الأولى حيث كان التركيز منصبا على تنظيم العمليات التقنية مثل إدارة الحوادث، إدارة المشكلات إدارة التغيير وإدارة الإصدارات، إلى ITIL الإصدار الثالث الذي يعتمد منطق دورة حياة الخدمة، بدءاً من استراتيجيات الخدمة إلى تصميمها، ثم تشغيلها، ثم تحسينها المستمر، في حين الإصدار الرابع كان أكثر تركيزاً على خلق القيمة، المرونة، التعاون، التحسين المستمر وكذا التكامل مع المناهج مثل Lean و Agile أما التوجهات الحديثة فهي أكثر تركيزاً على إدارة المنتجات والخدمات الرقمية، الخبرة، الاستراتيجيات، التحول والذكاء الاصطناعي المسؤول. ويتم وصف ITIL الجديد بأنه عملي ومصمم لبيئة رقمية قائمة على الذكاء الاصطناعي.

3. علاقة ITIL بحوكمة تكنولوجيا المعلومات

يمثل ITIL إطاراً غير مستقلاً عن الحوكمة، فهو أداة داعمة لها، حيث إذا كانت حوكمة تكنولوجيا المعلومات تهتم بالسؤال هل تستخدم المؤسسة التكنولوجيا بطريقة تخلق قيمة وتدير المخاطر فإن معيار ITIL يهتم بالسؤال كيف تهتم خدم التكنولوجيا المعلومات بطريقة فعالة، موثوقة وقابلة للتحسين.

يرى كل من (Weill, Ross, 2004) أن حوكمة تكنولوجيا المعلومات تركز على تحديد حقوق القرار وآليات المسألة التي توجه استخدام تكنولوجيا المعلومات داخل المؤسسة، وعليه فإن ITIL يساعد على ترجمة هذه القرارات إلى ممارسات خدمتية مثل تحديد

مستويات الخدمة ، إدارة الحوادث، تحسين تجربة المستخدم، ضبط التغيير الإداري، الموردین، وتقييم الأداء.

يرتبط ITIL بمعيار 2018 : ISO 20000-1 الذي يهتم بإدارة خدمات تكنولوجيا المعلومات حيث يحدد متطلبات إنشاء، صيانة وتحسين نظام إدارة ال خدمات ويشمل التخطيط، التصميم، الانتقال، التسليم و التحسين بهدف خلق القيمة وتلبية متطلبات الح وكمة. وعليه فإن ITIL يعتبر إطارا عملي ا يساعد على عملية الاستعداد لتطبيق ISO 20000-1، بينما يمنح هذا الأخير الطابع المعياري القابل للتدقيق والشهادة.

4. المفاهيم الأساسية في ITIL

- مفهوم الخدمة: الخدمة من منظور ITIL، لا تعني مجرد نظام معلوماتي أو تطبيق تقني، فهي تعني الوسيلة لتمكين الزبون أو المستخدم من تحقيق نتيجة معينة دون أن يتحمل كل التغيرات والمخاطر المرتبطة بالتكنولوجيا. فعلى سبيل المثال فإن خدمة البريد الإلكتروني ليست فقط خادما وبرنامج ا، ولكن هي قدرة المستخدمين على التواصل بطريقة آمنة موثوقة ومستمرة. وهذا ما يؤكد (الطائي والعبادي، 2009) أي أن نظم المعلومات الإدارية لا تفهم فقط من خلال مكوناتها التقنية ولكن من خلال مساعدتها في تحسين العمل الإداري ، وتدقق المعلومات واتخاذ القرار.
- مفهوم القيمة: لا تخلق القيمة في ITIL من طرف مزود الخدمة لوحده ، بل تخلق من خلال التفاعل بين مزود الخدمة والمستخدمين منها . وتكون الخدمة ذات قيمة إذا كانت متقدمة تقنيا. وقد أشار (Devenport, Prusak, 1998) إلى أن المعلومات لا تتحول إلى معرفة وقيمة إلا إذا تم استخدامها في سياق تنظيمي مناسب. وعليه فإن الخدمة الرقمية لا تعد ناجحة إلا عندما تساهم في تحقيق نتيجة مفيدة للمؤسسة وكذلك للزبون.
- مفهوم المستخدم والزبون والراعي: حسب ITIL ا يتم التمييز بين عدة أطراف: المستخدم وهو من يستعمل الخدمة يوميا، الزبون وهو من يحدد متطلبات الخدمة ويقوم ملائمتها. الراعي وهو من يوافق على تمويل الخدمة أو يتحمل تكلفتها.

هذا التميز بين الأفراد الثلاثة ضروري في حوكمة تكنولوجيا المعلومات، لأن الخدمة قد تصمم بطريقة ترضي الإدارة لكنها لا تلبي حاجات المستخدم أو قد تكون مقبولة بالنسبة للمستخدم لكنها مكلفة وغير مستدامة مالياً.

- مفهوم مستوى الخدمة: يتمثل مستوى الخدمة في درجة الجودة المتوقعة من الخدمة، مثل توفر النظام، سرعة الاستجابة، زمن إصلاح الأعطال، عدد الكوارث المقبول، وحماية البيانات. وعادة ما يتم تنظيم ذلك من خلال اتفاقيات مستوى الخدمة.

5. نظام قيمة الخدمة في ITIL

يقوم ITIL على مفهوم أساسي وهو نظام قيمة الخدمة التي يمثل الطريقة التي تتكامل بها مكونات المؤسسة وأنشطتها لتحويل الطلبات والفرص إلى قيمة ويقدم المفاهيم والنماذج والمبادئ الأساسية لإدارة المنتجات والخدمات الرقمية، ويوفر لغة مشتركة لفهم كيفية خلق القيمة والحفاظ عليها، ويمكن تبسيط هذا النظام في مجموعة من العناصر، وهي:

- المبادئ الموجهة: تتمثل هذه المبادئ الموجهة في القواعد العلمية التي تساعد المؤسسة على اتخاذ قرارات رشيدة في إدارة الخدمات مثل التركيز على القيمة، البدء في الوضع الحالي، التقدم التدريجي مع التغذية الراجعة، التعاون، التفكير الشمولي، البساطة والتحسين المستمر.
- هذه المبادئ ذات أهمية لأنها تجنب المؤسسة من تطبيق ITIL بطريقة جامدة وكذلك من نسخ ممارسات جاهزة ، ولكن تقوم بتكييفها مع واقع المؤسسة، مواردها، ثقافتها، مستوى نضجها.
- الحوكمة: تسمح الحوكمة داخل ITIL بوجود آليات لتقييم الخدمات، توجيهها، ومراقبة نتائجها، لأن الخدمة لا يتم إدارتها من الناحية التقنية فقط ولكن يجب أن تخضع للرقابة، المساءلة، وقياس القيمة.
- سلسلة قيمة الخدمة: تتمثل هذه السلسلة في الأنشطة التي تقوم بها المؤسسة لخلق الخدمة وتحسينها وتشمل التخطيط، التحسين، التفاعل مع أصحاب المصالح، التصميم والانتقال أو البناء، التسليم والدعم.

- الممارسات: يتم استبدال العمليات الجامدة في ITIL بمفهوم الممارسات وتتمثل في الموارد التنظيمية المصممة لأداء عمل معين أو تحقيق هدف محدد وهذا التحول مهم لأنه يجعل ITIL أكثر مرونة وقابلية للتطبيق في بيئة التحول الرقمي.
- التحسين المستمر: التحسين المستمر مهم جدا في ITIL لأن المؤسسة تقوم بقياس أداء الخدمة، تجمع التغذية الراجعة، تحلل المشكلات، ثم تقوم بتطوير الخدمة تدريجيا.

6. الأبعاد الأربعة لإدارة الخدمات في ITIL

يتم إدارة الخدمات في نظام ITIL من خلال أربعة أبعاد مترابطة، لا يمكن إهمال أي منها حتى إذا كانت الأبعاد الأخرى قوية، لأن هذا سيؤدي إلى ضعف الخدمة.

- المنظمات والأفراد: يتمثل هذا البعد في الهيكل التنظيمي، الأدوار، المسؤوليات، الثقافة، الكفاءات، السلوك، والقيادة. ف في حالة المستخدمين مدربين جيدا، والمسؤوليات واضحة فإن الخدمة تكون جيدة. وهذا ما أكد عليه (أبو النصر، 2015) أن تكنولوجيا المعلومات لا تحقق قيمة دون رأس مال بشري ومعرفي قادر على استخدامها وتبادل المعرفة من خلالها.
- المعلومات والتكنولوجيا: يتمثل هذا البعد في كل البيانات، التطبيقات، البنية التحتية، الأمن، قواعد البيانات، أدوات المراقبة، والمنصات الرقمية. وحسب ITIL فإن التكنولوجيا لا يجب أن تكون مجرد اختيار تقني معزول، بل يجب أن تكون ملائمة للخدمة.
- الشركاء والموردين: قد تحتاج المؤسسة من أجل تقديم الخدمات الرقمية الى مزودي سحابة، شركات برمجيات، موردي شبكات، أو مراكز بيانات خارجية. وعليه لابد من إدارة الموردين والعقود ومستويات الخدمة وكل المخاطر المرتبطة بهم.
- تدفقات القيمة والعمليات: يركز هذا البعد على كيفية انتقال الخدمة من الطلب إلى التسليم، وكيف تتحرك المعلومات والأنشطة بين الوحدات المختلفة. وتكمن أهمية هذا البعد في كشف التعقيد، التكرار، التأخير، وكذلك نقاط الضعف داخل الخدمة.

7. أهم ممارسات ITIL في دعم حوكمة تكنولوجيا المعلومات

- **ادارة الحوادث:**الهدف من إدارة الحوادث: استعادة الخدمة في أسرع وقت ممكن بعد وقوع خلل أو توقف، مع تقليل أثر الحادث على المستخدمين والمؤسسة.ولا تهدف هذه الممارسة إلى حل السبب الجذري مباشرة، ولكن إلى إعادة الخدمة إلى وضع مقبول. فمثلا في حالة توقف نظام الفوترة، فإن الأولوية الأولى هي إعادة الخدمة أو ايجاد حل مؤقت.
- **ادارة المشكلات:**تهتم إدارة المشكلات بتحديد الأسباب الجذرية للحوادث المتكررة ومنع تكرارها. فمثلا في حالة توقف نظام الفوترة باستمرار، فإن إدارة المشكلات تبحث عن السبب الحقيقي: هل الخلل في الخادم؟ أم في ضعف التطبيق؟ أم المشكلة في قاعدة البيانات؟ أو نقص في السعة؟ تسمح هذه الممارسة في تحول المؤسسة من رد الفعل إلى التحسين والتعلم.
- **ادارة التغيير:**تسعى إدارة التغيير إلى ضمان أن التعديلات على الأنظمة والخدمات تتم بطريقة منظمة، مع تقييم المخاطر، الاختبار، والتوثيق. لأن كثير من الأعطال الكبرى لا تنتج عن هجمات خارجية، ولكن من تغييرات داخلية غير مضبوطة.
- **ادارة مستوى الخدمة:**تعد هذه الممارسات من أهم ممارسات ITIL لأنها تربط الخدمة بتوقعات المستخدمين ومؤشرات الأداء. ويتم ذلك عن طريق اتفاقيات مستوى الخدمة، مثل نسبة توفر النظام، زمن الاستجابة، و كذلك الزمن اللازم لحل الأعطال.
- **مكتب الخدمة:** يمثل مكتب الخدمة نقطة الاتصال الرئيسية بين مزود الخدمة والمستخدمين. وهو كذلك أداة استراتيجية تسمح بفهم تجربة المستخدم، تسجيل الحوادث، توجيه الطلبات، وقياس جودة الخدمة.
- **ادارة المعرفة:**تسمح إدارة المعرفة بتوفير المعلومات المناسبة للأشخاص الملائمين في الوقت الملائم. وهي مهمة جدا في بيئة الدعم التقني ، لأن وجود قاعدة معرفة جيدة يسمح بتقليل زمن حل المشكلات وكذلك يرفع جودة الخدمة.وقد أشار (أبو النصر، 2015) أن إدارة المعرفة وتكنولوجيا المعلومات تتطلبان بنية معلوماتية وثقافة تنظيمية تساعد على إنتاج المعرفة وتداولها وتوظيفها.

- إدارة الاستمرارية: تهدف هذه الممارسة إلى ضمان استمرارية الخدمات الحرجة أو استعادتها بعد الأزمات. و تكون مرتبطة مباشرة بمخاطر تكنولوجيا المعلومات، الأمن السيبراني، وخطط التعافي من الكوارث.
- إدارة أمن المعلومات: تهدف هذه الممارسة الى حماية سرية المعلومات، توافرها، وسلامتها.
- التحسين المستمر: يمكن التحسين المستمر المؤسسة منقياس الأداء، تحد يي الفجوات، ترتيب الأولويات، تنفيذ التحسينات، ثم تعيد التقييم. وهذا ما يجعل ITIL إطارا ديناميكيا

8. ITIL كأداة لتحسين جودة الخدمات الرقمية

يساهم ITIL في تحسين جودة الخدمات الرقمية من خلال تحويل العمل التقني إلى خدمة قابلة للقياس. فبدلا ما يكون قسم تكنولوجيا المعلومات منشغلا فقط بإصلاح الأعطال، يصبح مسؤولا عن تقديم قيمة مثل: خدمة مستقرة، معلومات موثوقة ، تجربة مستخدم جيدة، واستجابة فعالة.

ويمكن قياس جودة الخدمة الرقمية من خلال العديد من المؤشرات مثل:

- معدل توفر الخدمة.
- متوسط زمن الاستجابة.
- متوسط زمن حل الحوادث.
- عدد الحوادث المتكررة.
- مستوى رضا المستخدمين.
- نسبة الالتزام باتفاقيات مستوى الخدمة.
- عدد التغييرات الناجحة.
- عدد المشكلات التي تم معالجة سببها الجذري.
- جودة قاعدة المعرفة.

وهذا ما أشار اليه (Kaplan, Norton, 1996) في بطاقة الأداء المتوازن، حيث في رأيهم لا ينبغي قياس الأداء بالمؤشرات المالية فقط ، ولكن لا بد من إدماج العمليات الداخلية، التعلم، الزبائن، والتحسين المستمر.

9. علاقة بين ITIL و ISO 20000-1

يعتبر المعيار الدولي ISO 20000-1 الأكثر ارتباطاً بإدارة خدمات تكنولوجيا المعلومات لأنه يحدد متطلبات نظام إدارة ال خدمة، لكن ITIL يقدم ممارسات عملية يمكن أن تساعد المؤسسة على بناء هذا النظام. وعليه فإن ITIL يساعد على معرفة كيف يمكن إدارة الخدمة وتحسينها أما ISO 20000-1 فيحدد ما هي المتطلبات التي يجب احترامها لإثبات وجود نظام إدارة الخدمة وهو يشمل التخطيط، التصميم والانتقال والتسليم وتحسين الخدمات وتستعمله المؤسسات حتى تظهر قدرتها على إدارة الخدمات ومراقبتها وقياسها وتحسينها. وعليه فإن المؤسسة التي تطبق ITIL بصورة ناضجة تكون أكثر قدرة على المطابقة مع ISO 20000-1 خاصة إذا قامت بتوثيق إجراءاتها، تحديد مؤشرات الأداء وكذلك إقامة نظاماً واضحاً للتحسين المستمر.

10. العلاقة بين ITIL و COBIT

لا ينبغي تقديم ITIL كإطار بديل عن COBIT، بل مكملاً له لأن COBIT، يجب أن يجيب عن السؤال: كيف نوجه ونراقب تكنولوجيا المعلومات على مستوى المؤسسة؟ في حين ITIL يجيب عن سؤال إدارة الخدمة: كيف نصمم ونسلم ونندعم حسن الخدمات الرقمية؟ وعليه فإن المؤسسة الناضجة رقمياً لا تقوم باختيار بين هذين الإطارين، بل تدمجهما حسب حاجتها وهذا يتفق مع طرح (De Haes, Van Grembergen, 2015)، اللذان يؤكدان أن حوكمة تكنولوجيا المعلومات تتطلب دمج الأطر والممارسات بما يحقق المواءمة والقيمة وإدارة المخاطر.

11. تطبيق بين ITIL و COBIT

يتم تطبيق ITIL داخل المؤسسة، مروراً بعدة مراحل تدريجية:

- **تشخيص الوضع الحالي:** خلال هذه المرحلة، تبدأ المؤسسة بتحليل خدماتها الحالية: ما الخدمات المقدمة؟ من يستخدم هذه الخدمات؟ ما الأعطال المتكررة؟ هل توجد اتفاقيات مستوى الخدمة؟ هل توجد قاعدة معرفة؟ هل يتم قياس رضا المستخدمين؟
- **تحديد الخدمات الحرجة:** يجب تحديد الخدمات الأكثر أهمية وتطبيق ITIL عليها، حيث لا ينبغي تطبيق هذه المعايير دفعة واحدة على كل شيء. فمثلاً من الأفضل

البدء بالنظام المحاسبي أو البريد الإلكتروني، أو منصة الزبائن، أو الشبكة الداخلية، أو نظام الموارد البشرية.

- بناء مكتب خدمة: يعتبر مكتب الخدمة نقطة انطلاق عملية لأنه يسمح بتجميع الطلبات والحوادث بدلاً من تبقى موزعة بين الأفراد بطريقة غير منظمة.
- توثيق الحوادث والطلبات: يسمح التوثيق ببناء ذاكرة تنظيمية من جهة، وتحليل الحوادث المتكررة ومعرفة أسباب الضبط على الخدمات من جهة أخرى.
- تحديد مؤشرات الأداء: يجب اعتماد مؤشرات واضحة مثل زمن الاستجابة، عدد الحوادث، رضا المستخدمين، زمن الحل وغيرها.
- تنظيم إدارة التعبير: في هذه المرحلة، يجب أن يوضع أي تغيير في الأنظمة إلى تقييم، وموافقة واختبار وتوثيق خاصة في حالة الخدمات الحرجة.
- تفعيل التحسين المستمر: بعد جمع كل البيانات، يجب القيام بتحويلها ومن ثم اقتراح تحسينات دورية.

12. ITIL والتحول الرقمي

لا تقتصر أهمية ITIL على إدارة الدعم الفني، بل تمتد إلى إدارة المنتجات والخدمات الرقمية بصورة شاملة خاصة في حالة التحول الرقمي، فهو يقوي التركيز على الجودة وكفاءة الخبرة والقيمة وكذلك النتائج في إدارة المنتجات والخدمات الرقمية، كما يربط بين أهداف الأعمال، تجربة الزبون، وكذلك التنفيذ التشغيلي. ولكن يهتم بتقديم خدمات رقمية موثقة مستمرة ومبنية على تجربة المستخدم فمثلاً المؤسسة التي تطلق منصة إلكترونية بدون مكتب خدمة، أو إدارة الحوادث، أو دون اتفاقيات مستوى خدمة، ودون مراقبة الأداء، قد تفشل في كسب ثقة المستخدمين بالرغم من امتلاكها لتكنولوجيا حديثة.

13. تحديات تطبيق ITIL في المؤسسات الجزائرية

تواجه المؤسسات الجزائرية عدة تحديات في تطبيق ITIL منها:

- ضعف ثقافة الخدمة داخل بعض إدارات تكنولوجيا المعلومات.
- التركيز على الجانب التقني أكثر من تجربة المستخدم.
- غياب مؤشرات أداء واضحة.
- ضعف توثيق الحوادث والطلبات.

- مقاومة التغيير.
 - نقص التكوين في إدارة خدماتتكنولوجيا المعلومات.
 - غياب مكتب خدمة منظم
 - ظرف التكامل بين إدارة تكنولوجيا المعلومات وبقية الإدارات.
 - الاعتماد على الحلول الفردية بدلا من الإجراءات المؤسسية.
- وقد أكدت الأدبيات العربية (ياسين، 2018؛ أبو النصر، 2015؛ السالمي، 2008) أن نجاح نظم المعلومات في البيئة العربية يتطلب معالجة الجوانب التنظيمية والبشرية والثقافية إلى جانب الجانب التقني. وعليه فإنه تطبيق ITIL في هذه المؤسسات لا ينبغي أن يكون تطبيقا شكليا بل يجب أن يتكيف مع حجم المؤسسة ، مستوى نضجها الرقمي ، طبيعة خدماتها، ومواردها البشرية.

14. مزايا معيار ITIL

يوفر ITIL مجموعة من المزايا نذكر منها:

- تحسين جودة خدمات تكنولوجيا المعلومات.
- تقليل زمن معالجة الحوادث.
- رفع رضا المستخدمين.
- توضيح الأدوار والمسؤوليات.
- تحسين إدارة التغيير.
- تقليل الحوادث المتكررة من خلال إدارة المشكلات.
- ربط الخدمات الرقمية بالقيمة.
- دعم التحسين المستمر.
- تسهيل التوجه نحو ISO 20000-1.
- تعزيز لغة مشتركة بين التقنيين والإدارة والمستخدمين.

15. حدود ITIL

- قد يفشل تطبيق ITIL إذا لم يتم تطبيقه بطريقة صحيحة وإذا تم تبني ه بطريقة بيروقراطية حرفية بدون تكيف، وعليه من أبرز حدوده:
- يتحول معيار ITIL إلى إجراءات ثقيلة إذا اسيء تطبيقه.

- يحتاج إلى ثقافة تنظيمية قائمة على الخدمة والتحسين.
 - لا يمكنه تعويض الحوكمة الاستراتيجية في معيار COBIT.
 - بمفرده لا يمكنه منع شهادة المعيارية مثل ISO 20000-1.
 - يتطلب تكوين وتغييرا في طريقة العمل.
 - يمكن أن يواجه مقاومة من طرف الفرق التقنية وهذا إذا ما اعتبر وسيلة رقابة إضافية بدلا من أداة لتحسين.
- وعليه فإن التطبيق الناجح لـ ITIL يتطلب قيادة داعمة، توعية، تدرج في التنفيذ، مؤشرات أداء، ومراجعة مستمرة.

خاتمة

يمثل ITIL إطارا مرجعيا مهما بالنسبة لإدارة خدمات تكنولوجيا المعلومات فهو يساهم في دعم حوكمة التكنولوجيا من خلال تنظيم الخدمات الرقمية، ضبط الحوادث، إدارة التغيير، تحسين تجربة المستخدم، قياس الأداء، وتفعيل التحسين المستمر. وبلوغهم من أن ITIL ليس معيارا دوليا بالمعنى الصارم، إلا أنه يمكن أن يشكل أداة عملية لبناء إدارة خدمات قابلة للتقييم والتطوير وذلك إذا ما ارتبط بمعيار ISO 20000. وتؤكد العديد من الأدبيات (ياسين، 2005؛ السالمي، 2008؛ أبو النصر، 2015) أن نجاح تكنولوجيا المعلومات لا يتحقق من خلال امتلاك الأنظمة والمعايير فقط، ولكن من خلال تحويلها إلى خدمات ذات قيمة، منظمة، قابلة للقياس، وموجهة نحو المستخدمين وأهداف المؤسسة. إن دراسة معيار ITIL تساعد على فهم البعد التشغيلي والخدمي لحوكمة تكنولوجيا المعلومات، وتمنحه أدوات عملية لتحليل جودة الخدمات الرقمية ككل المؤسسات، خاصة في سياق التحول الرقمي.

أسئلة المناقشة:

- لماذا يعد ITIL إطاراً لأفضل الممارسات وليس معياراً دولياً بالمعنى الصارم؟
- ما الفرق بين ITIL و COBIT في حوكمة تكنولوجيا المعلومات؟
- كيف تساعد إدارة الحوادث وإدارة المشكلات في تحسين جودة الخدمات الرقمية؟
- ما أهمية اتفاقيات مستوى الخدمة في إدارة الخدمات؟
- كيف يرتبط ITIL بمعيار ISO 20000؟
- ما دور مكتب الخدمة في تحسين تجربة المستخدم؟
- ما أهم تحديات التي يواجهها تطبيق ITIL في المؤسسات خاصة الجزائرية منها؟

خاتمة

أصبحت حوكمة تكنولوجيا المعلومات من القضايا الأساسية في إدارة المؤسسات الحديثة، بسبب الدور المتزايد الذي أصبحت تؤديه التكنولوجيا في مختلف الوظائف الإدارية والمالية والتشغيلية والاستراتيجية.

لم تعد تكنولوجيا المعلومات وسيلة مساعدة لتسريع العمل أو تخزين البيانات فقط، ولكن تحولت إلى مورد استراتيجي، يؤثر في قدرة المؤسسة على المنافسة، جودة اتخاذ القرار، كفاءة الأداء، إدارة المخاطر، حماية المعلومات، وتحقيق القيمة المستدامة.

إن امتلاك التكنولوجيا وحدها لا يكفي لضمان النجاح المؤسسي، فيمكن للمؤسسة أن تتوفر على أنظمة معلومات متطورة، برمجيات حديثة، وبنية تحتية رقمية قوية، ولكن تفشل في تحقيق أهدافها في غياب رؤية إستراتيجية واضحة وضعف آليات الرقابة وغياب المسؤوليات واضحة. وهنا تظهر أهمية حوكمة تكنولوجيا المعلومات باعتبارها إطار يضمن توجيه التكنولوجيا نحو خدمة أهداف المؤسسة، بدلا أن تتحول إلى عبء مالي أو مصدر للمخاطر التنظيمية والأمنية.

وتتكون أهمية حكم التكنولوجيا المعلومات في قدرتها على تحقيق المواءمة بين الاستراتيجية المؤسسية والاستراتيجية الرقمية، لأن المؤسسة لا ينبغي أن تستثمر في التكنولوجيا لمجرد مواكبة الموضة الرقمية أو تقليد المنافسين. ولكن لابد أن يكون المشروع الرقمي مرتب بهدف واضح، كتحسين جودة الخدمات، دعم القرار، رفع الإنتاجية، تقليل التكاليف، تعزيز الشفافية، أو تحسين العلاقة مع المستخدمين والزبائن. وبالتالي تصبح التكنولوجيا أداة لتحقيق أهداف المؤسسة، وليس مجرد تجهيزات أو تطبيقات منفصلة عن الواقع التنظيمي.

كما تساهم حوكمة تكنولوجيا المعلومات المعلومات في خلق القيمة من الاستثمارات الرقمية لأن الإنفاق على التكنولوجيا لا يتحول تلقائيا إلى قيمة مضافة، ولكن يحتاج إلى تخطيط، تقييم، متابعة، وقياس الأداء وعليه فإن الحوكمة تساعد المؤسسة على تحديد المشاريع ذات الأولوية، تقييم العائد المتوقع منها، مراقبة تنفيذها، ومعرفة مدى مساهمتها

في تحسين الأداء المؤسسي. وهذا ما يجعل من القرار التكنولوجي قرارا عقلاني مبني على التحليل والمساءلة وليس قرارا عشوائيا أو تقني محدودا.

وتحتل إدارة المخاطر الرقمية مكانة أساسية في حوكمة تكنولوجيا المعلومات لأنه كلما زاد اعتماد المؤسسة على الأنظمة الرقمية، زادت درجة لمخاطر متعددة مثل فقدان البيانات، توقف الأنظمة، الاختراقات السيبرانية، استخدام الصلاحيات، ضعف جودة المعلومات، الاعتماد المفرط على الموردين الخارجيين وغيرها. وبالتالي، لا يمكن الحديث عن التحول الرقمي الناجح في غياب إطار حوكمي يحدد طبيعة المخاطر، درجة قبولها، آليات معالجتها، ومسؤولية الأطراف المعنية بها.

كما تبرز أهمية حوكمة تكنولوجيا المعلومات في مجال حوكمة البيانات باعتبار هذه الأخيرة من أهم أصول المؤسسة الحديثة وهي الأساس التي تبنى عليه القرارات الإدارية، المالية، التسويقية، الاستراتيجية. لكن البيانات لا تكون دقيقة إلا إذا كانت، آمنة، دقيقة، محدثة، قابلة للتتبع، ومحوكمة بسياسات واضحة من يملكها، من يستعملها، كيف تخزن، وكيف يتم حمايتها. وعليه فإن ضعف حوكمة البيانات يمكن أن يؤدي إلى ضعف القرار أو فقدان الثقة أو تعرض المؤسسة لمخاطر قانونية وتنظيمية.

كذلك تساهم حوكمة تكنولوجيا المعلومات في تعزيز الشفافية والمساءلة داخل المؤسسة لأنها تحدد بوضوح من يقرر في المجال الرقمي، من ينفذ ومن يراقب ومن يتحمل المسؤولية عند حدوث أي خلل أو فشل في مشروع تكنولوجي. فغياب واضح في توزيع المسؤوليات قد يؤدي إلى ضعف التنسيق، تضارب القرارات، تكرار الأنظمة، ارتفاع التكاليف، وفشل المشاريع الرقمية.

كما تظهر أهمية الحوكمة في تحسين جودة الخدمات الرقمية خاصة من خلال إطار ITIL الذي يركز على إدارة الخدمات، معالجة الحوادث، دعم المستخدمين، إدارة تغيير، وتحسين تجربة المستخدمين. لأن التكنولوجيا لا يتم تقييمها على أساس التطور التقني فقط، ولكن بمدى قدرتها على تقديم خدمة مستقرة، سريعة، آمنة، وملائمة الى احتياجات المستخدمين. ومنه فإن المؤسسة الناجحة رقا ليست تلك التي تمتلك عددا كبيرا من الأنظمة، ولكن التي تقدم خدمات رقمية فعالة، قابلة للقياس والتحسين.

وتستند حوكمة تكنولوجيا المعلومات إلى مجموعة من الأطر والمعايير التي تساعد المؤسسة على التنظيم، التقييم والتحسين. فإطار COBIT مثلا يقدم منظرا شاملا يربط التكنولوجيا بأهداف المؤسسة، القيمة، المخاطر، الموارد والأداء. في حين معايير ISO تمنح المؤسسة مرجعية معيارية رسمية في مجالات مثل الحوكمة، أمن المعلومات، إدارة المخاطر، وإدارة الخدمات. أما ITIL فيساعد المؤسسة على تحسين البعد التشغيلي والخدمات لتكنولوجيا المعلومات. ولكن لا يجب النظر إلى هذه الأطر كبداية متنافسة فيما بينها، ولكن كأدوات متكاملة يمكن توظيفها حسب طبيعة المؤسسة، حجمها، مستوى نضجها الرقمي، وأهدافها الاستراتيجية.

في السياق الجزائري، تزداد أهمية حوكمة تكنولوجيا المعلومات في ظل توجه المؤسسات والإدارات نحو الرقمنة، الإدارة الإلكترونية، الدفع الإلكتروني، الخدمات عن بعد والاعتماد المتزايد على نظم المعلومات.

لكن هذا التوجه لا يمكن أن يحقق النتائج المرجوة إذا تم حصره في شراء التجهيزات أو إطلاق من الصوت رقمية دون إصلاح إداري تنظيمي. لأن الرقم تحتاج إلى قيادة واعية، كفاءات مؤهلة، ثقافة رقمية عالية، بنية تنظيمية وقانونية ملائمة، مؤشرات أداء وحوكمة واضحة للبيانات والخدمات والمخاطر. ومنه فإن حوكمة تكنولوجيا المعلومات تعتبر شرطا أساسيا لنجاح عملية التحول الرقمي في المؤسسات الحديثة. لأنها تسمح بتجاوز التقنية الضيقة للتكنولوجيا وتضعها داخل إطار استراتيجي تنظيمي شامل، كما تضمن أن تكون التكنولوجيا في خدمة أصحاب المصالح والمؤسسة ككل وأن يتم استخدامها بطريقة آمنة، فعالة، مسؤولة، ومطابقة للقوانين والمعايير.

وبصفة عامة فإن نجاح المؤسسة في العصر الرقمي لا يرتبط فقط بامتلاكها التكنولوجيا ولكن بقدرتها على حوكمتها. تكنولوجيا غير المحكومة قد تؤدي إلى الهدر، الفوضى، المخاطر وضعف الثقة. ولكن التكنولوجيا المحكومة تصبح رافعة استراتيجية لتحسين الأداء، دعم الابتكار، تعزيز شفافية، حماية البيانات، وتحقيق القيمة المستدامة.

وعليه فإن حوكمة تكنولوجيا المعلومات ليست مجرد وظيفة تقنية أو إجراء إداري، بل هي مدخل متكامل لإدارة المؤسسة الرقمية. فهي تمثل قدرة المؤسسة على توجيه مواردها

الرقمية بوعي، ومراقبة نتائجها بفعالية، وتحقيق التوازن بين الابتكار بالمخاطر وبين الكفاءات والمثال وبين الاستثمار التكنولوجي والقيمة المؤسسية وهنا يصبح الاستثمار حوكمة تكنولوجيا المعلومات ضرورة حتمية لا تقل من الاستثمار في التكنولوجيا بحد ذاتها لأن القيمة الحقيقية لا تنتج عن التكنولوجيا في حد ذاتها ولكن تنتج عن حسن إدارتها، توجيهها، مراقبته و وربطها بأهداف المؤسسة والمجتمع.

المراجع

مراجع باللغة العربية

- ابراهيم الخلوف الملكاوي، (2023)، الحوكمة: المفاهيم والممارسات، مؤسسة الوراق للنشر والتوزيع، عمان.
- أبو النصر مدحت محمد (2015) الحوكمة الرشيدة: في ادارة المؤسسات عالية الجودة. القاهرة مصر: المجموعة العربية للتدريب والنشر.
- حماد طارق عبد العال. (2005) حوكمة الشركات: المفاهيم، المبادئ، التجارب، المتطلبات، تطبيقات الحوكمة في المصارف. الاسكندرية، مصر: الدار الجامعية.
- الخضيرى محسن أحمد. (2005) حوكمة الشركات. القاهرة، مصر: مجموعة النيل العربية.
- الطائي، إياد عبد الفتاح، والعابدي، علي حسون. (2009). إدارة ونظم المعلومات: منظور استراتيجي وتنظيمي. عمان: دار اليازوري العلمية.
- العابدي، علي حسون. (2004). دور نظم المعلومات الإدارية في تحسين الأداء المؤسسي. بغداد: دار الكتب والوثائق.
- علاء عبد الرزاق السالمي، (2003) نظم إدارة المعلومات، المنظمة العربية للتنمية الادارية القاهرة.
- علاء عبد الرزاق السالمي، (2008) تكنولوجيا المعلومات، وادارة المعرفة. عمان: دار المناهج للنشر والتوزيع.
- فريد كورتل، أمال أيوب، (2016) تكنولوجيا المعلومات ودورها في العمل الاداري والتسويقي، زمزم ناشرون وموزعون.
- محمد الشريف بن زاوي، (2016) حوكمة الشركات والهندسة المالية، دار الفكر الجامعي، الاسكندرية.
- محمد فتحي عبد الهادي، (2000) المعلومات وتكنولوجيا المعلومات على أعقاب قرن جديد، مكتبة الدار العربية للكتاب القاهرة، مصر.
- ياسين، سعد غالب. (2005). الإدارة الإلكترونية وآفاق تطبيقاتها العربية. الرياض: معهد الإدارة العامة.
- ياسين، سعد غالب. (2018). نظم المعلومات الإدارية. عمان: دار اليازوري العلمية.

مراجع باللغة الفرنسية

Braudel, F. (1979). *Civilisation matérielle, économie et capitalisme, XVe-XVIIIe siècle* (Tome 2 : Les jeux d'échange). Paris : Armand Colin.

Roland, P. (2005). *Gouvernance des entreprises et marchés financiers*. Paris : Éditions d'Organisation.

Charreaux, G. (Ed.). (1997). *Le gouvernement des entreprises: Corporategovernance, théories et faits*. Paris : Economica.

De La Bruslerie, H. (2010). *Analyse financière : Information financière, évaluation et diagnostic* (4e éd.). Paris : Dunod.

Georgel, F. (2009). *IT gouvernance: Maîtrise d'un système d'information* (3e éd.). Paris: Dunod.

Josse Roussel , *Economie et management de l'entreprise*, L'Harmattan, Paris, 2011.

Mohamed Meziane, *la communication et les nouvelles techniques de l'information*, Dar El Ayem, 1999.

Muller, J. L. (1999). *Réingénierie des processus et management des systèmes d'information*. Paris : Éditions d'Organisation.

Peter Wirtz, *Politique de financement et gouvernement d'entreprise*, Edition Economica Paris, 2002.

Reix, R., & Rowe, F. (2016). *Systèmes d'information et management des organisations* (7e éd.). Paris: Vuibert.

مراجع باللغة الإنجليزية

A.C Fernando, *CorporateGovernance: Principal, policier, practices*, Pearson Education, 2009.

Alter, S. (2002). *Information systems: The foundation of e-business* (4th ed.). Upper Saddle River, NJ: Prentice Hall.

Baskerville, R., & Siponen, M. (2002). *An information security meta-policy for emergent organizations*. *Logistics Information Management*, 15(5/6), 337–346.

- Berle, A. A., Jr., & Means, G. C. (1932). *The modern corporation and private property*. Macmillan.
- Bharadwaj, A., El Sawy, O. A., Pavlou, P. A., & Venkatraman, N. (2013). Digital business strategy: Toward a next generation of insights. *MIS Quarterly*, 37(2), 471–482.
- Carr, N. G. (2004). *Does IT matter? Information technology and the corrosion of competitive advantage*. Boston, MA: Harvard Business School Press.
- Castells, M. (2010). *The rise of the network society* (2nd ed.). Oxford: Wiley-Blackwell.
- Christman John, *The myth of property toward an egalitarian theory of ownership*, Oxford university press, New York, 1994
- Clarke, T. (2017). *International corporate governance: A comparative approach* (2nd ed.). London: Routledge.
- Clarke, T. (Ed.). (2004). *Theories of corporate governance: The philosophical foundations of corporate governance*. Routledge.
- Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2013). *Internal control — Integrated framework*. Durham, NC: COSO.
- Committee on the Financial Aspects of Corporate Governance. (1992). *Report of the Committee on the Financial Aspects of Corporate Governance*. Gee.
- Date, C. J. (2004). *An introduction to database systems* (8th ed.). Pearson
- Davenport, T. H., & Prusak, L. (1998). *Working knowledge: How organizations manage what they know*. Boston, MA: Harvard Business School Press.
- De Haes, S., & Van Grembergen, W. (2015). *Enterprise governance of information technology: Achieving alignment and value, featuring COBIT 5* (2nd ed.). Cham: Springer.

DiMaggio, P. J., & Powell, W. W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. *American Sociological Review*, 48(2), 147-160. <https://doi.org/10.2307/2095101>

Donaldson, L., & Davis, J. H. (1991). Stewardship theory or agency theory: CEO governance and shareholder returns. *Australian Journal of Management*, 16(1), 49-64. <https://doi.org/10.1177/031289629101600103>

Fama, E. F., & Jensen, M. C. (1983). Separation of ownership and control. *The Journal of Law and Economics*, 26(2), 301-325. <https://doi.org/10.1086/4/037>

Freeman, R. E. (2010). *Strategic management: A stakeholder approach*. Cambridge University Press.

Henderson, J. C., & Venkatraman, N. (1993). Strategic alignment: Leveraging information technology for transforming organizations. *IBM Systems Journal*, 32(1), 4–16. <https://doi.org/10.1093/hebz/9780198806769.001.0001>

ISACA. (2019). *COBIT 2019 framework: Governance and management objectives*.

ISO. (2018). *ISO 31000:2018: Risk management — Guidelines*. Geneva: International Organization for Standardization.

ISO/IEC. (2018). *ISO/IEC 20000-1:2018: Information technology — Service management — Part 1: Service management system requirements*. Geneva: International Organization for Standardization.

ISO/IEC. (2019). *ISO/IEC 27701:2019: Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines*. Geneva: ISO

ISO/IEC. (2022). *ISO/IEC 27001:2022: Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. Geneva: International Organization for Standardization.

ISO/IEC. (2024). ISO/IEC 38500:2024: Information technology — Governance of IT for the organization. Geneva: International Organization for Standardization.

IT Governance Institute. (2003). Board briefing on IT governance (2nd ed.). Rolling Meadows, IL: IT Governance Institute.

Jensen, M. C., & Meckling, W. H. (1976). Theory of the firm: Managerial behavior, agency costs and ownership structure. *Journal of Financial Economics*, 3(4), 305-360. [https://doi.org/10.1016/0304-405\(76\)90026-X](https://doi.org/10.1016/0304-405(76)90026-X)

Kaplan, R. S., & Norton, D. P. (1996). The balanced scorecard: Translating strategy into action. Boston, MA: Harvard Business School Press.

Kimball, R., & Ross, M. (2013). The data warehouse toolkit: The definitive guide to dimensional modeling (3rd ed.). Indianapolis, IN: Wiley.

Kral, P. (2012). Incident response and management in enterprise IT governance. New York: Academic Press.

La Porta, R., Lopez-de-Silanes, F., Shleifer, A., & Vishny, R. W. (1999). Corporate ownership around the world. *Journal of Finance*, 54(2), 471–517.

Laudon, K. C., & Laudon, J. P. (2022). Management information systems: Managing the digital firm (17th ed.). Harlow: Pearson.

Mahmood, R., Shah, A., & Khan, S. (2013). Risk management frameworks in cloud computing environments. *Journal of Information Technology Management*, 24(3), 12–25.

Mallin, C. A. (2019). Corporate governance (6th ed.). Oxford University Press.

Meyer, J. W., & Rowan, B. (1977). Institutionalized organizations: Formal structure as myth and ceremony. *American Journal of Sociology*, 83(2), 340-363. <https://doi.org/10.1086/226550>

Mintzberg, H. (1982). Structure et dynamique des organisations. Paris: Éditions d'Organisation.

Monk, E., & Wagner, B. (2012). *Concepts in enterprise resource planning* (4th ed.). Boston, MA: Cengage Learning.

Monks, R. A. G., & Minow, N. (2011). *Corporate governance* (5th ed.). Wiley.

National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0 (NIST CSWP 29)*. Gaithersburg, MD: U.S. Department of Commerce.

O'Brien, J. A., & Marakas, G. M. (2010). *Management information systems* (10th ed.). New York, NY: McGraw-Hill.

Organisation for Economic Co-operation and Development.(2004). *OECD principles of corporate governance 2004*. OECD Publishing. <https://doi.org/10.1787/9789264015999-en>

Organisation for Economic Co-operation and Development.(2023). *G20/OECD principles of corporate governance 2023*. OECD Publishing. <https://doi.org/10.1787/ed750b30-en>

Peltier, T. R. (2016). *Information security policies, procedures, and standards: Guidelines for effective information security management*. Auerbach publication.

Pfeffer, J., & Salancik, G. R. (1978). *The external control of organizations: A resource dependence perspective*. Harper & Row.

Porter, M. E., & Millar, V. E. (1985). How information gives you competitive advantage. *Harvard Business Review*, 63(4), 149–160.

Romney, M. B., & Steinbart, P. J. (2017). *Accounting information systems* (14th ed.). Harlow: Pearson.

Ross, J. W., Weill, P., & Robertson, D. C. (2006). *Enterprise architecture as strategy: Creating a foundation for business execution*. Boston, MA: Harvard Business School Press.

Russell, S., & Norvig, P. (2020). *Artificial intelligence: A modern approach* (4th ed.). Hoboken, NJ: Pearson.

Shleifer, A., & Vishny, R. W. (1997). A survey of corporate governance. *The Journal of Finance*, 52(2), 737-783. <https://doi.org/10.1111/j.1540-6261.1997.tb04820.x>

Snedaker, S. (2013). *Business continuity and disaster recovery planning for IT professionals* (2nd ed.). Waltham, MA: Syngress.

Solomon, J. (2020). *Corporate governance and accountability* (5th ed.). Wiley.

Solove, D. J. (2013). *Nothing to hide: The false tradeoff between privacy and security*. New Haven, CT: Yale University Press.

Stair, R. M., & Reynolds, G. W. (2017). *Principles of information systems* (13th ed.). Boston, MA: Cengage Learning.

Stallings, W. (2016). *Network security essentials: Applications and standards* (6th ed.). Boston, MA: Pearson.

Tanenbaum, A. S., & Wetherall, D. J. (2010). *Computer networks* (5th ed.). Boston, MA: Pearson.

Tricker, B. (2019). *Corporate governance: Principles, policies, and practices*. Oxford University Press.

Turban, E., Volonino, L., & Wood, G. (2021). *Information technology for management: Advancing sustainable, profitable business growth* (12th ed.). Hoboken, NJ: Wiley.

Weill, P., & Ross, J. W. (2004). *IT governance: How top performers manage IT decision rights for superior results*. Boston, MA: Harvard Business School Press.

Westerman, G., Bonnet, D., & McAfee, A. (2014). *Leading digital: Turning technology into business transformation*. Boston, MA: Harvard Business Review Press.

Whitman, M. E., & Mattord, H. J. (2021). *Principles of information security* (7th ed.). Boston, Cengage Learning.

Willcocks, L. P., & Lacity, M. C. (2012). *The new IT outsourcing landscape: From innovation to cloud services*. London: Palgrave Macmillan