إدراك أهمية نظام المعلومات الإلكتروني في تفعيل نظام الرقابة الداخلية في المؤسسة الاقتصادية –دراسة حالة مؤسسة Hess–

Realizing the importance of the electronic information system in activating the internal control system in the economic institution - Hess Foundation case study-

أسامة معمري[1] *، جمال عمورة[2]

[1] جامعة البليدة 2 (الجزائر)، o.mameri@uviv-blida2.dz

[2] جامعة البليدة 2 (الجزائر)، amoura_djamel@yahoo.fr

تاريخ الارسال: 2021/10/16؛ **تاريخ القبول:** 2021/11/02؛ **تاريخ النشر:** 2022/06/08

ملخص: تهدف هذه الدراسة إلى إبراز مدى إسهام نظام المعلومات الإلكتروني المعتمد على البرمجيات الحديثة والأجهزة في تفعيل نظام الرقابة الداخلية في المؤسسة Hess، ومعرفة مدى كفاءة نظام المعلومات الإلكتروني في ذات المؤسسة.

خلصنا إلى أن المؤسسة Hess تتمتع بنظام معلومات إلكتروني كفء، يسمح بتفعيل نظام الرقابة الداخلية من خلال اتباع سياسة خاصة لحماية وأمن المعلومات، بتخصيص قسم خاص بصيانة الأجهزة والمعدات وتصليحها وحمايتها من الفيروسات. وشبكة الإتصالات بتقنية IPBX يمنع اختراق الأنظمة والتلاعب بالمعلومات. وفرض قوانين تمنع نسخ وادخال المعلومات من خارج الشبكة. مع وجود فصل بين المستخدم User وAdministrator، واتباع أسلوب الرقابة المزدوجة. كما يتم وضع كلمة مرور لكل مستخدم مع إجبارية التغيير كل 45 يوم.

كلمات مفتاحية: نظام معلومات إلكتروني، نظام رقابة داخلية، برمجيات، حماية وأمن المعلومات.

رموز تصنيف jel: M42

Abstract: This study aims to highlight the extent of the contribution of the electronic information system based on modern software in activating the internal control system in Hess.

We concluded that Hess has an efficient electronic information system that allows the internal control system to be activated by following the information protection and security policy by allocating a special section for the maintenance and repair of devices and equipment, as well as protecting them from viruses. End communication network with IPBX technology that prevents penetration and spying on Phone calls.

* المؤلف المرسل

With laws prohibiting copying and entering information from outside the network. End existence of a separation between the User and the Administration, and the method of double control. A password is set for each user with the obligation to change every 45 days.
Keywords: Electronic information system, internal control system, software, information protection and security.
Jel Classification Codes: M42.

تمهيد : إن البيئة الرقابية داخل المؤسسة تلعب دورا هاما جدا في الحد من المخاطر التي قد تتعرض لها المؤسسة، لذلك وجود نظام رقابي جيد مبني على تقييم المخاطر وتحديد الاستجابة الملائمة لها من خلال وضع اجراءات رقابة تتناسب واهمية هذه المخاطر وتطبيقه من قبل الادارات التنفيذية يقلل من احتمالية حدوث المخاطر والحد من اثارها السلبية إذا حدثت. ويلاحظ في بعض الاحيان عدم اهتمام الموظفين والمسؤولين بتطبيق اجراءات الرقابة اما بسبب الاهمال او لعدم معرفتهم بخطورة عدم الالتزام بتطبيقها واثاره السلبية على المؤسسة (الرمحي، 2019، صفحة 34). والاعتماد على الادوات التكنولوجية أصبح متداخل في أغلب المتطلبات التشغيلية اليومية بمعظم المؤسسات التي تهدف الى تيسير العمليات التشغيلية والانتاجية وتفعيل إجراءات الرقابية، وحماية أنظمتها، وتسهيل سرعة التواصل بين كافة أطراف المؤسسة.

من خلال ما سبق، يمكن طرح **إشكالية الدراسة** على النحو التالي:

إلى أي مدى يسهم نظام المعلومات الإلكتروني في تفعيل نظام الرقابة الداخلية من ناحية حماية وأمن المعلومات في المؤسسة الإقصادية بالتطبيق في المؤسسة Hess ؟

تتفرع من الإشكالية **الأسئلة الفرعية** التالية:

1. ما هي العلاقة بين نظام المعلومات والرقابة الداخلية ؟
2. ما هي خصائص مكونات الرقابة الداخلية الإلكترونية ؟
3. ما هي كفاءة نظام المعلومات الإلكتروني في المؤسسة Hess ؟

4. كيف يسهم نظام المعلومات الإلكتروني في المؤسسة Hess في تفعيل نظام الرقابة الداخلية ؟

تتمثل **الهدف الأساسي للدراسة** في محاولة معرفة مدى مساهمة نظام المعلومات الإلكتروني المعتمد على البرمجيات الحديثة واستخدام الأساليب المتطورة في المعالجة البيانات في تفعيل نظام الرقابة الداخلية في المؤسسة Hess من ناحية حماية وأمن المعلومات، كما تهدف الدراسة إلى معرفة مدى كفاءة نظم المعلومات الإلكتروني في نفس المؤسسة من خلال التطرق إلى المعدات والتجهيزات المستخدمة وبرمجيات وأنظمة تشغيل، سياسة الحماية والصيانة المتبعة من طرف مصالح المؤسسة، وكذا الكفاءات وتكوينات والتدريبات الموارد البشرية.

بهدف الوصول لأهداف الدراسة، والإجابة على مختلف التساؤلات المطروحة والإحاطة بجوانب الموضوع، قمنا بالإعتماد على **المنهج الوصفي التحليلي** في كافة جوانب الإطار النظري للدراسة، من خلال تغطية الخلفية النظرية التي يرتكز عليها الموضوع. أمّا في الجانب الميداني للدراسة وكمحاولة لإسقاط الجانب النظري على أرضية الواقع، اعتمد الباحثان على المقابلة الفردية، والتحليل والاستنتاج، حيث ساعدهما في تحليل البيانات المقدمة من طرف المؤسسة محل الدراسة، والوصول إلى نتائج الدراسة.

وكإجابات قبلية عن الإشكالية والأسئلة الفرعية، اقترحنا **الفرضيتين** التاليتين:

الفرضية الأولى: يتمتع نظام المعلومات الإلكتروني للمؤسسة Hess بالكفاءة، بامتيازه لعنصر بشري كفء، ومعدات وتجهيزات حديثة وشبكات، وصيانة مستمرة لها، ومضادات للفيروسات؛

الفرضية الثانية: يسهم نظام المعلومات الإلكتروني للمؤسسة Hess بتفعيل نظام الرقابة الداخلية من ناحية حماية وأمن المعلومات.

I- الجانب النظري

1.I– أهمية ومفهوم نظم المعلومات الإلكتروني

نظرا لما تتميز به نظم المعلومات الحديثة من تعقد وتضخم في حجم البيانات التي يتم معالجتها كنتيجة منطقية لكبر حجم منشآت الأعمال، ونظرا للحاجة إلى سرعة الوصول إلى المعلومات، فقد اتجهت منشآت الأعمال في الوقت الحاضر إلى استخدام الحاسب الآلي في تشغيل بياناتها المالية والغير المالية، مما أدى إلى ما يمكن أن يطلق عليه تزاوج أو اندماج كل نظم المعلومات ونظم الحاسب الآلي ونشوء ما يمكن أن يطلق عليه بـ "نظم المعلومات الإلكترونية أو الآلية Systèmes d'information automatisé" (مصطفى، 2008، صفحة 5).

يمكن تعريف نظم المعلومات الإلكتروني على أنها: "تلك الأنظمة التي يتم الاعتماد فيها على الحاسبات ومختلف البرمجيات في تشغيل النظام، وعادة ما يتم الاعتماد على طريقة التشغيل هذه في حالة الوحدات الاقتصادية كبيرة الحجم بسبب كبر حجم البيانات التي يمكن تشغيلها" (تعلب، 2011، صفحة 147).

يمكن من خلال التعريف السابق تحديد مكونات نظام المعلومات الآلي كما يلي:

- الاعتماد على معايير تكنولوجيا المعلومات وطبقات الاتصالات والمكونات التقنية وعناصر النظام؛
- قبول الأسس الحالية للأنظمة المفتوحة: بنية متعددة الخدمات وقائمة على الويب؛
- تحديد تعليمات وإجراءات جديدة بما تتلاءم مع معايير تكنولوجيا المعلومات؛
- كما يتبع النظام المعلومات الآلي ضوابط رقابية جديدة تكون أكثر دقة من أجل تحقيق أهداف نظام الرقابة الداخلية.

I.2– العلاقة بين نظام الرقابة الداخلية ونظم المعلومات

نظام المعلومات ونظام الرقابة الداخلية يعتبران متلازمان تربطهما علاقة قوية، حيث يعد نظام المعلومات **جزءاً أساسياً** من نظام الرقابة الداخلية داخل المؤسسة، كما يجب تزويد نظم المعلومات (تنظيمها، مواردها، كفاءتها) بنظام رقابة داخلي خاص بها وتفعليه باستمرار من خلال الرقابة عليه، فنظم المعلومات تخضع لمزيد من القيود المالية والتنظيمية، كما تحتاج إلى تقدم في إطار

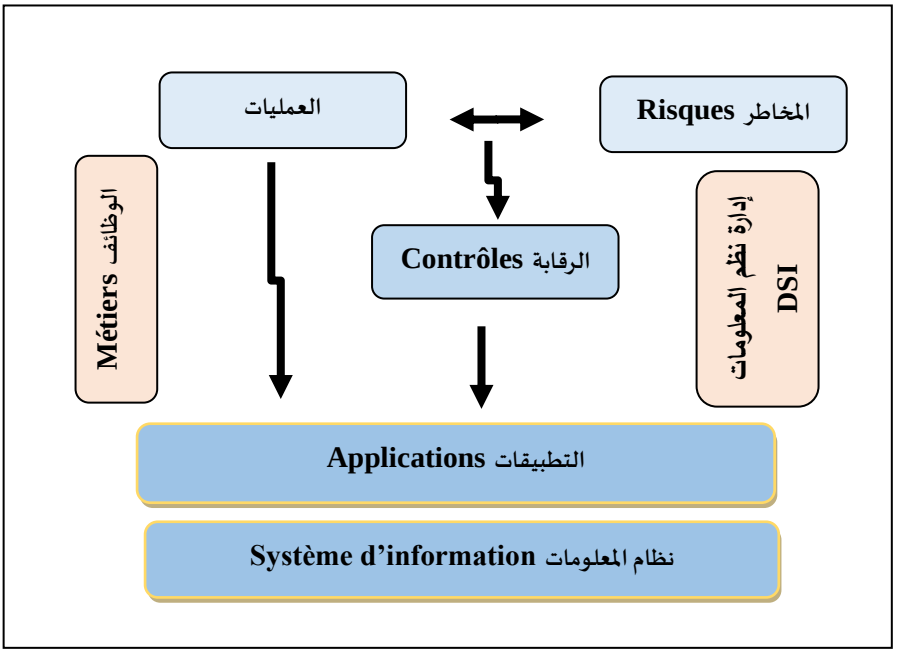
الرقابة الداخلية من خلال تعزيز الضوابط الرقابية واستخدام المعايير المتعارف عليها كالمعيار COBIT ((Brongniart, 2009, p. 30) (بتصرف).

المبادئ الخمسة للرقابة الداخلية لنظم المعلومات تتمثل في ((Delayat, 2009, p. 13:

1. يجب على الإدارة أن تخلق ثقافة وديناميكية للرقابة؛
2. يجب دمج الرقابة الداخلية في عمليات المؤسسة؛
3. تلعب نظم المعلومات دورًا رئيسيًا، فهي في نفس الوقت عنصر وأداة للرقابة الداخلية؛
4. يجب تطبيق مبدأ التناسب والأفضلية؛
5. يجب أن يكون على دراية بعدم شمولية ونطاق آليات الرقابة.

والشكل الموالي يوضح الرقابة الداخلية لنظام معلومات ما:

الشكل 1: الرقابة الداخلية لنظام المعلومات: جزئين منفصلين ومتكاملان



Source : Palais Brongniart, "**Le contrôle interne du système d'information des organisations**", Colloque IFACI_CIGREF, Mars 2009, P. 9

من خلال الشكل يمكن استخراج ثلاث نقاط أساسية تربط بين الرقابة الداخلية ونظم المعلومات الإلكتروني: ((Brongniart, 2009, p. 47:

- ✓ **رقابة الوظائف:** أي السيطرة والتحكم في الوظائف (مثل عمليات التحقق من تفويض المعاملة، والتسويات الشاملة أو غير الشاملة، ..إلخ) التي تقوم بها المؤسسات التشغيلية كجزء من العمليات. غالبًا ما تكون عناصر التحكم اليدوية التي تعتمد على التقارير التي تنتجها التطبيقات.
- ✓ **الضوابط الرقابية العامة لتقنيات تكنولوجيا المعلومات والاتصال:** الضوابط الرقابية العامة لتقنيات تكنولوجيا المعلومات هي تلك الضوابط المدمجة في عمليات وخدمات تقنيات المعلومات المتعلقة بتطوير النظم، إدارة التغيير، الأمن، التشغيل.
- ✓ **الضوابط الرقابية للتطبيقات:** تعتبر إجراءات رقابية مدمجة في استخدام التطبيقات الوظائف لكل عملية، تحديد الخطوات، الجهات الفاعلة، المخاطر والضوابط عند تصميم التطبيق.

I.3– نظام الرقابة الداخلية في بيئة التشغيل الإلكتروني " Le control interne en environment informatisé"

تعد أنظمة تكنولوجيا المعلومات جزءًا أساسيًا من عمليات المؤسسات. فهي تشكل أساس أنشطة الرقابة. وهذا الأخير يعتبر المكوّن الرابع لمكونات الرقابة الداخلية وفق إطار COSO. يمكن أن تكون عناصر الرقابة هذه إمّا: يدوية "manuels"، أو آلية "automatisés".

بالنسبة لعناصر الرقابة الإلكترونية، يتم ترميزها في التطبيقات "Applications"، لذلك من الضروري كي تكون الرقابة الداخلية في ظل التشغيل الآلي فعّالة، وجب التحقق من أن:

- ➢ الضوابط الرقابية الإلكترونية ذات صلة، مكيّفة ومنفذة بشكل صحيح ومستدام؛
- ➢ التأكد من صلاحية التطبيقات التي تنتج التقارير عند الاستخدام؛

- لا يمكن تجاوز الضوابط الرقابية باستخدام الأدوات المساعدة، سواء على قاعدة البيانات أو البرامج أو نظام التشغيل أو على مستوى الشبكة.

تكمن أهداف أنظمة المعلومات في أنه يتم تصميمها وتنفيذها من أجل معالجة وتقديم المعلومات الموثوقة التي يتم تكييفها مع احتياجات المؤسسة في الوقت المناسب، في جميع الظروف. ويجب عليهم حماية المعلومات من التلاعب والاختلاسات. كما يجب التحكم في تطور هذه الأنظمة مع أهداف المؤسسة.

يجب أن تتضمن بيئة الرقابة الداخلية للمؤسسة تقنيات تكنولوجيا المعلومات. غالبًا ما نعتبر تكنولوجيا المعلومات نشاطًا منفصلًا. يمكن أن تقدم تكنولوجيا المعلومات مخاطر جديدة، التي تتطلب ضوابط جديدة أو تعويضية أو محسنة للضوابط السابقة، أحيانًا ما تكون مهمة الرقابة غير واضحة بين تكنولوجيا المعلومات ووظائف المؤسسة. ومن هنا تكمن أهمية دور نظم المعلومات في نظام الرقابة الداخلية، الذي أكده الباحثون في وصف المكوّن الأول للرقابة الداخلية "بيئة الرقابة Contrôle environnement".

يفرض استخدام الأنظمة الإلكترونية احترام قوانين محددة، كما تؤدي استعمالها إلى ظهور مخاطر جديدة يجب تحديدها ومعالجتها، نذكر على سبيل المثال المخاطر التالية:

- الثقة المفرطة في الأنظمة أو التطبيقات التي تعالج البيانات بشكل غير صحيح، أو تعالج البيانات الغير الصحيحة، أو كليهما؛
- الوصول الغير المصرح به إلى البيانات، والتي قد تؤدي إلى تغيير أو إتلاف المعلومات، وتسجيل المعاملات الاحتيالية أو مرور إدخالات محاسبية غير صحيحة؛
- حقوق الوصول الممنوحة لموظفي تكنولوجيا المعلومات إلى الأنظمة التي يمكن أن تؤدي إلى انتهاك مبدأ الفصل بين الوظائف أو مبدأ الحاجة إلى المعرفة؛
- التعديل الغير المصرح به للبيانات المرجعية؛
- التعديل الغير المصرح به للبرامج أو الإعدادات؛
- عدم القدرة على إجراء التغييرات المطلوبة في الأنظمة والبرامج؛

- التدخلات اليدوية الغير المرغوب فيها في الأنظمة؛
- فقدان البيانات أو عدم القدرة على الوصول إلى البيانات عند الضرورة (AFAI, 2008, pp. 8-10).

أخيرًا، يتم الاستعانة بمصادر خارجية –إذا تطلب الأمر– بشكل متزايد في حال اعتمدت المؤسسة على معالجة العمليات بطريقة آلية باستخدام مكونات تكنولوجيا المعلومات. في هذه الحالة تحتفظ المؤسسة بمسؤولية الرقابة الداخلية للأنشطة الخارجية ويجب أن تتخذ الإجراءات وتعزز من الظوابط الرقابية اللازمة لضمان الحفاظ على مستوى الرقابة الداخلية من البداية إلى النهاية.

I.4– خصائص مكونات الرقابة الداخلية اليدوية "Manuels" و الإلكترونية (الآلية) "Informatisés"

نصّ المعيار الدولي للتدقيق رقم 315 الموسوم بـ "التعرف على مخاطر التحريف الجوهري وتقديرها من خلال فهم المؤسسة وبيئتها" في فقرته أ.60 على أنّ: "نظام الرقابة الداخلية في مؤسسة ما يحتوي على عناصر يدوية، وعادةً ما يحتوى على عناصر آلية. وتُعد خصائص العناصر اليدوية أو الآلية ذات صلة بتقدير المدقق للخطر، بالإضافة إلى إجراءات مراجعة اضافية مبنية علي ذلك " (SOCPA, 2017, p. 385).

كما تناولت الفقرة أ.61 من نفس المعيار 315 على أنّ "استخدام العناصر اليدوية أو الآلية في الرقابة الداخلية يؤثر على نشأة وتسجيل ومعالجة المعاملات والتقرير عنها: قد تتضمن أدوات الرقابة في نظام آلي إجراءات، مثل: الموافقات، وفحص المعاملات والتسويات. وكبديل أخر يمكن للمنشأة أن تستخدم إجراءات آلية لإنشاء، وتسجيل، ومعالجة، والتقرير عن المعاملات، وفي هذه الحالة تحل السجلات في شكلها الإلكترونى محل الوثائق الورقية. تتكون أدوات الرقابة في نظم تقنية المعلومات من السجلات الآلية (مثل أدوات الرقابة المدمجة في برامج الحاسب) وأدوات الرقابة اليدوية. إضافة إلى ذلك فإن أدوات الرقابة اليدوية قد تكون مستقلة عن تقنية المعلومات، وقد تستخدم المعلومات التي تنتجها تقنية المعلومات، أو قد تقتصر على متابعة العمل الفعال لتقنية المعلومات والسجلات الآلية والتعامل مع الاستثناءات. عندما يتم استخدام تقنية المعلومات في

إنشاء، أو تسجيل، أو معالجة، أو التقرير عن المعاملات. فإنه من الممكن أن تشمل النظم والبرامج أدوات رقابة خاصة بالإقرارات المقابلة للحسابات المهمة، أو قد تكون ضرورية للقيام بأدوات رقابة يدوية فعالة تعتمد على تقنية المعلومات. إن استخدام المؤسسة لمزيج من العناصر اليدوية والآلية في الرقابة الداخلية يختلف حسب طبيعة ومدى تعقد استخدام المؤسسة لتقنية المعلومات".

وقد نصت الفقرة أ.62 من نفس المعيار 315 على أنه "تعود تقنية المعلومات بالفائدة على الرقابة الداخلية للمؤسسة، حيث تُمكنها من تطبيق بشكل متسق قواعد عمل محددة مسبقا، وأداء عمليات حسابية معقدة عند معالجة أحجام كبيرة من المعاملات أو البيانات، وتحسين توقيت، وإتاحة، ودقة المعلومات، وتسهيل التحليل الإضافي للمعلومات، وكذا زيادة القدرة على متابعة أداء أنشطة المؤسسة وسياساتها وإجراءاتها، وتخفيض مخاطر التحايل علي أدوات الرقابة، وزيادة القدرة على تحقيق الفصل الفعال للمهام من خلال تنفيذ أدوات رقابة أمنية في التطبيقات، وقواعد البيانات، ونظم التشغيل" ((SOCPA, 2017, p. 385.

II – الجانب الميداني

بغية تسليط الضوء على مدى أهمية نظام المعلومات الإلكتروني في تفعيل نظام الرقابة الداخلية في المؤسسة، قمنا بإجراء دراسة ميدانية في الشركة المتعددة الجنسيات Hess –سوناطراك (أمريكية–جزائرية).

II.1– تقديم مختصر عن المؤسسة Hess

المؤسسة Hess هي شركة طاقة عالمية أمريكية مستقلة متعددة الجنسيات، مقرها الرئيسي نيويورك، تعمل في استكشاف وإنتاج النفط الخام والغاز الطبيعي، تم تشكيلها بواسطة اندماج شركة Hess النفط والكيميائية وشركة أمردا للبترول في عام 1968 بقيادة ليون هيس (الحرة، مؤسسة هيس، 2020).

ولقد تم انشاء الشراكة بين شركة Hess وشركة سوناطراك سنة 2000، وحسب القانون المعارف عليه فإنه تملك الشركة سوناطراك 51% بينما المؤسسة Hess تملك 49%. تاريخ تأسيسها بالشراكة مع سوناطراك في 2012، وتضم 2314 عامل (رجم، 2018، صفحة 42).

II.2– تشخيص نظام المعلومات الإلكتروني المستخدم في المؤسسة Hess

قمنا بتسليط الضوء على نظام المعلومات الإلكتروني بصفة عامة (تجهيزات ومعدات وحماية وصيانة وتراخيص ...) المستخدم من قبل المؤسسة Hess محل الدراسة. فمن خلال استخدام أداة المقابلة الشفهية وكذا المعلومات المتحصل عليها من مسؤولي مصلحة نظم المعلومات، وكذا دراسة "رجم خالد، بن عمارة الطاهر وذكار مُحَمَّد يزيد"، توصلنا إلى ما يلي:

الجدول 1: أهم مميزات نظام المعلومات الإلكتروني المستخدم في المؤسسة Hess

	التعيين	شركة Hess
الجانب المادي Hardware Networks	المعدات والتجهيزات	تحتوي معدات المؤسسة من اجهزة الكمبيوتر مكتبية لكل منصب (HP 8300, HP 8000، 12 جهاز كمبيوتر محمول (HP Pavillon i7)، أجهزة حماية فيزيائية ضد القرصنة والفيروسات (CISCO)، الجدار الناري (firewall)، مولد كهرباء، وأجهزة تخزين الكهرباءOnduleurs. كما يتوفر في المؤسسة ثلاثة خوادم متطورة اثنين منها في حالة عمل بتناوب والآخر لضمان التخزين الجيد داخل وخارج الجزائر. كما متوفر ثلاث طابعات مركزية ملونة حجم كبير و32 طابعة مكتبية من نفس النوع لتقليل تكاليف تخزين المستهلكات.
	الشبكات الموصولة بالخادم	شبكات الداخلية LAN، شبكة كمرات المراقبة، شبكة الهاتف IPBX، شبكة الاقفال اللكترونية، وVSAT.
	الحماية	CISCO وانظمة الحماية ضد الحرائق والانذار المبكر، وحدة تخزين كهرباء لكل جهاز كمبيوتر، بطاقة هوية الكترونية تخول لحاملها التنقل في لاماكن والاوقات المسموح له بها، كما متوفر مولد كهرباء.
	الصيانة والمراقبة	صيانة الشبكات، تغييرها وإضافة شبكات جديدة، وتقليص أخرى، وبعض اعمال الصيانة البسيطة لاجهزة الكمبيوتر والطابعات، والصيانة عن بعد، ومراقبة الاستغلال، اغلب الصيانة تتم خارج المؤسسة.

الموارد البشرية People Resources	الكفاءات	جزائرية واجنبية بشهادات جامعية وخبرة حسب المنصب والمهام المسندة اليه والمسؤليات، يتم التعيين عن طريق التحويل، او خارجي وفق شروط ومرحلة تجريب.
	التكوينات والتدريبات	استخدام تقنية التدريس في مكان العمل وانظمة المحاكات، وجود قاعة دائمة للتكوينات (لغة، برامج، امن صناعي..). الأستاذ جزائري او اجنبي حسب نوع التكوين.
	التوظيف والانتقاء	تعتمد على الخبرة بالدرجة الاولى والشهادات الجامعية.
	الاستجابة وقابلية التغيير	سرعة الاستجابة لكل المستحدثات، مرونة كبيرة في التغيير، لان المنصب والمهام ليست مرتبطة بالجهاز وجميع الوثائق آليا تقريبا.
البرمجيات، الصيانة وجوانب أخرى	البرمجيات وأنظمة التشغيل	- نظام التشغيل Windows 7 مرخص لكل حاسوب مكتبي؛ - نظام التشغيل Windows 2008-2012 Server مرخص للخوادم؛ - نظام ERP MAXIMO 7.0 من صنع IBM؛ - برنامج تسيير البريد الإلكتروني Exchange - الجدار الناري Firewal Cisco ASA
	التحديث	برامج حديثة ويتم تحديثها، والبعض يتم عن طريق الشركة الام كلما استدعت الحاجة لذلك، مثل ERP نسخة 2014.
	المعلومة	لا تعتبر معلومة ولا تعتمد إلا اذا ارسلت بالبريد الالكتروني، طلب حجز او تغبير حجز، اعلان اجتماع غير مبرمج ..، يتم ادخالها في النظام مرة واحدة مهما كان شكلها.
	الصيانة وعقودها	تتم الصيانة وقائية دورية مع التحسنات عند الطلب من المستعمل، وفجائية في حالة التوقف. كما أنعقود الصيانة خارجية حسب الجهاز (كمبيوتر، كامرات..)
	التراخيص	جميع المعدات ملك للشركة بوثائق والبرامج أصلية مع المفتاح.
	الارشفة الإلكترونية	لا يتم غلق اي اجراء مهما كان بدون الارشفة الالكترونية وجود مصلحة مختصة Doc Control
	الطباعة	يمنع الطباعة الا اذاا استدعت الحاجة لذلك للمحافظة على البيئة، وتقليل تكاليف الطباعة.

المصدر: من إعداد الباحثين بالإعتماد على دراسة رجم خالد، بن عمارة الطاهر وذكار محمد يزيد

من خلال الجدول نلاحظ أن المؤسسة Hess تعتمد على سياسة شراء التجهيزات والمعدات، حيث تتوفر لكل مستعمل جهاز محمول على مستوى كل مكتب من نوع HP Pavillon i7، طابعات رقمية متصلة بالشبكة نوع HP وآلات نسخ، وآلات طبع لكشف الاجر، أجهزة تأمين الكهرباء Onduleur.

كما نلاحظ أن المؤسسة Hess في إطار تدعيم العنصر البشري، تعتمد على سياسة توظيف أصحاب الخبرة والكفاءة لتشغيل الأنظمة في مديرية نظم المعلومات ومديرية تكنولوجيا المعلومات. فقد أرغمت هذه الأخيرة على ضرورة توفر الكفاءة في المورد البشري، وضمان توزيعه الأمثل على مختلف الأقسام بالمديرية، لا سيما قسم مطوري البرمجة، قسم الشبكة، قسم صيانة الأجهزة. كما تعتمد المؤسسة على سياسة التكوين في مختلف الإختصاصات، لا سيما (لغة، برامج، امن صناعي..). كما تبين لنا وجود جدار ناري عبارة عن جهاز Cisco، وأجهزة تخزين الكهرباء Onduleurs من الحجم الكبير خاصة بالخوادم.

II.3– تحليل إسهام نظام المعلومات الإلكتروني في تفعيل نظام الرقابة الداخلية

لقياس مدى إسهام نظام المعلومات الإلكتروني في تفعيل نظام الرقابة الداخلية في المؤسسة Hess، قمنا بدراسة تحليلية، من خلال الوقوف على كفاءة نظام المعلومات المطبق في المؤسسة فيما يتعلق بجانب الحماية والصيانة وصعوبة الإختراق للقواعد البيانات. ولتحديد هذا التفعيل، تبين لنا ما يلي*:

- لاحظنا وجود نقطة قوة في التصميم العام للرقابة الداخلية للمؤسسة، حيث تعزى بوجود خلية تدقيق داخلية "Cellule d'audit interne".

* تحليل الباحثين، مع الإعتماد على دراسة رجم خالد، مرجع سبق ذكره، ص ص 44-45 و47

- لاحظنا تحسن في تحديد الإجراءات الرقابية وتطويرها على مستوى المديريات والمصالح، حيث وجدنا رقابة ملائمة لمستوى المعاملات المختلفة على سبيل المثال دورة المبيعات، حيث لاحظنا وجود إجراءات رقابية مكثفة بهدف ضمان المصداقية وصحة المعلومات: استلام طلبية الشراء الخاصة بالزبون، ثم تحديد سقف الإئتمان المسموح له، إخراج فاتورة الزبون والتحقق من مطابقتها للطلبية الشراء، تسليم البضائع أو المنتجات المباعة للزبون، تحرير وصل التسليم والتحقق من مطابقته مع وصل الخروج من المخزن، تسجيل كل العمليات المنجزة في نظام معلومات محاسبي ببرمجيات غير قابلة للإختراق وتتميز بنظام أمن المعلومات.
- توفر إجراءات لحماية الأصول من التلف والضياع في دليل الإجراءات الخاص بالمؤسسة،
- وجود الفصل في المهام، حيث كل موظف يقوم بما تم توكيله في المهام، وفي حال وجود خلل معين، يتم معرفة من المتسبب في ذلك.
- مضادات للفيروسات شبكية حديثة، مع قوانين تمنع نسخ وادخال معلومات من خارج الشبكة، وجود فصل واضح بين المستخدم User وAdministrator، كما لاحظنا أنه لايمكن لأي مستخدم User التغيير في إعدادات الجهاز.
- كما قامت المؤسسة بمنح اجهزة الحاسوب ممولة لكل المسؤولين، وايظا المهندسين في مديريةDINTIC بوصل استلام وتعهد يتحمل المسؤولية التامة لحماية الجهاز ومحتواه، ويسمح لهم باخراجه من المؤسسة حتى في اوقات العطل، وذلك للتواصل مع باقي العمال في حال حدوث أي مشاكل اثناء العمل والتي تتعلق بالبرنامج، فيمكّن ذلك المسؤولين بتوجيه العمال عن كيفية تصليح المشكل. وكذلك لضمان عدم اختراق الملفات أو تحريف الأرقام في الحواسيب.
- كما يوجد على مستوى المديرية قسم صيانة الأجهزةDépartement Maintenace وهو خاص بصيانة الاجهزة والمعدات والشبكات، واي عطل مادي او فيزيائي Hard, Soft في الجهاز من ناحية التشغيل يقوم القسم بالاهتمام به وتصليحه

وصيانته وكذلك حمايته من الفيروسات بتثبيت برامج مضادات الفيروسات من شأنه دعم نظام الرقابة الداخلية.

- غرفة الخوادم Serveurs محمية بقفل إكتروني خاص يقوم بتسجيل مدة البقاء داخل الغرفة ولا يفتح إلا للأشخاص المرخص لهم أثناء أوقات العمل فقط، ومجهزة بمكيفين لضمان درجة الحرارة المناسبة داخل الغرفة، وأجهزة إنذار ضد الحرائق وأرتفاع درجة حرارة التوصيلات الكهربائية، تحتوي على خادمين Serveurs يعملان بالتوازي وفي حالة حدوث عطب في أي منهما لا يشعر المستخدمين بذلك، وتوجه رسالة من الخادم Serveur قيد التشغيل إلى رئيس قسم الإعلام الآلي للتدخل، وجود خادم ثالث يقوم بمهمة التخزين الآلي للبيانات B de Stockage.
- تمتلك مؤسسة Hess شبكة الإتصالات بتقنية IPBX: وهي عبارة عن محمول وموزع رقمي هاتف بتقنية العنوان الالكتروني IP، يسمح بتخفيض تكاليف الاتصالات ومراقبة الهاتف عن طريق شبكة LAN بتقنية عالية لنقاء الصوت، ويمنع الاختراق والتجسس على المكالمات الهاتفية.
- شبكة خاصة بالأقفال الالكترونية تعمل عن طريق البطاقات المهنية، تمكن من متابعة دخول المستخدمين إلى المؤسسة وإلى المكاتب كل حسب الصلاحيات المخصصة له، مثلا لا يمكن لأي فرد دخول غرفة الخادم إلا مهندسي تكنولوجيا المعلومات IT. وأيضا تمكن هذه البطاقات من مراقبة قيادة السيارات التابعة للمؤسسة، واكتشاف المسؤول عن الأخطاء وتجاوزات السرعة الحادة المرتكبة والمخزنة في ذاكرة السيارة.
- كما لاحظنا اتباع سياسة الرقابة المزدوجة.
- تستخدم مؤسسة Hess نظام تخطيط موارد المؤسسات ERP MAXIMO 7.0 ERP من صنع IBM استعملت المؤسسة نظام MAXIMO المصنع من قبل شركة المعلوماتية المتخصصة IBM، وهذا لما يتوفر عليه من ميزات فهو برنامج متكامل يعمل وفق نمانج، فهو نظام تقني صمّم لتنسيق جميع الموارد والمعلومات والأنشطة اللازمة لإتمام الإجراءات العملية مثل المحاسبة والموارد البشرية، وإدارة المشتريات والتخزين .... كما

يمكنه تبادل البيانات بين أجزائه المختلفة، وحملت المؤسسة Hess على عاتقها تكوين العمال الجدد على استعماله وعلى أي تحديث في البرنامج كل حسب احتياجاته.

- **سياسة حماية وأمن المعلومات المتبعة من طرف المؤسسة:** لاحظنا وجود صرامة في تشغيل البرمجيات في مختلف المصالح، حيث يتم وضع كلمة مرور " Un mot de passe " لكل مستخدم Utilisateur مع إجبارية التغيير كل 45 يوم (وفقا لما يمليه دليل الإجراءات الصادر عن الإدارة العليا للمؤسسة)، (نظام العمل 4/4) حيث تدرج كلمة المرور ضمن تسليم المهام لكل مستخدم، مع وضع قوانين صارمة تعاقب المتصرفين في البرمجيات في حال عدم الإمتثال لهذه الإجراءات، تضمن الحفاظ على الأنظمة. كما تم تسجيل طرد لموظفين تابعين لمصلحة المحاسبة والمالية وذلك راجع لعدم الإمتثال للإجراءات وإختراق كلمة المرور لمصلحة شخصية.

الخلاصة واختبار الفرضيات

من خلال الدراسة بشقيها النظري والميداني، توصلنا إلى جملة من **النتائج** أهمها أنّ نظام المعلومات الإلكتروني الخاص بالمؤسسة Hess تم تطويره وتحديثه، من خلال الإعتماد على البرمجيات الحديثة والأجهزة، حيث يسمح للمهندسين باخراج من المؤسسة الحواسيب المحمولة واستخدامها في أوقات العطل، وذلك للتواصل مع باقي الموظفين في حال حدوث أي مشاكل اثناء العمل والتي تتعلق بالبرنامج، فيمكّن ذلك المسؤولين بتوجيههم عن كيفية تصليح المشكل، وهذا من اجل ضمان السير السليم للعمل. وكذلك لضمان عدم اختراق الملفات أو تحريف الأرقام في الحواسيب. وتخصيص قسم خاص بالصيانة الأجهزة Département Maintenace وهو خاص بصيانة الاجهزة والمعدات والشبكات، واي عطل مادي او فيزيائي Hard, Soft في الجهاز من ناحية التشغيل، مهامه تصليح الأجهزة وصيانتها وكذلك حمايتها من الفيروسات بتثبيت برامج مضادات الفيروسات من شأنه دعم نظام الرقابة الداخلية. كما تمتلك مؤسسة Hess شبكة الإتصالات بتقنية IPBX وهي عبارة عن محمول وموزع رقمي هاتف بتقنية العنوان الالكتروني IP، يمنع الاختراق والتجسس على المكالمات الهاتفية. وهذا ما يثبت صحة الفرضية الأولى التي تنص على

أن نظام المعلومات الإلكتروني للمؤسسة Hess يتمتع بالكفاءة، بامتيازه لعنصر بشري كفء، ومعدات وتجهيزات حديثة وشبكات، وصيانة مستمرة لها، ومضادات للفيروسات.

كما وصلنا إلى وجود فصل بين مهام المستخدم User وAdministrator، ولا يمكن لأي مستخدم التغيير في إعدادات الجهاز. وتوفر مضادات للفيروسات شبكية حديثة، مع قوانين تمنع نسخ وادخال معلومات من خارج الشبكة. وتوفر خادمين Serveurs يعملان بالتوازي، فتوجه رسالة من الخادم Serveur قيد التشغيل إلى رئيس قسم الإعلام الآلي للتدخل. وخادم ثالث يقوم بمهمة التخزين الآلي للبيانات. كما يتم وضع كلمة مرور "Un mot de passe" لكل مستخدم مع إجبارية التغيير كل 45 يوم. ووضع قوانين صارمة تعاقب المتصرفين في البرمجيات في حال عدم الإمتثال لهذه الإجراءات، تضمن الحفاظ على الأنظمة. وهذا ما يثبت **صحة الفرضية الثانية** الدالة على أن نظام المعلومات الإلكتروني للمؤسسة Hess يسهم بتفعيل نظام الرقابة الداخلية من ناحية حماية وأمن المعلومات.

قائمة المراجع

1. رجم خالد. (2018). تقييم كفاءة نظام المعلومات الإلكتروني –دراسة مقارنة بين المؤسسة الوطنية للجيو فيزياء ENAGEO و .HESS مجلة العلوم الاقتصادية وعلوم التسيير، 42.
2. زاهر الرمحي. (2019). كيفية التعامل مع النظم الرقابية داخل المؤسسة. مجلة الأولى في التدقيق .... Auditors magazine، 34.
3. سيد صابر تعلب. (2011). نظم المعلومات الإدارية. عمان –الأردن–: دار الفكر ناشرون وموزعون، الطبعة الأولى.
4. عبد العزيز السيد مصطفى. (2008). استخدام الحاسب في التدقيق المالي والمراجعة. القاهرة –مصر–.
5. الموسوعة الحرة. (17 .October, 2020) مؤسسة هيس. تم الاسترداد من https://ar.wikipedia.org/wiki/%D9%85%D8%A4%D8%B3%D8%B3%D8%A9_%D9%87%D8%B3
6. AFAI, G. d. .(2008) *Contrôle interne et système d'information.* Paris -France-: Version validée, 2éme édition.
7. Brongniart, P. .(2009) Le contrôle interne du système d'information des organisations. *Colloque IFACI_CIGREF*) ,p..(47
8. Delayat, R. .(2009) Le contrôle interne du système d'information des organisation. *Assises de la Sécurité_ CIGREF*.
9. SOCPA..(2017) *Handbook of International Quality Control, Auditing, Review, Other Assurance, and Related Services Pronouncements -Arabic-*. Saudi.