أبرز الحلول | أطر حوكمة تكنولوجيا المعلومات

المملكة العربية السعودية | 23 يناير 2023

أصدر البنك المركزي السعودي في شهر نوفمبر 2021 تعميماً حول أطر حوكمة تكنولوجيا المعلومات كجزء من ارشادات الأمن السيبراني الصادرة عنه. حيث أن البنك المركزي السعودي يدرك دور تكنولوجيا المعلومات في هذه الأيام وبشكل أساسي في مختلف الأوساط المعتمدة على بياناتها مما يعّرض المؤسسات المالية المرخصة أخطار تكنولوجيا المعلومات بشكل مجدّد ومستمر ولمواجهة هذه المخاطر فقد استحدث البنك المركزي السعودي أطر حوكمة تكنولوجيا المعلومات مما يتيح للمرخصين تحديد ومعالجة المخاطر المتعلقة بتكنولوجيا المعلومات بفعالية.

حوكمة تكنولوجيا المعلومات والإدارة

- وجود هيكل حوكمة تكنولوجيا المعلومات محدد ومعتمد مما يمكّن ويعزّز الموارد المناسبة
- تطابق استراتيجية تكنولوجيا المعلومات مع الأهداف الاستراتيجية ومع المتطلبات القانونية والتنظيمية
- وجود بنية للمؤسسة تستعرض العمليات والبيانات ومستويات الدعم التكنولوجي لها
- وضع أهداف لتكنولوجيا المعلومات محددة ومفهومة لأصحاب المصلحة المعنيين
- تحديد أدوار ومسؤوليات
- تحديد اللوائح الملائمة والإبلاغ عنها والإمتثال بها
- وجود عمليات التدقيق الداخلي لتكنولوجيا المعلومات للتحقق من تنفيذ ضوابط تكنولوجيا المعلومات وسير عمالها مما يجب.
- وجود موظفين لديهم المهارات والمعرفة المطلوبة
- وجود عمليات وخدمات تكنولوجيا المعلومات فعّالة وذات كفاءة وتقاس باستمرار من خلال مؤشرات الأداء

إدارة مخاطر تكنولوجيا المعلومات

- وضع عمليات إدارة مخاطر تكنولوجيا المعلومات واعتمادها وتنفيذها والإبلاغ عنها وتكون موائمة مع عمليات إدارة المخاطر المؤسسية
- وجود أصول محددة ومسجلة ومحفوظة
- تحليل الضوابط والمخاطر بناءً على احتمالية حدوثها وتقييم آثارها المحتملة
- معالجة مخاطر تكنولوجيا المعلومات المرتبطة بأصول تكنولوجيا المعلومات على اساس معايير عملية
- معالجة مخاطر تكنولوجيا المعلومات وفقاً لخطط محددة ومن خلال مراجعتها ومراقبتها

إدارة العمليات

- توفير سجل دقيق من عملية إدارة الأصول
- تحديد وإدارة ترابطات الأصول الهامة
- وجود شروط وأحكام تعاقدية لضبط أدوار المدراء والعلاقات والالتزامات ومسؤوليات أصحاب المصلحة
- دعم العمليات.
- وجود توقعات للأداء المستقبلي ومتطلبات الكفاءة
- حماية معدات وسائل تكنولوجيا المعلومات من التلف والوصول الغير المصرح به
- قيام إدارة حوادث تكنولوجيا المعلومات وضوابط بنية الشبكة من الوصول غير المصرح به
- تحديد عملية إدارة حوادث تكنولوجيا المعلومات بتحديد الحوادث والإستجابة لها ومعالجتها وأيضاً عن حوادث مماثلة إلى مؤسسة البنك المركزي السعودي
- تحديد اجراءات رفع التقارير عن المشكلات للحد من أثرها
- تحديد وإعتماد وتنفيذ استراتيجية إدارة حفظ البيانات الاحتياطية
- وجود عملية لإنشاء وتوزيع وتخزين واستخدام وسحب الصور الافتراضية المحددة والمدارة

إدارة تغيير النظام

- ضمانة عملية إدارة التغيير تصنيف تغييرات الأصول واختبارها والموافقة عليها قبل تطبيقها
- تعريف وتوثيق والموافقة على التغييرات في أصول المعلومات من قبل المالك قبل التنفيذ
- ضمانة عملية الشراء على تقييم مخاطر اقتناء النظام وتقدّم الخدمة على نحو كاف
- ضمان الصرامة والضبط في منهج تطير النظام
- يتم اختبار تغييرات نظام المعلومات في بيئة مخضضة للتجربة وذلك لضمان تلبية متطلبات العمل، وأيضاً لتحديد العيوب/نقاط الضعف قبل اصدارها في بيئة الإنتاج
- تحديد متطلبات الأمن السيبراني وإختبارها في بيئة مخصصة للتجربة المعنية لتحديد الثغرات الأمنية والحدّ منها قبل عملية إصدارها في بيئة الإنتاج
- ضبط عملية إدارة التغيير بشكل صارم لتغييرات النظام
- معالجة عملية إدارة إعداد النظام على معلومات موثوقة/دقيقة حول عناصر الإعداد
- ضبط عملية إدارة لتصحيح آخر التحديثات القابلة للتطبيق وذات العلاقة
- ايجاد عملية لادارة مشروع تكنولوجيا المعلومات والمخاطر ذات العلاقة طوال دورة حياة المشروع.

منهجيتنا لتقييم حوكمة تكنولوجيا المعلومات:

يمكن لفريقنا الرائد في السوق - ذوي الخبرة الواسعة في حوكمة تكنولوجيا المعلومات - بتقييم اكتمال إطار حوكمة تكنولوجيا المعلومات بناءً على اطار المطلوب من قبل البنك المركزي السعودي.

للاتصال بنا:

سرسكانت رانجناثان
رئيس القسم
srikant.ranganathan@keypoint.com
+966 50 063 8273

توم جيلبرت
عضو إداري معاون
tom.gilbert@keypoint.com
+966 53 250 9866

دارشان مانوكولوسوريا
مدير أول
darrshan.m@keypoint.com
+966 55 395 1254

محمد نعمان تشيشتي
مساعد مدير
nauman.chishti@keypoint.com
+966 13 845 9237