**الجمهورية التونسية**

**-\*-**

**وزارة أملاك الدولة والشؤون العقارية**

**الكتابة العامّـــة**

**الإدارة العامّة لتكنولوجيا المعلومات والإدارة الالكترونية**

**كراس الشروط الإداريّة والفنيّة**

**استشارة عدد 33 لسنة 2022**

**للقيام بمهمة تدقيق في مجال السلامة المعلوماتية**

**وإنجاز سياسة أمن نظم المعلومات**

**آخر أجل لقبول العروض: يوم الثلاثاء 17 جانفي 2023**

***ديسمبر 2022***

# الفصل 1 : موضوع الاستشارة

تتكون الاستشارة من قسطين

* **القسط عدد01**  **لإنجاز مهمة تدقيق لهياكل وزارة أملاك الدولة و الشؤون العقارية** :

تعتزم وزارة أملاك الدولة والشؤون العقاريّــة إجراء استشارة لدى شركات الخدمات والهندسة الإعلامية للقيام بمهمة تدقيق لهياكلها في مجال السلامة المعلوماتية وذلك وفقا للخاصيّات الفنيّة المحددة بكرّاس الشروط الفنيّة ومقتضيات هذا الكرّاس وللتشريع الجاري به العمل وخاصة الأمر عدد 1250 لسنة 2004 المؤرخ في 25 ماي 2004 المتعلق بضبط النظم المعلوماتية وشبكات الهياكل الخاضعة إلى تدقيق إجباري دوري للسلامة المعلوماتية والمعايير المتعلقة بطبيعة التدقيق ودوريته وإجراءات متابعة تطبيق التوصيات الواردة في تقرير التدقيق

* **القسط عدد 02 إعداد خطة استمرارية نشاط و سياسة أمن المعلومات:**
* تعتزم وزارة أملاك الدولة والشؤون العقاريّــة إجراء استشارة لدى شركات الخدمات والهندسة الإعلامية لصياغة ووضع خطة إستمرارية الأعمال Plan de continuité d’activité PCA)). وفقاً للمعايير ISO 22301 .
* إنجاز سياسة الأمن لتكنولوجيا المعلومات (Politique de sécurité de système d’information PSSI) وفقا لأساس معايير ISO 27001: 2013 و 27005: 2018.

# الفصل 2: المسؤولية وسرية المعطيات والبيانات

يلتزم صاحب الصفقة بالمحافظة على سرية البيانات والمعطيات التي قد يحصل الإطلاع عليها من قبل الأعوان الراجعين له بالنظر سواء عن طريق أوعية ورقية أو إلكترونية أو مشافهة، ويتحمل مسؤولية كل إفشاء أو استغلال لتلك المعطيات.

كما يلتزم أثناء أعمال التدقيق بحفظ الوثائق وعدم الإلقاء بها في أماكن غير محمية ويتعهد بمجرد انتهاء الأعمال إما بإعدام الوثائق المستعملة أو بحفظها في مكان على درجة عالية من الحماية.

# الفصل 3: المناولة

لا يمكن لصاحب الصفقة أن يفوّت في كامل الصفقة أو في جزء منها إلى طرف آخر أو أن يلتجئ إلى طريقة المناولة ما لم يتحصّل مسبقا على موافقة كتابيّة من وزارة أملاك الدولة والشؤون العقارية.

إذا قبلت الإدارة طريقة المناولة يعتبر صاحب الصفقة المسؤول الأصلي والوحيد عن إنجاز الصفقة وإعلام المناول بالمعطيات الضروريّة لتنفيذ طلبات الإدارة.

# الفصل 4 : شروط المشاركة في الاستشارة

يمكن أن يشارك في الاستشارة بالنسبة **للقسط الأول** كل شركات الخدمات والهندسة الإعلامية التي لها تجربة في ميدان التدقيق في مجال السلامة المعلوماتية والمصرّح لهم بإجراء عمليات تدقيق لأمن تكنولوجيا المعلومات وفقًا للقانون 2004-05 والأمر الصادر عن وزير تقنيات الاتصال والاقتصاد الرقمي ووزير التنمية والاستثمار والتعاون الدولي. بتاريخ 01 أكتوبر 2019 المتعلق بضبط كراس شروط ممارسة نشاط التدقيق في مجال السلامة المعلوماتية والتي تلتزم بتوفير الضمانات المطلوبة لتأمين تنفيذ هذه الاستشارة وفقا للتشريع الجاري به العمل وكرّاس الشّروط الإداريّة والفنيّة الخاصّة.

كما يتعين أن تكون مهمة التدقيق تحت إشراف خبير تدقيق في مجال السلامة المعلوماتية مرخص له من طرف الوكالة الوطنية للسلامة المعلوماتية.

كما يتعين أن تكون مهمة التدقيق تحت إشراف خبير تدقيق في مجال السلامة المعلوماتية مرخص له من طرف الوكالة الوطنية للسلامة المعلوماتية

يمكن أن يشارك في الاستشارة بالنسبة **للقسط الثاني** كل شركات الخدمات والهندسة الإعلامية التي لها تجربة في مجال السلامة المعلوماتية والتي تلتزم بتوفير الضمانات المطلوبة لتأمين تنفيذ هذه الاستشارة وفقا للتشريع الجاري به العمل وكرّاس الشّروط الإداريّة والفنيّة الخاصّة.

* يلتزم المشارك في الاستشارة بتحمل جميع المتطلبات اللازمة لإنجازها.
* يمكن المشاركة في أحد الأقساط المطلوبة أو جميعها وإسناد المزود قسط واحد أو أكثر.
* **لا يمكن للمزود أن يقدم أكثر من عرض واحد بعنوان كل قسط**.

# الفصل 5: كيفية تقديم العروض وتضمينها

للمشاركة في الاستشارة يجب على المشارك أن يوجه عرضه عن طريق البريد مضمون الوصول أو البريد السريع أو يسلّمه مباشرة إلى مكتب الضبط المركزي للوزارة مقابل وصل إيداع في أجل أقصاه **يوم الثلاثاء 17 جانفي 2023** بدخول الغاية**.**

- تقصى العروض الواردة أو المسلّمة بعد آخر أجل لتقديم العروض ويعتمد ختم مكتب الضبط المركزي لتحديد تاريخ الوصول.

- لا يمكن لأي عارض أن يسحب عرضه بعد إيداعه أو أن يدخل عليه أية تغييرات وإلاّ اعتبر هذا العرض لاغيا.

يتكوّن العرض من:

- عرض فني

- عرض مالي

ترسل العروض طبقا لما يلي:

ظرف خارجي مغلق ومختوم ويحمل عبارة: **"لا يفتح استشارة عدد 33 لسنة 2022 للقيام بمهمة التدقيق في مجال السلامة المعلوماتية "** ويرسل على العنوان التالي:

**وزارة أملاك الدولة والشؤون العقاريّة**

**الكتابة العامّـــة**

**الإدارة العامّة لتكنولوجيا المعلومات والإدارة الالكترونية**

**عمارة الوطن شارع محمد الخامس – 1080 – تونس**

**" استشارة عدد 33 لسنة 2022 للقيام بمهمة التدقيق في مجال السلامة المعلوماتية وإنجاز سياسة أمن نظم المعلومات"**

ويحتوي هذا الظرف الخارجي على ظرفين داخليين منفصلين ومختومين واحد للعرض الفني وواحد للعرض المالي، كما يحتوي إضافة إلى ذلك على الوثائق الإدارية التالية:

1. نسخة من شهادة الانخراط في نظام للضمان الاجتماعي،
2. نظير من السجل التجاري ساري المفعول (النسخة المجردة غير مقبولة)،
3. تصريح على الشرف يقدمه العارضون يلتزمون بموجبه بعدم القيام مباشرة أو بواسطة الغير بتقديم وعود أو عطايا أو هدايا قصد التأثير في مختلف إجراءات إبرام الاستشارة ومراحل إنجازها طبقا للأنموذج الملحق بكراس الشروط،
4. تصريح على الشرف يقدّمه المشارك بأنّه لم يكن عونا عموميا لدى وزارة أملاك الدولة والشؤون العقارية أو مضى على انقطاعه عن العمل بها مدّة خمس سنوات على الأقل طبقا للأنموذج الملحق بكرّاس الشروط،
5. بطاقة إرشادات عامة حول المشارك ممضاة ومختومة طبقا للأنموذج الملحق بكراس الشروط،
6. التزام بسرية البيانات Engagement sur la confidentialité des données التعهد بإتلاف جميع المعطيات الحية والمخزنة بعد الانتهاء من الاشغال (َAnnexe 8)
7. كراس الشروط الإدارية والفنية الخاصة مختوم ومؤشر عليه في جميع صفحاته،
8. ضمان وقتي صالح لمدة (90) يوما ابتداء من اليوم الموالي للتاريخ الأقصى المحدد لقبول العروض تكون قيمته:

**400 دت بالنسبة للقسط الأول**

1. ضمان وقتي صالح لمدة (90) يوما ابتداء من اليوم الموالي للتاريخ الأقصى المحدد لقبول العروض تكون قيمته: **150دت بالنسبة للقسط الثاني**

**\* ملاحظات هامّة 1:**

**1-** كل تصريح أو التزام يقدّمه العارض يجب أن يكون مطابقا للنماذج المطلوبة من طرف الإدارة والمبيّنة بالملاحق المصاحبة.

**2**- تقصى آليّا العروض التي لم تتضمّن وثيقة الضمان الوقتي.

**3**- يقصى عرض كلّ مشارك لم يستوفي الوثائق الإدارية المطلوبة أو لم يقم بتسوية وضعية عرضه في الأجل الذي قد تحدّده له لجنة فتح الظروف.

**4**- يتعيّن على كل ّمشارك يرغب في الحصول على توضيحات تتعلق بكراس الشروط الحالي تقديم ملاحظاته واستفساراته كتابيّا للإدارة في أجل لا يتجاوز 10 أيام من تاريخ الإعلان عن الاستشارة وتلتزم وزارة أملاك الدولة والشؤون العقارية بالإجابة على الملاحظات والاستفسارات المطلوبة وتعميمها على بقية المشاركين.

إضافة إلى الوثائق الإدارية والضمان الوقتي يحتوي العرض على:

**1/ الظرف الداخلي الأول- يحمل عبارة العرض الفني واسم المزود وختمه ويحتوي على الوثائق التالية:**

* نسخة من شهادة إيداع كراس شروط لممارسة نشاط التدقيق في مجال السلامة المعلوماتية صالحة بتاريخ الأقصى لقبول العروض **بالنسبة للقسط عدد01**
* عرض مقتضب للنشاط العام وتنظيم المؤسسة المشاركة وخبرتها في الميدان،
* جداول الجذاذات الفنية معمرة ممضاة ومختومة (Formulaires de réponses َAnnexe 1 )
* السيرة الذاتية مدعومة بالوثائق المثبتة للفريق التدقيق المقترح (Annexe 2)
* عرض لأهم مراجع المشارك في المجال (Annexe 3)
* قائمة للفريق المتدخل (Annexe 4)
* المنهجية المقترحة لعملية التدقيق التنظيمي والهيكلي والفني (Annexe 5) **بالنسبة للقسط عدد01**
* الروزنامة العامّة للإنجاز مع توضيح مفصّل لجميع مراحله (Annexe 6)
* عرض للآليات الفنية المستعملة للقيام بعملية التدقيق (Annexe 7**) بالنسبة للقسط عدد01**

تكون جميع الصفحات للوثائق الفنية المطلوبة مؤرخة، ممضاة ومختومة من طرف المشارك.

/2الظرف الداخلي "ب" العرض المالي:

* وثيقة التعهد تحمل إمضاء وختم المشارك والتاريخ وبه كل البيانات المطلوبة وفقا للملحق المصاحب.
* الجدول التفصيلي للأسعار والمصاحب لهذه الاستشارة يكون وجوبا ممضى وعليه التاريخ وختم المشارك مع ضرورة الالتزام بالأنموذج للملحق المصاحب لكراس الشروط.

# الفصل 6 : محتوى الأثمان وطبيعتها

تشتمل الأسعار على كل الضرائب و الاداءات. كما تعدّ الأسعار ثابتة وغير قابلة للمراجعة أو التغيير. تكون الأسعار فردية و مفصلة طبقا لجدول الأثمان ( انظر إلى الملاحق)

يجب أن تكون الأثمان متضمنة لكل مصاريف مهمة التدقيق والمرافقة اللاحقة لها وكل الأعمال الأخرى الضرورية لتحقيق الالتزامات المحمولة على العارض.

في صورة اختلاف الثمن بالأرقام مع الثمن المنصوص عليه بلسان القلم يعتمد هذا الأخير.

# الفصل 7 : مدة صلوحية العروض

يبقى العارض ملزما بعرضه مدة 90 يوما بداية من اليوم الموالي لآخر اجل لقبول العروض ويمكن التمديد في الأجل المذكور أن اقتضى الأمر.

# الفصل 8: فتح الظروف

تتولى لجنة الشراءات ذات النظر فتح الظروف الفنية والمالية للاستشارة وإحالة العروض المستوفية للوثائق المطلوبة للفرز المالي والفني.

# الفصل 9: منهجيّة فرز العروض

تتولى لجنة الشراءات تقييم العروض على مرحلتين:

1. **المرحلة الأولى:** التثبت من الوثائق الإدارية والضمان الوقتي ومن صحة الوثائق المكونة للعرض المالي كما تتولى تصحيح الأخطاء الحسابية والمادية عند الاقتضاء ثم تقوم بترتيب العروض المالية خالية من الأداءات تصاعديا من الأقل ثمنا إلى الأعلى ثمنا بعنوان كل قسط.
2. **المرحلة الثانية:** تقوم اللجنة بالتثبت من العرض الفني المقدم من قبل صاحب العرض المالي الأقل ثمنا بعنوان كل قسط ، وتقترح إسناده الاستشارة (**القسط**) في صورة مطابقته لمقتضيات كراس الشروط.

إذا تبين أن العرض الفني المعني غير مطابق لكراس الشروط يتم اعتماد نفس التمشي مع العرض الموالي حسب الترتيب التصاعدي بعنوان كل قسط.

**الفصل 10: الإعـلام بإسناد الصفقة**

يتمّ إشعار صاحب العرض المقبول بإسناد الصفقة **بمقتضى إذن إداري أو من تسلمه الإذن بالتزود** وذلك قبل نهاية آخر أجل لصلوحية العروض. وحالما يقدّم صاحب الصفقة لوزارة أملاك الدولة والشؤون العقارية الضمان البنكي النهائي طبقا للفصل 13 من كرّاس الشّروط يقع إعلام العارضين الآخرين بعدم قبول عروضهم ويتمّ تسريح الضمانات البنكية الوقتية.

# الفصل 11: مدة انجاز

1. **القسط عدد 01 :** لا يمكن أن تتجاوز مدة الإنجاز المقترحة **45 يوم عمل.**
2. **القسط عدد 02** : لا يمكن أن تتجاوز مدة الإنجاز المقترحة **30 يوم عمل**.

آجال التنفيذ يجب أن تكون مطابقة للمدة الواردة بالروزنامة المقترحة ما لم يتم الاتفاق بين الطرفين قبل الانطلاق في انجاز المهمة موضوع الاستشارة.

لا يتم احتساب آجال المصادقة من طرف الإدارة والوكالة الوطنية للسلامة المعلوماتية في آجال التنفيذ.

# الفصل 12 : الإستلام

يتم التصريح بالاستلام بالنسبة :

* **القسط الأول :** يتم التصريح بالاستلام على مرحلتين و الذي يجب أن يتبع نموذج تقرير التدقيق الذي أصدرته الوكالة الوطنية للسلامة المعلوماتية ANSI " https://www.ansi.tn/sites/default/files/Modele rapport V1.4.pdf "
  + المرحلة الأولى : يصرح بانتهاء المرحلة الأولى بمجرد تسلم الإدارة لتقرير مبدئي لمهمة التدقيق للهياكل ممضى ومختوم ومتضمن على الأقل للعناصر المبوبة بالفصل الرابع من كراس الشروط الفنية في أجل أقصاه ثلاثون (45 ) يوما من تاريخ تسلم صاحب الصفقة للإذن الإداري أو إذن بالتزود.

وعلى الإدارة إبداء ملاحظاتها في التقرير المبدئي في أجل أقصاه عشرة (10) يوم عمل من تاريخ تسلمها للتقرير ويعد سكوتها أو إحالتها للتقرير بعد انقضاء الأجل المذكور مصادقة ضمنية على محتوى التقرير.

على صاحب الصفقة الاستجابة لجميع الملاحظات والاستفسارات المبداة من قبل الإدارة في أجل أقصاه عشرة (10) أيام عمل من تاريخ توصله بها.

يتم تحرير محضر في المصادقة على التقرير المبدئي قبول هذه المرحلة يمضى من قبل الإدارة وصاحب الصفقة ويعتبر تاريخ قبول هذه المرحلة تاريخ انطلاق المرحلة الثانية.

* + المرحلة الثانية: يصرح بانتهاء المرحلة الثانية بمجرد تسلم الإدارة لتقرير نهائي لمهمة التدقيق للهياكل متضمن للإجابات والتحفظات المثارة من قبل الإدارة و تقرير ملخص و تأليفي و تقرير يتضمن توصيات و خطة عمل لمدة ثلاث سنوات.

وعلى الإدارة إبداء ملاحظاتها في التقرير النهائي في أجل أقصاه عشرة (10) يوم عمل من تاريخ تسلمها للتقرير ويعد سكوتها أو إحالتها للتقرير بعد انقضاء الأجل المذكور مصادقة ضمنية على محتوى التقرير.

وعلى صاحب الصفقة الاستجابة لجميع الملاحظات والاستفسارات المبداة من قبل الإدارة في أجل أقصاه عشرة (10) أيام عمل من تاريخ توصله بها.

ويتم تحرير محضر استلام في الغرض يمضى من قبل الإدارة وصاحب الصفقة.

* **القسط الثاني :** يتم التصريح بالاستلام بمجرد تسلم الإدارة لتقارير الخاصة بخطة استمرارية الأعمال PCA وسياسة أمن نظام معلومات PSSI ممضى ومختوم ومتضمن على الأقل للعناصر المبوبة بالفصل الرابع من كراس الشروط الفنية في أجل أقصاه ثلاثون (30 ) يوما من تاريخ تسلم صاحب الصفقة للإذن الإداري أو إذن بالتزود.

وعلى الإدارة إبداء ملاحظاتها في التقارير في أجل أقصاه عشرة (10) يوم عمل من تاريخ تسلمها للتقارير ويعد سكوتها أو إحالتها للتقارير بعد انقضاء الأجل المذكور مصادقة ضمنية على محتوى التقرير.

على صاحب الصفقة الاستجابة لجميع الملاحظات والاستفسارات المبداة من قبل الإدارة في أجل أقصاه عشرة (10) أيام عمل من تاريخ توصله بها.

وبمجرد تسلم الإدارة لتقارير النهائية المتضمنة للإجابات والتحفظات المثارة يتم تحرير محضر استلام في الغرض يمضى من قبل الإدارة وصاحب الصفقة.

**وفي كل الحالات لا تتجاوز مدة الانجاز المدة المذكورة بالفصل 11 بعنوان كل قسط**

ويمكن للإدارة الالتجاء للتحكيم بواسطة الوكالة التونسية للسلامة المعلوماتية في صورة نشوب خلاف بينها وبين صاحب الصفقة بخصوص الملاحظات والاستفسارات المبداة من قبلها سواء بعنوان المرحلة الأولى أو الثانية .

ويفسخ عقد الصفقة او الغاء الاذن بالتزود في صورة عدم احترام صاحب الصفقة لقرار اللجنة المذكورة وذلك بقطع النظر عن كل الإجراءات القانونية الأخرى التي يمكن للإدارة اتخاذها لجبر الضرر الحاصل لها.

# الفصل 13: الضمانات

**1- الضمان الوقتي**

يرجع الضمان الوقتي للعارضين الذين لم يقع قبول عروضهم بعد اختيار صاحب الصفقة على أن لا يتمّ إرجاع الضمان الوقتي المقدّم من هذا الأخير إلاّ بعد تقديمه لضمـان نهـائي يقدّر بـ 3 % من قيمة الصفقة (بعنوان كل قسط).

يمكن حجز الضمان الوقتي وتفعيله في الحالات التاليّة :

* عندما يطلب العارض سحب عرضه أثناء فترة صلوحيته المنصوص عليها بهذا الكراس بما في ذلك فترة التمديد فيها إن اقتضى الأمر ذلك.
* عندما يمتنع العارض المسندة إليه الصفقة عن تقديم الضمان النهائي.

ولا تحول عملية الحجز هذه دون تتبع الإدارة للعارض المتخلي لجبر الضرر الحاصل لها.

**2- الضمان النهائي**

يجب على صاحب الصّفقة تقديم الضمان النهائي بمبلغ قدره 3% من القيمة الجمليّة للصفقة (بعنوان كل قسط) وذلك في ظرف عشرون يوما (20) من تاريخ إشعاره بإسناده الصفقة على أقصى تقدير.

يتم إرجاع الضمان النهائي لصاحب الصفقة في أجل أقصاه شهر من تاريخ الإمضاء على محضر الاستلام الوقتي للإستشارة بعنوان كل قسط وفي صورة عدم احترام صاحب الصفقة للالتزامات المحمولة عليه لا يتم إرجاع الضمان النهائي أو لا يوضع حد لالتزام الكفيل بالتضامن إلا برسالة رفع اليد يسلمها المشتري العمومي بقطع النظر عن كل الإجراءات القانونية الأخرى التي يمكن للإدارة اتخاذها لجبر الضرر الحاصل لها .

# الفصل 14: مهمة استطلاع

يمكن للمشاركين قصد إعداد عروضهم القيام باستطلاع لدى الهياكل المعنية بالتدقيق بعد تقديم طلب كتابي او مراسلة الكترونية وبعد بالتنسيق مع مصالح الإدارة العامة لتكنولوجيا المعلومات والإدارة الالكترونية لدى وزارة أملاك الدولة والشؤون العقارية.

# الفصل 15: خلاص الاستشارة

يتمّ الخلاص عبر تحويل بنكي او بريدي في الحساب الجاري للمزود وذلك بعد الاستظهار بـ :

* فاتورة في 5 نظائر
* شهادة توقيف حساب من الصندوق الوطني للضمان الاجتماعي سارية المفعول.
* الأصل من الإذن الإداري او الإذن بالتزود.

# الفصل 16 : غرامة التأخير

في صورة عدم احترام صاحب الصفقة للآجال المحدّدة بالفصلين 11 و 12 تطبّق غرامة التأخير على النحو التالي :

**(** قيمة العرض بالنسبة للقسط ) x عدد أيّام التأخير

غرامة التأخير = \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1000

ولا يمكن أن تتعدى غرامة التأخير 5% من مجموع قيمة القسط بعنوان غرامة التأخير.

يتم خصم مبلغ غرامة التأخير دون التنبيه المسبق على صاحب الصفقة ولا يحول تطبيقها دون المطالبة بغرامة لجبر الضرر الناتج عن هذا التأخير وعن الإخلال بالالتزامات التعاقدية.

# الفصل 17: مصاريف التسجيل

تحمل مصاريف التسجيل الطابع الجبائي على صاحب الصفقة .

# الفصل 18: أحكام عامّة

بالنسبة للمقتضيات التي لم تذكر بكراس الشروط يتمّ الرجوع إلى الأمر عدد 1039 لسنة 2014 المؤرخ في 13 مارس 2014 المتعلق بتنظيم الصفقات العمومية وجميع النصوص المنقحة والمتممة له وإلى كراس الشروط الإدارية العامة المتعلق بالتزوّد بمواد عادية وخدمات.

إني الممضي أسفله أقرّ بأني أطلعت على جميع الأحكام والشروط الواردة بهذا الكراس وألتزم بمقتضاها.

...................في ......................

**الإمضاء و الختم**

**كراس الشروط الفنيّة**

**استشارة عدد 33 لسنة 2022**

**للقيام بمهمة التدقيق في مجال السلامة المعلوماتية**

**وإنجاز سياسة أمن نظم المعلومات**

# Article 1 : Objet de la consultation

La mission objet de cette consultation concerne deux lots :

* **Lot 1** **audit de la sécurité du système d’information :**

La mission d’audit de la sécurité du système d’information au niveau des structures décrites dans l’Article 8 du ministère des domaines de l’état et des affaires foncières.

L’objet de cet audit devra se conformer, au minimum, aux dispositions énoncées dans le décret N°2004-1250 du 25 mai 2004 et être réalisé par un expert auditeur, personne physique ou morale, habilités à exercer l’audit de la sécurité informatique conformément à la loi 2004-05 et à l’arrêté du ministre des technologies de la communication et de l'économie numérique et du ministre du développement, de l’investissement et de la coopération internationale du 01 Octobre 2019, fixant le cahier des charges relatif à l'exercice de l’activité d’audit dans le domaine de la sécurité informatique.

Cet audit devra suivre une approche méthodologique conforme au [référentiel établi par l’ANSI](https://www.ansi.tn/sites/default/files/Referentiel_Audit%202.1_0.pdf) qui couvre les aspects organisationnels, physiques et opérationnels relatifs à la sécurité du système d’information inclus dans le périmètre de cet audit.

Cet audit devra prendre comme référentiel de base la norme ISO/IEC 27002 et suivre une approche méthodologique aussi proche que possible de ce référentiel.

La mission d’audit devra ainsi concerner les aspects organisationnels, physiques et techniques relatives à la sécurité du système d’information inclus dans le périmètre de cet audit.

* **Lot 2 Elaboration d’un plan de continuité des activité PCA et politique de sécurité Informatique (PSI):**
  + L’élaboration d’un Plan de Continuité des Activités (PCA) selon la norme ISO 22301 et conformément aux prescriptions de ce cahier des charges
  + L’élaboration d’une politique de sécurité de système d’information PSI

# Article 2 :LOT 1 Conduite et déroulement de la mission d’audit des systèmes d’information:

Décomposé en trois phases. Les phases numérotées de I jusqu’à III sont listées selon les conseils relatifs à la planification et à la réalisation des activités d’audit donnés dans la norme ISO 19011.

## Déclenchement de l’audit :

Au lancement de l’audit, le titulaire devra solliciter auprès des structures à auditer tout détail, information ou document nécessaire pour l’exercice de sa mission, entre autres la fourniture des rapports résultants du dernier audit réalisé.

Une réunion préparatoire de la mission sera organisée au début de la mission, dont l’objet sera de finaliser, sur la base des besoins et documents préparés par le titulaire, les détails de mise en œuvre de la mission.

Il concernera, sans s’y limiter, la finalisation des détails suivants :

* Désignation des chefs de projets et des interlocuteurs, côtés maîtres d’ouvrage le titulaire,
* Fourniture des détails complémentaires, relatifs au périmètre de l’audit (si le titulaire du marché fait recours à l’échantillonnage, il est tenu d’en présenter les critères pour chaque type d’objet de l’audit),
* Validation du périmètre de l’audit,
* Fourniture des documents requis pour l’audit (manuels d’exploitation, schémas d’architectures, politique de sécurité, …),
* Examen des détails des listes des interviews à réaliser par le titulaire et fourniture par le maître d’ouvrage de la liste nominative des personnes à interviewer,
* Affinement des plannings d’exécution (planning des actions par site, plannings des réunions de coordination et de synthèse, ….),
* Examen des détails logistiques nécessaires au déroulement de la mission (octroi des autorisations d’accès aux lieux où l’audit devra être élaboré sur la base d’études de terrain, octroi de locaux de travail au titulaire,…).

Ainsi tous les détails de mise en œuvre seront examinés et validés. Cette réunion débouchera, entre autres, sur la synthèse des plannings précis et détaillés de mise en œuvre de la mission.

Les résultats de cette réunion seront consignés dans un PV, qui sera annexé au rapport final d’audit.

En cas de difficultés notoires rencontrées lors de cette phase, le titulaire devra faire recours au Maître d’Ouvrage par écrit, pour lui permettre d’intervenir efficacement et dans les délais.

## Préparation des activités d’audit :

### Revue des documents:

Cette phase permettra de déterminer la conformité des documents existants aux exigences de la norme ISO/IEC 27002, d’arrêter la liste des documents manquants exigés par cette norme et d’examiner les problèmes éventuels relatifs à la mise à jour de la documentation.

Plus précisément, l’auditeur doit vérifier si :

* L’information contenue dans les documents fournis est :
* Complète (tout le contenu attendu figure dans le document),
* Correcte (le contenu est conforme à d'autres sources fiables telles que les normes et les règlements),
* Cohérente (le document est cohérent en soi et avec les documents associés),
* D’actualité (le contenu est à jour).
* Les documents en cours de revue couvrent le périmètre de l'audit et fournissent des informations suffisantes pour appuyer les objectifs de l’audit.

Aussi, est-il opportun d’examiner les documents relatifs à la mise en œuvre des recommandations émises dans le rapport de l’audit précédent ainsi que tout document issu d’autres audits éventuels.

Il convient d’accorder une attention particulière à cette phase compte tenu de l’importance que revêt la documentation dans le bon déroulement des activités de l’organisme indépendamment des personnes. Aussi faut-il tenir compte, durant cette phase, de la taille, de la nature et de la complexité de l’organisme.

## Conduite des activités d’audit :

C’est la phase d’audit proprement dite. Elle ne peut commencer qu’après l’achèvement de la revue des documents. Au fur et à mesure de l’avancement dans cette phase, l’auditeur doit vérifier la conformité des procédures opérationnelles avec celles figurant dans les documents fournis.

Ainsi, cette phase couvrira principalement trois (03) volets :

* Un volet d’audit organisationnel et physique,
* Un volet d’audit technique,
* Et un volet d’appréciation des risques.

### Audit organisationnel et physique:

Il s’agit, pour ce volet, d’évaluer les aspects organisationnels de gestion de la sécurité des structures objet de l’audit. Au cours de cette étape, le titulaire devra emprunter une approche méthodologique, basée sur des batteries de questionnaires pré-établis et adaptés à la réalité des entités auditées et aux résultats de la revue des documents. Cette approche permettra d’aboutir à une évaluation pragmatique des failles et des risques encourus et de déduire les recommandations adéquates pour la mise en place des mesures organisationnelles et d’une politique sécuritaire adéquate.

### Audit technique:

1. Objectifs de l’audit technique

Ce volet concerne l’audit technique de l’architecture de sécurité. Il s’agit de procéder à une analyse très fine de l’infrastructure sécuritaire des systèmes d’information. Cette analyse devra faire apparaître les failles et les risques conséquents d’intrusions actives (tentatives de fraude, accès et manipulation illicites de données, interception de données critiques…), ainsi que celles virales ou automatisées, et cette suite à divers tests de vulnérabilité conduits dans le cadre de cette mission. Ces tests doivent englober des opérations de simulation d’intrusions et tout autre test permettant d’apprécier la robustesse de la sécurité des systèmes d’information et leur capacité à préserver les aspects de confidentialité, d’intégrité, de disponibilité et d’autorisation.

Au cours de cette étape, le soumissionnaire devra, en réalisant des audits techniques de vulnérabilités, des tests et simulations d’attaques réelles :

* Dégager les écarts entre l’architecture réelle et celle décrite lors des entretiens ou dans la documentation, ainsi qu’entre les procédures techniques de sécurité supposées être appliquées (interviews) et celles réellement mises en œuvre.
* évaluer la vulnérabilité et la solidité des composantes matérielles et logicielles du système d’information ( réseau, systèmes, mécanismes d’administration et de gestion, plates-formes matérielles,...) contre toutes les formes de fraude et d’attaques connues par les spécialistes du domaine au moment où l’audit est conduit, et touchant les aspects de confidentialité, intégrité et disponibilité des informations (et le cas échéant, celles des mécanismes d’autorisation (authentification, certification, ..) et de non répudiation).
* évaluer l’herméticité des frontières du réseau contre les tentatives de son exploitation par des attaquants externes (sites d’amplification d’attaques, relais de spam, exploitation du PABX pour le détournement (« vol ») des lignes de communication, ….).

Il devra aussi inclure une évaluation des mécanismes et outils de sécurité présentement implémentés et diagnostiquer et tester toutes leurs failles architecturales et techniques, ainsi que les lacunes en matière d’administration et d’usage de leurs composantes logicielles et matérielles.

Les tests réalisés ne devront pas mettre en cause la continuité du service du système audité. Les tests critiques, pouvant provoquer des effets de bord, devront être notifiés au chef de projet (coté maître d’ouvrage). Ils devront, si nécessaire, être réalisés sous sa supervision conformément à un planning préalablement établi et validé et qui pourra concerner des horaires de pause et éventuellement de chôme.

1. Outils de l’audit technique

Lors des audits, l’utilisation d’outils commerciaux devra être accompagnée de la présentation d’une copie de la licence originale et nominative, permettant leur usage correct pour de telles missions (inexistence de restrictions quant à leur usage pour les audits : plages d’adresses ouvertes, ...).

De plus, étant donné qu'aucun produit commercial ne saurait prétendre à lui seul, à une complétude totale, les outils disponibles dans le domaine du logiciel libre (et généralement utilisés par les attaquants) devront être savamment déployés pour assurer une complétude correcte de cette phase, en s’appuyant, quand cela est possible, sur des scripts riches de mise en œuvre savante et combinée de ces outils.

Les outils proposés devront inclure, sans s’y limiter, les catégories d’outils suivants :

* outils de sondage et de reconnaissance du réseau,
* outils de test automatique de vulnérabilités du réseau,
* outils spécialisés dans l’audit des équipements réseau (routeurs, switchs, …),
* outils spécialisés dans l’audit de chaque type de plate-forme système (OS, ..) présente dans l’infrastructure,
* outils spécialisés dans l’audit des SGBD existants,
* outils de test de la solidité des objets d’authentification (fichiers de mots clés,…),
* outils d’analyse et d’interception de flux réseaux,
* outils de test de la solidité des outils de sécurité réseau (firewalls, IDS, outils d’authentification,….),
* outils de scan d’existence de connexions dial-up dangereuses (war-dialing),

et tout autre type d’outil, recensé nécessaire, relativement aux spécificités du système d’information audité (test d’infrastructure de PKI, ….).

Le soumissionnaire devra donner la référence et une description concise (résumé de la liste des fonctionnalités offertes) des outils et scripts qu’il compte utiliser, en spécifiant l’objectif, le lieu (phase de l’audit) et les types de fonctionnalités de l’outil ou script qui seront mises en œuvre (Voir modèle en annexe7).

### Appréciation des risques :

Dans ce volet et après avoir identifié les failles de sécurité organisationnelles, physiques et techniques, il s’agit de suivre une approche méthodologique pour évaluer les risques encourus et leurs impacts sur la sécurité de la structure auditée.

Le volet d’appréciation des risques se déroulera en deux étapes :

**Etape 1 : Analyse**

A cette étape le titulaire est amené à :

1. identifier les **processus critiques** : les informations **traitées**, les actifs matériels, les actifs logiciels, les personnels,…qui supportent ces processus,
2. identifier les **menaces** auxquelles sont confrontés ces actifs (intentionnelles ou non intentionnelles),
3. identifier les **vulnérabilités** (au niveau organisationnel, au niveau physique et au niveau technique) qui pourraient être exploitées par les menaces,
4. identifier les **impacts** que les pertes de confidentialité, d'intégrité et de disponibilité peuvent avoir sur les actifs,
5. évaluer la **probabilité** réaliste d'une défaillance de sécurité au vu des mesures actuellement mises en œuvre.

**Etape 2 : Evaluation**

A cette étape le titulaire est amené à :

1. établir une classification des risques par niveaux, et déterminer le niveau du risque acceptable,
2. évaluer les risques, en fonction des facteurs identifiés dans la phase d’analyse, et les classifier par niveaux,
3. identifier les mesures préventives et les mesures correctives de sécurité à implémenter pour éliminer ou réduire les risques identifiés.

## Préparation du rapport d’audit :

Le titulaire est invité, à la fin de la phase d’audit sur terrain, à remettre au commanditaire de l’audit un rapport daté, signé par le responsable de l’audit et portant le cachet du titulaire. Ce rapport doit contenir une synthèse permettant l’établissement de la liste des failles (classées par ordre de gravité et d’impact), ainsi qu’une évaluation de leurs risques et une synthèse des recommandations conséquentes.

Les recommandations devront inclure au minimum :

1. les actions détaillées (organisationnelles et techniques) urgentes à mettre en œuvre dans l’immédiat, pour parer aux défaillances les plus graves, ainsi que la proposition de la mise à jour ou de l’élaboration de la politique de sécurité à instaurer,
2. les actions organisationnelles, physiques et techniques à mettre en œuvre sur le court terme (jusqu’à la date du prochain audit), englobant entre autres :
   * les premières actions et mesures à entreprendre en vue d’assurer la sécurisation de l’ensemble du système d’information audité, aussi bien sur le plan physique que sur le plan organisationnel (structures et postes à créer, opérations de sensibilisation et de formation à intenter, procédures d’exploitation sécurisées à instaurer,…) et technique (outils et mécanismes de sécurité à mettre en œuvre), ainsi qu’éventuellement des aménagements architecturaux de la solution de sécurité existante,
   * une estimation des formations requises et des ressources humaines et financières supplémentaires nécessitées.
3. la proposition d’un plan d’action cadre s’étalant sur trois années et présentant un planning des mesures stratégiques en matière de sécurité à entreprendre, et d’une manière indicative les moyens humains et financiers à allouer pour réaliser cette stratégie.

## Méthodologie(s) adoptée(s)

Pour la réalisation de la mission, le soumissionnaire devra emprunter une approche méthodologique, en indiquant les références de la (ou des) méthodologie(s) adoptée(s), tout en respectant [le référentiel établi par l’ANSI](https://www.ansi.tn/sites/default/files/Referentiel_Audit%202.1_0.pdf) (**https://www.ansi.tn/sites/default/files/Referentiel\_Audit 2.1\_0.pdf**)

La (les) méthodologie(s) adoptée(s) devra(ont) être adaptée(s), dans sa (leur) mise en œuvre, à la réalité métier et à la taille des entités auditées et devra(ont) permettre d’aboutir à l’élaboration de bilans et de recommandations et des solutions pragmatiques et pertinentes, qui tiennent compte, pour les plus urgentes, de la réalité humaine et matérielle de l’entité, et en la corrélant à la gravité des failles décelées et à l’efficacité, l’urgence et la faisabilité des actions à mener.

Ainsi, le soumissionnaire est appelé à indiquer, clairement dans son offre, la (les) méthodologie(s) d’audit qu’il envisage de mettre en œuvre. Le Maître d’Ouvrage tiendra compte dans son évaluation de la consistance de la (des) méthodologie(s) proposée(s), ou parties de cette (ces) méthodologie(s) et ce à chaque phase ainsi que de son (leur) adéquation à la réalité de l’entreprise et du temps imparti.

Il devra aussi indiquer dans son offre la qualité des moyens techniques et humains qui seront déployés lors de la mise en œuvre de cette (ces) méthodologie(s) (expérience dans la mise en œuvre de la (des) méthodologie(s) consignée(s), outils logiciels accompagnant la mise en œuvre de cette (ces) méthodologie(s)).

Le soumissionnaire devra spécifier dans la rubrique « Démarche d’audit proposée », au minimum, et pour chaque composante du système d’information :

* le Type de méthodologie(s) à mettre en œuvre pour le volet physique et organisationnel et les structures recensées utiles à interviewer, ainsi que l’(es) outil(s) logiciel(s) accompagnant la mise en œuvre de cette (ces) méthodologie(s) (traitement automatisé des interviews et calcul des risques associés, …),
* la méthode de mise en œuvre du volet technique, en spécifiant les types de tests techniques à effectuer et leurs objectifs, ainsi que les outils utilisés,
* la séquence des actions à mener (interviews, tests techniques, synthèse, rédaction de rapports, …) et une estimation de la volumétrie homme/jour de chaque action, incluant un résumé des corrections de volumétrie proposées par rapport à l’estimation préliminaire proposée dans le cahier des charges
* la liste nominative des équipes qui interviendront pour chaque composante (site, structure) avec référence de l’expérience dans la mise en œuvre de la (des) méthodologie(s) et des outils consignés.

Il est à noter que toute modification des personnes initialement proposées est une cause de rupture du contrat ou de disqualification, sauf cas exceptionnel, via l’octroi de l’accord préalable et écrit du Maître d’Ouvrage (avec insertion de ces écrits dans le rapport final). De plus,le personnel en charge de l’audit devra être un personnel permanent du soumissionnaire. Pour autant, le soumissionnaire pourrait éventuellement faire intervenir du personnel consultant, sur la foi de présentation du contrat de consultation y afférant, qui devrait inclure une clause sur la confidentialité, tout en assumant totalement la responsabilité envers tout risque de divulgation par ce personnel de tout type de renseignements concernant cet audit.

# Article 3 : Lot 2 Conduite et déroulement de la mission Elaboration des plans de continuité des activités PCA et l’élaboration du Politique de sécurité de système d’information PSSI:

1. Elaboration des plans de continuité des activités PCA:

La mission d’élaboration du PCA devra être conforme aux recommandations de la norme ISO 22301 et il devra couvrir les orientations stratégiques de l’organisation.

## Conduite et déroulement de la mission

La mission devra démarrer par une réunion de préparation qui vise à assurer les conditions nécessaires au bon déroulement de la mission. Cette réunion doit couvrir les aspects suivants : planning des actions, planning des réunions de coordinations et de synthèse et intervenants...

Le PCA devra être conforme aux recommandations de la norme ISO 22301.

Cette mission se déroulera en sept (7) phases comme suit :

1. Etude de contexte,

2. Analyse des risques,

3. Analyse des impacts d'activité : Business Impact Analysis (BIA),

4. Développement de la stratégie de continuité du système d'information et des processus métiers les plus critiques

5. Mise en œuvre des plans de continuité d'activité,

6. Test et simulation du plan de continuité d'activité,

### Phase 1: étude de contexte

A cette phase le titulaire est amené à identifier les services et processus métier critiques de l’organisme /administration : les informations traitées, les actifs matériels, les actifs logiciels, les personnels qui supportent ces processus. De présenter une analyse détaillée des besoins de continuité des activités :

- La liste des activités et services critiques,

- L’environnement externe: partenaires et partie prenantes,

- Les objectifs de continuité,

- Les parties intéressées: citoyens, entreprises, clients,

- Les exigences réglementaires et contractuelles,

- Le périmètre ou domaine d’application:

* Organisationnel : représente les directions, services, filiales,
* Fonctionnel : les activités et/ou services concernés,
* Physique : emplacements physiques qui sont concernés par le PCA

### Phase 2 : Analyse des risques / Cartographie des risques

- Identification des risques perturbateurs,

- Analyse de ces risques,

- Evaluation de ces risques,

- Traitement de ces risques.

### Phase 3 : Analyse des impacts d'activité : Business Impact Analysis (BIA)

Il s’agit de mettre en place un processus d’évaluation formel et documenté des niveaux de dégradation supportable des activités permettant ainsi de déterminer les priorités, les objectifs et les cibles de continuité d’activité et de reprise, comprenant l’évaluation des impacts relatifs à un événement perturbateur sur la continuité d’activité en précisant :

- Les activités,

- Les priorités,

- Les délais par ordre de priorité de reprise des activités à un niveau minimum acceptable spécifié,

- Les mesures nécessaires pour augmenter la résilience des opérations critiques,

- Les ressources nécessaires pour la restauration à temps des opérations critiques.

### Phase 4 : Développement de la stratégie de continuité

Il s’agit de fournir les documents de stratégie de continuité à l’issue de l’analyse du risque et du BIA :

- La stratégie de continuité,

- Plans de continuité d’activité

- Les exigences concernant les ressources

### Phase 5 : Mise en œuvre des plans de continuité d’activité

Il s’agit de spécifier, documenter et mettre en œuvre les plans de continuité :

- Les procédures de continuité d’activité permettant de gérer les incidents perturbateurs,

- La structure de réponse à un incident perturbateur,

- Les procédures de communication avec les parties prenantes,

- Les procédures de reprise temporaires,

- Les procédures de surveillance, détection et communication des incidents,

- Les rapports (modèles) de test, évaluation, …

### Phase 6 : Test et simulation du plan de continuité d’activité

Il s’agit de :

- Préparer les exercices et les tests des procédures de continuité d’activité,

- Définir les indicateurs de performances KPI,

- Evaluer la conformité des plans de continuité par rapports aux exigences métiers, légales et réglementaires.

## Procédure de validation des rapports de la mission

A la fin de chaque étape, l‘organisme / administration donnera son avis quant à la consistance et la pertinence des rapports daté, signé par le responsable et portant le cachet du titulaire. Ce rapport doit contenir le plan de continuité d’activité PCA en regard de :

- La qualité de réalisation des objectifs assignés à la mission et fixés dans le Cahier des Clauses

Techniques,

- De l'adéquation de la méthodologie mise en œuvre par le titulaire lors de la réalisation de la mission avec celle consignée dans son offre.

- De la qualité des résultats (estimation des risques, ...) issus des travaux d'analyse des risques et de leurs complétudes.

## Méthodologie

Pour la réalisation de la mission, le soumissionnaire devra suivre une approche méthodologique, en Indiquant les références de la (ou des) méthodologie(s) adoptée(s), tout en gardant comme référentiel normatif les normes ISO 27001- ISO 22301- ISO 27005.

Le soumissionnaire doit spécifier sa méthodologie en indiquant :

- Les moyens techniques et humains,

- Le plan d'action et le plan de charges,

- La gestion du projet.

1. Elaboration du Politique de sécurité de système d’information PSSI:

Le soumissionnaire est tenu d’élaborer la politique de sécurité des systèmes information du ministère **PSSI** qui doit répondre à l’ensemble des enjeux, actions et procédure faisions partie de la stratégie du ministère, l’élaboration du politique de Sécurité Informatique (PSI) doit se baser sur la norme ISO 27001 :2013 et 27005 :2018.

## Conduite et déroulement de la mission

le projet de l’élaboration de la Politique de Sécurité de Informatique passe par les phases suivantes :

1. Initialisation de la mission

2. Définir le périmètre et les objectifs

3. Effectuer une étude de l’existant

4. Effectuer une analyse des risques informatiques

5. Formalisation du cadre et du plan d’intervention

6. Elaboration de la politique de sécurité.

7. Communiquer sur la politique de sécurité informatique

**Phase 1 : Initialisation de la mission**

Cette étape consiste à effectuer une ou plusieurs réunions de cadrage afin de :

* Valider la méthodologie du soumissionnaire et sa démarche.
* Identifier les acteurs impliqués ;
* Lister les résultats attendus et les livrables ;
* Elaborer un calendrier des phases et des différents livrables.
* Valider le budget alloué pour le projet
* Valider la méthodologie de validation des phases et des livrables

**Output de cette phase** : Une note de cadrage qui formalise les informations nécessaires pour cette phase.

**Phase 2 : Définir le périmètre, les objectifs et le contexte de l’organisme :**

Cette phase consiste à déterminer les axes stratégiques et les premières grandes orientations à partir desquelles sera déclinée la PSI. Pour cela, elle doit obligatoirement identifier et prendre en compte le périmètre d'étude et les domaines d’activités à couvrir, les missions du maître d’ouvrage, ses enjeux et orientations stratégiques, les obligations et engagements vis-à-vis de ses partenaires, ses clients et sous-traitants, ses aspects réglementaires, l'échelle de besoins et les besoins de sécurité des biens à protéger afin d’aboutir à une note de stratégie validée fixant les grandes orientations de la PSI.

Pour ce faire, le titulaire devra solliciter auprès de l’organisme tout détail, information ou document nécessaire pour l’exercice de sa mission.

Des réunions pourront ainsi avoir lieu afin de faciliter le déroulement de cette phase.

**Output de cette phase** : Une note de stratégie détaillant le périmètre, les objectifs et le contexte de l’organisme.

**Phase 3 : Effectuer une étude de l’existant**

Cette phase permet d’effectuer une analyse des écarts par rapport à la norme ISO 27002 : 2022. En effet, elle consiste à inventorier l’existant matériel et logiciel en matière de sécurité du système d’information et d’évaluer les écarts par rapport à l’ensemble des chapitres de la Norme ISO 27002: 2022.

**Output de cette phase** : Un document décrivant le registre matériel et logiciel du Maître d’Ouvrage

ainsi que les écarts constatés entre l’existant et les bonnes pratiques de la norme ISO 27002 : 2022.

**Phase 4 : Effectuer une appréciation des risques**

Cette étape concerne l’appréciation des risques et devra couvrir les aspects suivants :

* Classification des actifs informatiques.
* Identification et étude des risques pouvant nuire à la sécurité du système d’information (description des menaces, probabilité d’occurrence, ressources impactées,…).
* Identification des risques résiduels.
* Classement des risques selon leur criticité.
* Estimation de l’impact, la potentialité et la gravité des risques.
* Une évaluation et un plan de traitement des risques liés aux technologies Informatique et de communication, conformément à la norme ISO 27005 :2018.

**Output de cette phase** : Rapport incluant les résultats des différentes étapes de l’appréciation des risques ainsi qu’un plan de traitement des risques.

**Phase 5 : Formalisation du cadre et du plan d’intervention**

Cette phase consiste à élaborer le cadre complet d’intervention ainsi que la planification des phases suivantes. En effet, il s’agit de :

* Elaborer le plan de communication de la PSI ;
* Elaborer le plan de formation et sensibilisation de la PSI ;
* Raffiner le périmètre de l’intervention et les domaines à inclure ;
* Définir les principes de sécurité de la PSI à élaborer ;
* Instancier les principes de sécurité retenus en règles de sécurité selon les éléments contenus dans la note de cadrage et la note de stratégie de sécurité.

Chaque principe de sécurité retenu doit être décliné en une ou plusieurs règles de sécurité adaptées au contexte du périmètre de la PSI.

L’élaboration des règles de sécurité doit faire l’objet d’une argumentation systématique se basant sur les éléments stratégiques. Il est nécessaire de mettre en évidence les rapports coûts-bénéfices, en estimant les coûts de mise en œuvre des règles de sécurité, afin d'effectuer des choix cohérents avec les ressources de l'organisme.

**Output de cette phase** : Rapport de formalisation du cadre d’intervention qui comporte tous les éléments listés dans cette phase.

**Phase 6 : Elaboration de la politique de sécurité**

Cette phase comprend :

* L’élaboration de la liste des documents de la politique de sécurité Informatique.

Cette liste devra inclure au minimum la liste suivante :

* Politique de contrôle d’accès
* Politique de gestion des actifs
* Politique de conservation des données
* Politique de gestion des risques
* Politique de classification et de traitement des informations
* Politique de sensibilisation et de formation à la sécurité Informatique
* Politique d’utilisation acceptable des actifs
* Politique relative au bureau et à l’écran transparents
* Politique relative au travail mobile et au télétravail
* Politique de continuité des activités
* Politique de sauvegarde
* Politique relative aux logiciels malveillants et aux antivirus
* Politique de gestion des changements
* Politique de sécurité des fournisseurs tiers
* Politique d’amélioration continue
* Politique de journalisation et de surveillance
* Politique de gestion de la sécurité du réseau
* Politique de transfert d’informations
* Politique de développement sécurisé
* Politique de sécurité physique et environnementale
* Politique de gestion des clés cryptographiques
* Politique de contrôle cryptographique et de chiffrement
* Politique en matière de documents et d’enregistrements
* Etc
* Les chartes de sécurité et les guides de bonnes pratiques ;
* Les procédures de sécurité : telles que les procédures de gestion des mots de passe, gestion de sauvegarde (sauvegarde, restauration, conservation des médias, etc.), gestion d’autorisation d’accès, gestion des incidents, etc.
* Un plan d’action pour la mise en œuvre qui comprendra deux principaux volets : Des actions de type méthodologique, organisationnelle ou procédurale, applicable à l’ensemble de l’organisme participant au périmètre de l’étude et qui détermine les moyens nécessaires pour la réduction des risques et la prise en charge des incidents, qu’il s’agisse de moyens matériels ou humains (formation d’une équipe dédiée, mise en place de nouveaux logiciels, dispositifs, consultation d’experts…).
* L’estimation du budget et le planning de mise en œuvre.

La politique de sécurité du système d’information devra être conforme aux bonnes pratiques de la norme ISO 27002 : 2022 et couvrir tous les domaines de cette norme. Elle devra également respecter les règles de sécurité validés output de la phase précédente.

La PSI doit identifier clairement les rôles et les responsabilités au sein de l’organisme.

**Phase 7 : Communiquer sur la politique de sécurité informatique**

Cette phase devra couvrir les aspects suivants :

* Mise en œuvre des moyens de communication jugés pertinents qui serviront à la communication de la politique de sécurité et à la sensibilisation des utilisateurs du système d’information aux enjeux de la sécurité.
* Sensibilisation de l’ensemble du personnel portant sur la PSI et les procédures y afférant.

## Procédure de validation des livrables des phases

A la fin de chaque phase, le comité de pilotage du projet donnera son avis quant à la consistance et

la pertinence des livrables, en regard de :

* La qualité de réalisation des objectifs assignés à la mission et fixés dans le Cahier des Clauses Techniques.
* La qualité des résultats issus des travaux de la phase « **Effectuer une analyse des risques informatique**»
* La qualité des documents de la PSI, de leur adéquation au contexte de l’organisme, et du degré de leur applicabilité.
* La qualité, la complétude et la pertinence des livrables de toutes les phases de la mission.
* La pertinence de sa démarche.

Le passage d’une phase à une autre ne se fera que à la suite de la validation de la phase d’avant et se fera suite à une validation avec PV.

## Méthodologie

Pour la réalisation de la mission, le soumissionnaire devra suivre une approche méthodologique, en Indiquant les références de la (ou des) méthodologie(s) adoptée(s) ainsi que son adéquation avec les référentiels ISO 27002 : 2022 et ISO 27005 :2018.

En outre, le soumissionnaire devra aussi indiquer dans son offre :

* Les moyens techniques et humains qui seront déployés lors de la mise en œuvre de cette méthodologie (expérience dans la mise en œuvre de la méthodologie consignée et outils logiciels accompagnant la mise en œuvre de cette méthodologie).
* La séquence des actions à mener (interviews, classification des actifs informatiques, synthèse, rédaction de rapports, etc.) et une estimation de la volumétrie homme/jour de chaque action.
* Une description détaillée de la méthode d’appréciation des risques ainsi que les moyens à mettre en œuvre (outils, logiciels…)

# Article 4 : Livrables

Le titulaire doit remettre au maitre d’ouvrage :

**Pour le LOT 01 :**

* Un rapport d’audit préparé conformément au modèle de rapport d’audit établi par l’ANSI ([Modèle de rapport d’audit](https://www.ansi.tn/sites/default/files/Modele%20rapport%20V1.4.pdf) **https://www.ansi.tn/sites/default/files/ModelerapportV1.4.pdf**),
* Un rapport de synthèse destiné à la direction générale (destiné décideurs).

**Pour le LOT 02 :**

* Plan de continuité D’activité PCA
* Politique de sécurité du système d’information PSSI

Ces rapports doivent être datés, visés et porter le cachet de l’expert auditeur. Les captures d’écran et les résultats de l’exécution des différents outils de l’audit technique doivent figurer dans une annexe à part.

# Article 5: Critères de conformité technique

Il sera tenu compte lors de l’évaluation technique des offres, des compétences et de la qualification de l’équipe d’audit et de la méthodologie d’audit.

Les critères de conformité technique (éliminatoires) sont :

1. **LOT 01 : Audit des systèmes d’informations :**
2. Le soumissionnaire est habilité par l’Agence Nationale de la Sécurité Informatique, conformément à l’arrêté du ministre des Technologies de la communication et de l'économie numérique et du ministre du développement, de l’investissement et de la coopération internationale du 01 Octobre 2019, fixant le cahier des charges relatif à l'exercice de l’activité d’audit dans le domaine de la sécurité informatique.
3. Le soumissionnaire doit avoir au moins 05 missions d’audit de sécurité
4. Le nombre d’intervenants est de 02 personnes au minimum, sans compter le chef de projet,
5. Le chef du projet est un auditeur parmi les cadres déclarés dans le cahier des charges pour l’exercice de l’activité d’audit déposé à l’ANSI,
6. L’expérience du chef de projet est supérieure ou égale à 05 ans,
7. Le chef de projet doit avoir piloté au moins 05 missions d’audit de sécurité des systèmes d’information pour le compte d’organismes de taille similaire,
8. L’expérience générale de chaque membre de l’équipe intervenante est supérieure ou égale à 3 ans,
9. Chaque membre de l’équipe intervenante doit avoir participé à au moins 3 missions d’audit de sécurité des systèmes d’information,
10. Présentation de la méthodologie de conduite du projet conformément aux exigences citées en annexe 5.
11. **LOT 02 : Elaboration PCA et PSSI:**
12. Le soumissionnaire doit avoir au moins 02 missions d’élaboration PCA et PSSI
13. Le nombre d’intervenants est d’une personne au minimum, sans compter le chef de projet,
14. L’expérience du chef de projet est supérieure ou égale à 05 ans,
15. Le chef de projet doit avoir piloté au moins 02 missions élaboration du politique de sécurité PSSI et élaboration du plan de continuité d’activité PCA pour le compte d’organismes de taille similaire
16. L’expérience générale de chaque membre de l’équipe intervenante est supérieure ou égale à 3 ans,
17. Chaque membre de l’équipe intervenante doit avoir participé à au moins 01 mission d’élaboration PCA et PSSI pour le compte d’organismes de taille similaire,

# Article 6 : Evaluation Techniques

1. **LOT 01 : Audit des systèmes d’informations :**

L’évaluation des propositions sera faite conformément à la méthodologie suivante :

**Critère 1 : Soumissionnaire**

|  |  |  |
| --- | --- | --- |
| **Ordre** | **Sous-critère** | **Valeur minimale exigée (éliminatoire)** |
| **1** | le soumissionnaire est habilité par l’Agence Nationale de la Sécurité Informatique, conformément à l’arrêté du ministre des technologies de la communication et de l'économie numérique et du ministre du développement, de l’investissement et de la coopération internationale du 01 Octobre 2019, fixant le cahier des charges relatif à l'exercice de l’activité d’audit dans le domaine de la sécurité informatique. | Oui |
| 2 | Spécialisation de l’entreprise dans l’activité d’audit sécurité | Oui |
| 3 | Spécialisation de l’entreprise dans l’activité de la sécurité Informatique (Intégration, Conseil, formation, ….) | Oui |
| 4 | Nombre des missions d’audit sécurité, conformes au décret N° 2004-1250, effectuées durant les cinq dernières années. | 05 Missions : Les missions effectuées doivent être justifiées par des PV de réception ou attestation du client [1]. |

[1] Seules les missions effectuées par le soumissionnaire (seul ou avec des partenaires) et justifiées par des P.V. de réception ou attestations du client seront considérées dans l’évaluation.

**Critère 2 - Qualité des Moyens humains mis à la disposition de la mission**

**Tableau 2.1**

**Compétence du chef du projet**

|  |  |  |
| --- | --- | --- |
| **Ordre** | **Sous-critère** | **Valeur minimale exigée (éliminatoire)** |
| 1 | Expérience générale du chef du projet (en nombre d‘années) | **05 ans** |
| 2 | Expérience en matière de sécurité informatique | **4 ans** |
| 3 | Nombre de Missions d’audit et conformes au décret N° 2004-1250 conduits sous sa gestion directe en Tunisie ou à l’étranger | **05 missions** |
| 4 | le chef du projet est un auditeur parmi les cadres déclarés dans le cahier des charges pour l’exercice de l’activité d’audit déposé à l’ANSI, | **Oui** |
| 5 | Diplôme universitaire | **Ingénieur Informatique ou Télécoms** |

**Tableau 2.2**

**Qualité du personnel affecté à la mission**

|  |  |  |
| --- | --- | --- |
| **Ordre** | **Sous-critère** | **Valeur minimale exigée (éliminatoire)** |
| 1 | Nombre minimale des personnes affectées à la mission sans compter le chef de projet (couvrant l’ensemble des certifications cités au point 4) | 02 |
| 2 | Compétence du personnel affecté, en matière d’audit et sécurité | Voir sous-tableau  2.2**.1** |
| 3 | Nombre des membres auditeurs certifiés par l’ANSI (autres que le chef de projet) | 01 |
| 4 | **Ensemble des Certificats exigés des personnes affectées au projet** | 1. **Linux Server ou Windows Server** 2. **CCNP ou équivalent** |

**Pour chaque type de certifications, le fournisseur doit présenter un certificat pour au moins un membre de l’équipe proposés**

**Tableau 2.2.1 : Compétence du Personnel affectés**

**Pour chaque membre de l’équipe :**

|  |  |  |
| --- | --- | --- |
| **Ordre** | **Sous-critère** | **Valeur minimale exigée (éliminatoire)** |
| 1 | Nombre d’années d’Expérience générale | 3 |
| 2 | Expérience en matière de sécurité informatique | 2 |
| 3 | Nombre de Missions d’audit et conformes au décret N° 2004-1250 conduites durant les cinq dernières années. | 3 |
| 6 | Diplômes universitaire | Maîtrise en Informatique ou Télécoms ou équivalent |

**Tableau 3.1 :**

**Méthodologie suivie pour l’audit Organisationnel et analyse de risque**

|  |  |  |
| --- | --- | --- |
| **Ordre** | **Sous-critère** | **Valeur minimale exigée (éliminatoire)** |
| 1 | Adéquation de la méthodologie proposée, avec la nature de la mission | Oui |
| 2 | Copie électronique ou papier des interviews à effectuer | A fournir |
| 3 | Expérience de l’équipe dans la mise en œuvre de cette méthodologie (Formations, pratique de la méthodologie) | Oui |
| 4 | Outils d’accompagnement utilisés (traitement automatisé des interviews, …) | A préciser |
| 5 | Méthodologie de calcul de risques | A préciser |

**Tableau 3.2 :**

**Méthodologie suivie pour l’audit Technique**

|  |  |  |
| --- | --- | --- |
| **Ordre** | **Sous-critère** | **Valeur minimale exigée (éliminatoire)** |
| 1 | Adéquation de la méthodologie proposée avec la nature de l’infrastructure.(décrire l’approche méthodologique d’audit technique que le soumissionnaire entend appliquer) | Oui |
| 2 | Une description des tests à effectuer | A fournir |
| 3 | Une description des outils et scripts utilisés | A fournir |
| 4 | Méthodologie d’analyse et de report des failles | A préciser |

1. **LOT 02 : Elaboration du plan de continuité d’activité PCA et Politique de Sécurité des systèmes d’information PSSI :**

L’évaluation des propositions sera faite conformément à la méthodologie suivante :

**Critère 1 : Soumissionnaire**

Les soumissionnaires sont tenus de respecter les caractéristiques minimales éliminatoires mentionnées dans les tableaux ci-dessous. Une réponse non justifiée à une caractéristique demandée est considérée non fournie, par conséquent l’offre fera l’objet d’un rejet :

|  |  |  |
| --- | --- | --- |
| **Ordre** | Critères | Valeurs minimales exigées |
| 01 | Spécialisation de l’entreprise dans l’activité de la sécurité Informatique (Intégration, Conseil, formation, ….) | Oui |
| 02 | Nombre total de références du soumissionnaire dans l’élaboration des plans de continuité des activités (PCA) et la politique de sécurité durant les cinq dernières années. | 02 Missions (attestation, PV de réception, ou autre document justifiant la bonne exécution). [1]. |
| 03 | Nombre total de références du soumissionnaire dans l’élaboration du politique de sécurité du système d’information durant les cinq dernières années. | 02 Missions (attestation, PV de réception, ou autre document justifiant la bonne exécution). [1]. |

[1] Seules les missions effectuées par le soumissionnaire (seul ou avec des partenaires) et justifiées par des P.V. de réception ou attestations du client seront considérées dans l’évaluation.

**Critère 2 - Qualité des Moyens humains mis à la disposition de la mission**

**Compétence du chef du projet**

|  |  |  |
| --- | --- | --- |
| **Ordre** | **Sous-critère** | **Valeur minimale exigée (éliminatoire)** |
| 1 | Expérience générale du chef du projet (en nombre d‘années) | **05 ans** |
| 2 | Expérience en matière de sécurité informatique | **4 ans** |
| 3 | Nombre de Missions élaboration PCA et PSSI | **02 missions** justifiées par des P.V |
| 4 | Diplôme universitaire | **Ingénieur Informatique ou Télécoms** |

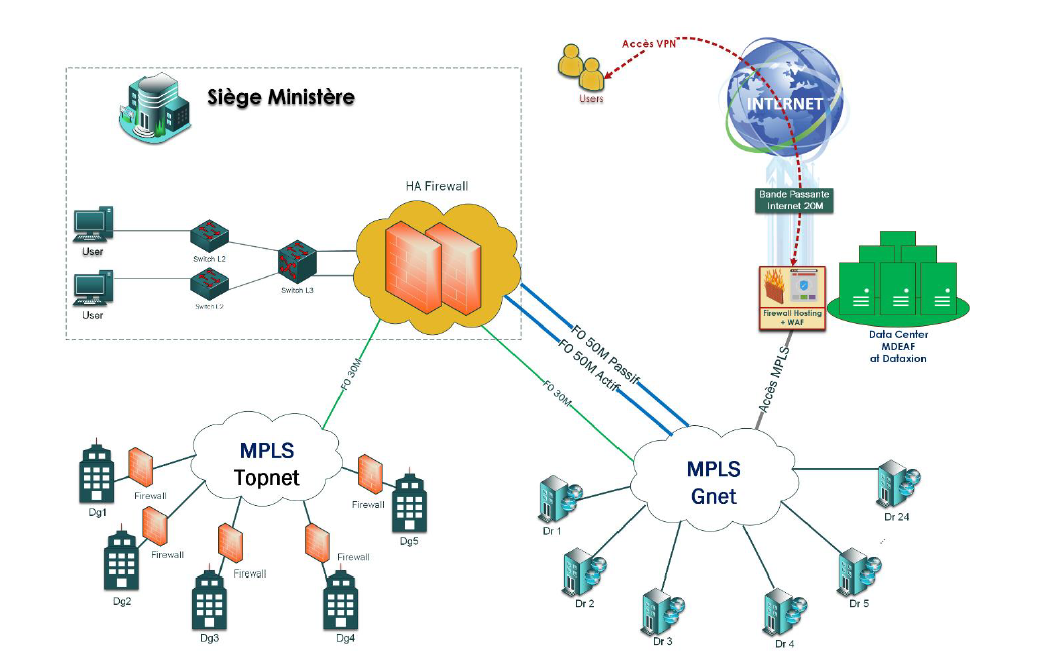
**Qualité du personnel affecté à la mission**

|  |  |  |
| --- | --- | --- |
| **Ordre** | **Sous-critère** | **Valeur minimale exigée (éliminatoire)** |
| 1 | Nombre minimale des personnes affectées à la mission sans compter le chef de projet | 01 |
| 2 | Nombre d’années d’Expérience générale | 3 |
| 3 | Une mission de réalisation PCA (pour au moins un membre de l’équipe) | 01 justifiées par des P.V |
| 4 | Une mission de réalisation PSSI (pour au moins un membre de l’équipe) | 01 justifiées par des P.V |
| 5 | Diplômes universitaire | Maîtrise en Informatique ou Télécoms ou équivalent |

Il est obligatoire de joindre les pièces suivantes :

* Les CVs (datés et signés par le soumissionnaire et l’intéressé) portant les photos des intervenants,
* Des copies des diplômes des intervenants,
* Des copies des attestations d’expériences signées,
* Des copies des certificats,
* Les pièces justificatives nécessaires prouvant la bonne exécution des projets mentionnés,
* Les pièces justificatives nécessaires prouvant la participation des membres de l’équipe intervenante à la bonne exécution des projets cités dans leurs CVs,
* Toute autre pièce justificative jugée nécessaire.

# Article 7 : Organigramme global des entités à auditer:



# Article 8 : Description Volumétrique des structures à auditer

Le ministère des domaines de l’état bénéfice des services de Cloud Computing en mode IaaS (Infrastructure As A Service) location de ressources pour l’hébergement de l’infrastructure de production de son système d’information dans un Datacenter du **DATAXION** en collaboration de **GNET,** Les serveurs de production métier sont hébergés dans ce DataCenter certifié ISO 2700. Des visites seront programmées au centre durant la mission d’audit.

L’environnement Cloud pour le site de production et mise en place d’une :

• Solution de sécurité Virtuelle pour la Datacenter

• Solution de sauvegarde

• Une solution de firewall Web Applicatif (WAF) pour la protection des applications Web, la protection du trafic http/https pour la Datacenter.

• Solution d’accès Intranet via IP/MPLS avec une fibre redondante du 50 Méga (actif-passif)

Liste des structures à auditer, via un audit sur terrain

|  |  |  |
| --- | --- | --- |
|  | Structure | Lieu d’implantation (gouvernorat) |
|  | Dataxion Hébergeur Cloud | Local Dataxion Manouba qui héberge les serveurs |
|  | Siège du Ministère des Domaines de l’Etat | Tour de la Nation Avenue Med V Tunis |
|  | Contentieux de l’ Etat | 19 avenue Paris Tunis |
|  | Directions (Gestion et Vente, Acquisition et délimitations, Biens Etrangers) | Boulevard 9 Avril Tunis |
|  | Direction Générale des immeubles Agricoles | Rue Iran Tunis |
|  | Directions Générales des Expertises | Rue Jean Jacque Ressou Mont plaisir Tunis |

**Nb :**

1. Toutes les directions situées ci-dessus sont inclus dans le périmètre d’Audit
2. Dans chaque direction prendre un échantillon de 3 postes de travail avec différents OS à auditer

|  |  |  |
| --- | --- | --- |
| Site 1 : DATAXION GNET | Volumétrie du Système d’Information | Périmètre de l’audit |
|  |  |
| Lieu | Manouba |  |
| Nombre de responsables à interviewer |  |  |
| Centres de calcul à auditer | Centre Cloud  01 |  |
| Nombre des serveurs | 26 Serveurs Virtuelles |  |
| **Serveurs** | | |
| Nombre Total de Serveurs | 26 Serveurs |  |
| - Type d'OS | Windows 2019, 2016, 2008 Server  Centos 6, 7 |  |
| - Nombre d'utilisateurs supportés | 600 |  |
| **Applications** | | |
| Nombre d’applications (objet de l’audit de sécurité) | 26 Applications |  |
| - Nombre d'utilisateurs | 600 |  |
| - Environnement des applications | Voir les applications ci-dessous |  |
| **Réseau** | | |
| - Nombre de sites distants interconnectés | 27 |  |
| - Nombre de sous-réseaux (internes et externes) | 04 sous Réseaux |  |
| - Connexions externes : |  |  |
| . Nombre de connexions permanentes, leur type (LS, FR,…) et leurs utilisations (Internet, inter-sites, avec des sites externes) | 2 Fibre Optique |  |
| Outils de Sécurité | | |
| Firewalls |  |  |
| Nombre de systèmes de Firewalling, leurs types et Nombre de DMZs supportées | 02 Fortigate VM |  |
| Type de connexions VPN activées au niveau des firewalls. | 1 |  |
| Serveurs anti-virus | | |
| Nombre de serveurs anti-virus et nombre de licences | 1 Serveur + 1200 licences |  |
| Nombre de passerelles anti-virales et leur usage (e-mail, web, FTP,… | 2 |  |
| Outils de sauvegarde automatique et leurs types | Serveur Veeam Backup & Replication 11 |  |

Serveurs et Applications métiers :

Les serveurs sont hébergés dans le cloud Dataxion sont présenté ci joints :

1. ACTIVE Directory (prinicpale et secondaire):

|  |  |  |  |
| --- | --- | --- | --- |
| **Applications** | | | |
| Nom | Environnement de développement | Développée par /Année | Nombre d’utilisateurs |
| Active Directory |  | 2022 / RFC | 600 |

|  |  |  |
| --- | --- | --- |
| **Serveurs** | | |
| **Nom** | **Système d’exploitation** | **Fonctionnalités (2)** |
| **Active-Directory** | **Windows 2019 Server** | **Active Directory, DNS** |

1. Microsoft Endpoint configuration Management :

|  |  |  |  |
| --- | --- | --- | --- |
| **Applications** | | | |
| Nom | Environnement de développement | Développée par /Année | Nombre d’utilisateurs |
| Gestion des postes de travail Windows |  | 2022 / RFC | 600 |

|  |  |  |
| --- | --- | --- |
| **Serveurs** | | |
| **Nom** | **Système d’exploitation** | **Fonctionnalités (2)** |
| **Serv-Mecm** | **Windows 2019 Server** | **Mecm, gestion des mise à jour windows , gestion des applications** |

1. Serveur Fichier et impression:

|  |  |  |  |
| --- | --- | --- | --- |
| **Applications** | | | |
| Nom | Environnement de développement | Développée par /Année | Nombre d’utilisateurs |
| Serveur de fichier et de gestion d’impression |  | 2022 / RFC | 600 |

|  |  |  |
| --- | --- | --- |
| **Serveurs** | | |
| **Nom** | **Système d’exploitation** | **Fonctionnalités (2)** |
| **Serv-File-Impres** | **Windows 2019 Server** | **Serveur de fichier**  **Serveur d’impression** |

1. Gestion des Véhicules :

|  |  |  |  |
| --- | --- | --- | --- |
| **Applications** | | | |
| Nom | Environnement de développement | Développée par /Année | Nombre d’utilisateurs |
| Gestion Véhicules | Jsp | Interne | 30 |

|  |  |  |
| --- | --- | --- |
| **Serveurs** | | |
| **Nom** | **Système d’exploitation** | **Fonctionnalités (2)** |
| **App\_Serv** | **Windows 2008 Server** | **Base de données Postgresql**  **application métier**  **Apache Tomcat** |

1. Contentieux de l’état :

|  |  |  |  |
| --- | --- | --- | --- |
| **Applications** | | | |
| Nom | Environnement de développement | Développée par /Année | Nombre d’utilisateurs |
| CNX | J2ee | Externe | 100 |

|  |  |  |
| --- | --- | --- |
| **Serveurs** | | |
| **Nom** | **Système d’exploitation** | **Fonctionnalités (2)** |
| **CNX** | Linux Centos | **Base de données oracle**  **Application métier**  **Apache Tomcat** |

1. Systèmes d’administration intégré bien de l’état :

|  |  |  |  |
| --- | --- | --- | --- |
| **Applications** | | | |
| Nom | Environnement de développement | Développée par /Année | Nombre d’utilisateurs |
| SAIBE | J2ee | Interne | 100 |

|  |  |  |
| --- | --- | --- |
| **Serveurs** | | |
| **Nom** | **Système d’exploitation** | **Fonctionnalités (2)** |
| **Saibe** | Windows 2008 server | **Base de données oracle**  **Application métier**  **Apache Tomcat** |

1. Demande d’expertise:

|  |  |  |  |
| --- | --- | --- | --- |
| **Applications** | | | |
| Nom | Environnement de développement | Développée par /Année | Nombre d’utilisateurs |
| Gde Expertise | Dotnet | Microsystem/2017 | 50 |

|  |  |  |
| --- | --- | --- |
| **Serveurs** | | |
| **Nom** | **Système d’exploitation** | **Fonctionnalités (2)** |
| Gde Expertise | Windows 2008 server | **Base de données Postgresql/SqlServer**  **Application métier**  **IIS** |

1. Serveur Carte numérique SIG :

|  |  |  |  |
| --- | --- | --- | --- |
| **Applications** | | | |
| Nom | Environnement de développement | Développée par /Année | Nombre d’utilisateurs |
| SIG | Java | Yebni/2016 | 50 |

|  |  |  |
| --- | --- | --- |
| **Serveurs** | | |
| **Nom** | **Système d’exploitation** | **Fonctionnalités (2)** |
| SIG | Linux Centos | **Base de données Postgresql/Postgis**  **Application métier, Tomcat** |

1. SIG Frontale:

|  |  |  |  |
| --- | --- | --- | --- |
| **Applications** | | | |
| Nom | Environnement de développement | Développée par /Année | Nombre d’utilisateurs |
| SIG | Java | Yebni/2016 | 50 |

|  |  |  |
| --- | --- | --- |
| **Serveurs** | | |
| **Nom** | **Système d’exploitation** | **Fonctionnalités (2)** |
| SIG | Linux Centos | **Base de données Postgresql/Postgis**  **Application métier, Tomcat** |

1. Web Service :

|  |  |  |  |
| --- | --- | --- | --- |
| **Applications** | | | |
| Nom | Environnement de développement | Développée par /Année | Nombre d’utilisateurs |
| Webservice | Java | Interne |  |

|  |  |  |
| --- | --- | --- |
| **Serveurs** | | |
| **Nom** | **Système d’exploitation** | **Fonctionnalités (2)** |
| Webservices | Linux Centos | **Base de données Postgresql/mysql**  **Application métier, Tomcat** |

1. Gestion électronique des documents :

|  |  |  |  |
| --- | --- | --- | --- |
| **Applications** | | | |
| Nom | Environnement de développement | Développée par /Année | Nombre d’utilisateurs |
| GED | Alfresco+ ASP.net | |  | | --- | | InterneOpen Source | |  |

|  |  |  |
| --- | --- | --- |
| **Serveurs** | | |
| **Nom** | **Système d’exploitation** | **Fonctionnalités (2)** |
| GED | Windows 2008 server | **Base de données Postgresql/mysql**  **Application métier, Tomcat** |

1. Primes :

|  |  |  |  |
| --- | --- | --- | --- |
| **Applications** | | | |
| Nom | Environnement de développement | Développée par /Année | Nombre d’utilisateurs |
| Application Prime MDEAF | PHP PostgreSQL | |  | | --- | | Interne Open Source | |  |

|  |  |  |
| --- | --- | --- |
| **Serveurs** | | |
| **Nom** | **Système d’exploitation** | **Fonctionnalités (2)** |
| Server Primes | Windows 2008 server | **Base de données Postgresql**  **Application métier**  **Tomcat** |

1. Saibe Agricoles :

|  |  |  |  |
| --- | --- | --- | --- |
| **Applications** | | | |
| Nom | Environnement de développement | Développée par /Année | Nombre d’utilisateurs |
| Saibe Agricoles | Dotnet et SQL Server | |  | | --- | | Société externe | |  |

|  |  |  |
| --- | --- | --- |
| **Serveurs** | | |
| **Nom** | **Système d’exploitation** | **Fonctionnalités (2)** |
| Multibase | Windows 2016 server | **Base de données SQL Server**  **Application métier**  **IIS** |

1. Serveur Antivirus:

|  |  |  |  |
| --- | --- | --- | --- |
| **Applications** | | | |
| Nom | Environnement de développement | Développée par /Année | Nombre d’utilisateurs |
| Eset Antivirus | Serveur Antivirus ESET SERVER |  | 1200 |

|  |  |  |
| --- | --- | --- |
| **Serveurs** | | |
| **Nom** | **Système d’exploitation** | **Fonctionnalités (2)** |
| Eset Server | Centos | Serveur Antivirus |

1. Solution de Backup:

|  |  |  |  |
| --- | --- | --- | --- |
| **Applications** | | | |
| Nom | Environnement de développement | Développée par /Année | Nombre d’utilisateurs |
| Veeam Backup | Veeam Backup et replication |  | 17 |

|  |  |  |
| --- | --- | --- |
| **Serveurs** | | |
| **Nom** | **Système d’exploitation** | **Fonctionnalités (2)** |
| Mde-Veeam-Bkp | Windows 2019 Server | Serveur Backup |

**Le fournisseur est tenue d’auditer le site web et le serveur mail du ministère hébergé au niveau de ATI**

**Site Web du Ministère Externe :** [**www.domainetat.tn**](http://www.domainetat.tn)

**Serveur Mail** [**https://mail.domainetat.tn**](https://mail.domainetat.tn)

|  |  |
| --- | --- |
| Site 2 : Siège du Ministère des Domines de l’Etat  Tour de la Nation Av Med V Tunis | Volumétrie du Système d’Information |
|  |
| Nombre de responsables à interviewer | 01 |
| Centres de calcul à auditer | 1 Plateforme Virtuelle Vmware |
| Autres infrastructures spécifiques à auditer physiquement et/ou organisationnellement |  |
| Autre détails particuliers sur le niveau d’inspection physique ou/et organisationnel désiré |  |
| PC | |
| Nb Total de PCs | 250 |
| Type d'OS : |  |
| - Nombre moyen de PC sous Windows | 250 |
| - Nombre moyen de PC sous Mac OS |  |
| - Nombre moyen de PC sous Linux |  |
| Autres OS. |  |
| Serveurs | |
| Nombre Total de Serveurs | 5 |
| - Type d'OS | Linux Centos , Windows Server |
| - Nombre d'utilisateurs supportés | Public |
| Applications | |
| Nombre d’applications (objet de l’audit de sécurité) | 3 |
| - Nombre d'utilisateurs | Public |
| Réseau | |
| - Nombre de sites distants interconnectés | 30 Sites |
| - Nombre de sous-réseaux (internes et externes) | 14 Vlan |
| - Connexions externes : |  |
| . Nombre de connexions permanentes, leur type (LS, FR,…) et leurs utilisations (Internet, inter-sites, avec des sites externes) | 02Fibre Optique Topnet  02 Fibre Gnet  01 Fo ATI  01 FO CNI (RNIA2) |
| . Nombre de Connexions Dial-Up et leurs utilisations (Internet, inter-sites, avec des sites externes) |  |
| . Nombre de routeurs et types de connexions supportées | 02 routeur cisco  01 routeur cisco 981  01 routeur ciscoTrunksip |
| Nombre de switchs et niveau (2,3,…) | -13SwitchsCisco SG 300 et SG 500 niveau 2  -02 Switch (stack)Cisco 3850 Niveau 3 |
| Outils d'administration réseau et leurs types | ssh et web |
| Autres : …… |  |
| Outils de Sécurité | |
| Firewalls |  |
| Nombre de systèmes de Firewalling, leurs types et Nombre de DMZs supportées | * 02 Firewalls Fortigate 100 F * 02 Firewalls Fortigate 300 E * 1 Firewall Fortigate 200 D |
| Type de connexions VPN activées au niveau des firewalls. | VPN IPSec fortigate |
| Serveurs anti-virus | |
| Nombre de serveurs anti-virus et nombre de licences |  |
| Nombre de passerelles anti-virales et leur usage (e-mail, web, FTP,… | 01 |
| Outils d’authentification | |
| Nombre de serveurs d'authentification réseau internes et nombre moyen d’utilisateurs supportés |  |
| Nombre de serveurs d'authentification réseau pour les accès distants et nombre moyen d’utilisateurs supportés |  |
| Outils de détection d'intrusion | |
| Nombre de NIDS (IDS réseau) | 02 Fortigate 100 F |
| Nombre de sondes HIDS (IDS hôte) |  |
| Nombre de Firewalls PC ou Distribués |  |
| Outils de sauvegarde automatique et leurs types |  |
| Outils intégrés d'administration de la sécurité et leurs types |  |
|  |  |
| Autres outils, le cas échéant (authentification forte, PKI, chiffrement, ...) |  |

A auditer les équipements à auditer

Réseaux :

1. Deux Switchs Cisco niveau 3 Catalyst L3 WS-C3850-12S
2. 11 Switchs d’acces Cisco managed Switch Poe SG300 et SG500

Sécurité

1. Deux fortigates 100 F
2. Deux Fortigates 300 E
3. Un fortigate 200 D

Pour les postes de travail prendre des échantillons selon le modèle du systèmes d’exploitation et des applications utilisées.

|  |  |
| --- | --- |
| Site 3: Siège de Contentieux de l'Etat 19 Av. de Paris | Volumétrie du Système d’Information |
| Nombre de responsables à interviewer |  |
| Centres de calcul à auditer | 00 |
| Autres infrastructures spécifiques à auditer physiquement et/ou organisationnellement |  |
| Autre détails particuliers sur le niveau d’inspection physique ou/et organisationnel désiré |  |
| PC | |
| Nb Total de PCs | 150 |
| Type d'OS : |  |
| - Nombre moyen de PC sous Windows | 150 |
| - Nombre moyen de PC sous Mac OS |  |
| - Nombre moyen de PC sous Linux |  |
| Autres OS. |  |
| Réseau | |
| - Nombre de sites distants interconnectés | 2 |
| - Nombre de sous-réseaux (internes et externes) | 1sous Réseaux |
| - Connexions externes : |  |
| . Nombre de connexions permanentes, leur type (LS, FR,…) et leurs utilisations (Internet, inter-sites, avec des sites externes) | Fibre Optique  1 Fibre Gnet  1 Fibre Topnet (redonandat) |
| . Nombre de Connexions Dial-Up et leurs utilisations (Internet, inter-sites, avec des sites externes) |  |
| . Nombre de routeurs et types de connexions supportées | 4 |
| Nombre de switchs et niveau (2,3,…) | 15 Switchs niveau 2  2 Switch Niveau 3 |
| Outils d'administration réseau et leurs types | Ssh et web |
| Autres : …… |  |
| Outils de Sécurité | |
| Firewalls |  |
| Nombre de systèmes de Firewalling, leurs types et Nombre de DMZs supportées | 1 Fortigate 60 F |
| Type de connexions VPN activées au niveau des firewalls. | 1 |
| Nombre de passerelles anti-virales et leur usage (e-mail, web, FTP,… | 1 |
| Outils d’authentification | |
| Nombre de serveurs d'authentification réseau internes et nombre moyen d’utilisateurs supportés |  |
| Nombre de serveurs d'authentification réseau pour les accès distants et nombre moyen d’utilisateurs supportés |  |
| Outils de détection d'intrusion | |
| Nombre de NIDS (IDS réseau) | 1 Fortigate 60 F |
| Nombre de sondes HIDS (IDS hôte) |  |
| Nombre de Firewalls PC ou Distribués |  |
| Outils intégrés d'administration de la sécurité et leurs types |  |
| Autres outils, le cas échéant (authentification forte, PKI, chiffrement, ...) |  |

Auditer les équipement réseaux switchs (huawei, hp, ) et l’équipement de sécurité Fortigate 60 F ainsi que des échantillons des postes de travail.

|  |  |
| --- | --- |
| Site 4: DG Vente & Acquisition Rue 9 Avril | Volumétrie du Système d’Information |
| Nombre de responsables à interviewer | 01 |
| Centres de calcul à auditer | 00 |
| Autres infrastructures spécifiques à auditer physiquement et/ou organisationnellement |  |
| Autre détails particuliers sur le niveau d’inspection physique ou/et organisationnel désiré |  |
| PC | |
| Nb Total de PCs | 150 |
| Type d'OS : |  |
| - Nombre moyen de PC sous Windows | 150 |
| - Nombre moyen de PC sous Mac OS |  |
| - Nombre moyen de PC sous Linux |  |
| Autres OS. |  |
| Réseau | |
| - Nombre de sites distants interconnectés | 01 |
| - Nombre de sous-réseaux (internes et externes) | 01 |
| - Connexions externes : |  |
| . Nombre de connexions permanentes, leur type (LS, FR,…) et leurs utilisations (Internet, inter-sites, avec des sites externes) | 01 Fibre Optique (backup Adsl) |
| . Nombre de Connexions Dial-Up et leurs utilisations (Internet, inter-sites, avec des sites externes) |  |
| . Nombre de routeurs et types de connexions supportées | 01 |
| Nombre de switchs et niveau (2,3,…) | 13 Switchs niveau 2 |
| Outils d'administration réseau et leurs types | Telent ,ssh et web |
| Autres : …… |  |
| Outils de Sécurité | |
| Firewalls |  |
| Nombre de systèmes de Firewalling, leurs types et Nombre de DMZs supportées | 01 Fortigate 60 F |
| Type de connexions VPN activées au niveau des firewalls. | 0 |
| Outils d’authentification | |
| Nombre de serveurs d'authentification réseau internes et nombre moyen d’utilisateurs supportés |  |
| Nombre de serveurs d'authentification réseau pour les accès distants et nombre moyen d’utilisateurs supportés |  |
| Outils de détection d'intrusion | |
| Nombre de NIDS (IDS réseau) | 01 Fortigate 60 F |
| Nombre de sondes HIDS (IDS hôte) |  |
| Nombre de Firewalls PC ou Distribués |  |
| Outils de sauvegarde automatique et leurs types |  |
| Outils intégrés d'administration de la sécurité et leurs types |  |
| Autres outils, le cas échéant (authentification forte, PKI, chiffrement, ...) |  |

Auditer les équipement réseaux switchs (huawei, hp, ) et l’équipement de sécurité Fortigate 60 F ainsi que des échantillons des postes de travail.

|  |  |
| --- | --- |
| Site 5 : DG Terre Agricole  Rue d'Iran | Volumétrie du Système d’Information |
|  |
| Nombre de responsables à interviewer | 01 |
| Centres de calcul à auditer | 00 |
| Autres infrastructures spécifiques à auditer physiquement et/ou organisationnellement |  |
| Autre détails particuliers sur le niveau d’inspection physique ou/et organisationnel désiré |  |
| PC | |
| Nb Total de PCs | 100 |
| Type d'OS : |  |
| - Nombre moyen de PC sous Windows | 100 |
| - Nombre moyen de PC sous Mac OS |  |
| - Nombre moyen de PC sous Linux |  |
| Autres OS. |  |
| Réseau | |
| - Nombre de sites distants interconnectés | 02 |
| - Nombre de sous-réseaux (internes et externes) | 02 sous réseaux |
| - Connexions externes : |  |
| . Nombre de connexions permanentes, leur type (LS, FR,…) et leurs utilisations (Internet, inter-sites, avec des sites externes) | 01 Fibre Optique (backup Adsl) et 1 ADSL |
| . Nombre de Connexions Dial-Up et leurs utilisations (Internet, inter-sites, avec des sites externes) |  |
| . Nombre de routeurs et types de connexions supportées | 01 |
| Nombre de switchs et niveau (2,3,…) | 07 Switchs niveau 2 |
| Outils d'administration réseau et leurs types | Telent ,ssh et web |
| Autres : …… |  |
| Outils de Sécurité | |
| Firewalls |  |
| Nombre de systèmes de Firewalling, leurs types et Nombre de DMZs supportées | 01 Fortigate 60 F |
| Type de connexions VPN activées au niveau des firewalls. | 0 |
| Outils d’authentification | |
| Nombre de serveurs d'authentification réseau internes et nombre moyen d’utilisateurs supportés |  |
| Nombre de serveurs d'authentification réseau pour les accès distants et nombre moyen d’utilisateurs supportés |  |
| Outils de détection d'intrusion | |
| Nombre de NIDS (IDS réseau) | 01 |
| Nombre de sondes HIDS (IDS hôte) |  |
| Nombre de Firewalls PC ou Distribués |  |
| Outils de sauvegarde automatique et leurs types |  |
| Outils intégrés d'administration de la sécurité et leurs types |  |
| Autres outils, le cas échéant (authentification forte, PKI, chiffrement, ...) |  |

Auditer les équipement réseaux switchs et l’équipement de sécurité Fortigate 60 F ainsi que des échantillons des postes de travail.

|  |  |
| --- | --- |
| Site 6 : DG Expertise ue J.J Rousseau | Volumétrie du Système d’Information |
| Nombre de responsables à interviewer | 01 |
| Centres de calcul à auditer | 00 |
| Autres infrastructures spécifiques à auditer physiquement et/ou organisationnellement |  |
| Autre détails particuliers sur le niveau d’inspection physique ou/et organisationnel désiré |  |
| PC | |
| Nb Total de PCs | 45 |
| Type d'OS : |  |
| - Nombre moyen de PC sous Windows | 45 |
| - Nombre moyen de PC sous Mac OS |  |
| - Nombre moyen de PC sous Linux |  |
| Autres OS. |  |
| Réseau | |
| - Nombre de sites distants interconnectés | 01 |
| - Nombre de sous-réseaux (internes et externes) | 01 |
| - Connexions externes : |  |
| . Nombre de connexions permanentes, leur type (LS, FR,…) et leurs utilisations (Internet, inter-sites, avec des sites externes) | 01 Fibre Optique+ backup ADSL |
| . Nombre de Connexions Dial-Up et leurs utilisations (Internet, inter-sites, avec des sites externes) |  |
| . Nombre de routeurs et types de connexions supportées | 01 |
| Nombre de switchs et niveau (2,3,…) | 04 Switchs niveau 2 |
| Outils d'administration réseau et leurs types | Telent ,ssh et web |
| Autres : …… | Point d’accés Wifi |
| Outils de Sécurité | |
| Firewalls |  |
| Nombre de systèmes de Firewalling, leurs types et Nombre de DMZs supportées | 01 Fortigate 60 F |
| Type de connexions VPN activées au niveau des firewalls. | 0 |
| Outils d’authentification | |
| Nombre de serveurs d'authentification réseau internes et nombre moyen d’utilisateurs supportés |  |
| Nombre de serveurs d'authentification réseau pour les accès distants et nombre moyen d’utilisateurs supportés |  |
| Outils de détection d'intrusion | |
| Nombre de NIDS (IDS réseau) | 01 |
| Nombre de sondes HIDS (IDS hôte) |  |
| Nombre de Firewalls PC ou Distribués |  |
| Outils de sauvegarde automatique et leurs types | NAS |
| Outils intégrés d'administration de la sécurité et leurs types |  |
| Autres outils, le cas échéant (authentification forte, PKI, chiffrement, ...) |  |

Auditer les équipement réseaux switchs et l’équipement de sécurité Fortigate 60 F ainsi que des échantillons des postes de travail.

Liste des Formulaires types, à remplir par le Soumissionnaire

ANNEXE 1

Présentation des offres LOT 01

**Critère 1 : Soumissionnaire**

|  |  |  |  |
| --- | --- | --- | --- |
| **Ordre** | **Sous-critère** | **Valeur minimale exigée** | **Réponse** |
| **1** | le soumissionnaire est habilité par l’Agence Nationale de la Sécurité Informatique, conformément à l’arrêté du ministre des technologies de la communication et de l'économie numérique et du ministre du développement, de l’investissement et de la coopération internationale du 01 Octobre 2019, fixant le cahier des charges relatif à l'exercice de l’activité d’audit dans le domaine de la sécurité informatique. | Oui |  |
| 2 | Spécialisation de l’entreprise dans l’activité d’audit sécurité | Oui |  |
| 3 | Spécialisation de l’entreprise dans l’activité de la sécurité Informatique (Intégration, Conseil, formation, ….) | Oui |  |
| 4 | Nombre des missions d’audit sécurité, conformes au décret N° 2004-1250, effectuées durant les cinq dernières années. | 05 Missions : Les missions effectuées doivent être justifiées par des PV de réception ou attestation du client [1]. |  |

[1] Seules les missions justifiées par des P.V. de réception ou par des attestations du client seront considérées dans l’évaluation.

**Critère 2 - Qualité des Moyens humains mis à la disposition de la mission**

**Tableau 2.1**

**Compétence du chef du projet**

|  |  |  |  |
| --- | --- | --- | --- |
| **Ordre** | **Sous-critère** | **Valeur minimale exigée** | **Réponse** |
| 1 | Expérience générale du chef du projet (en nombre d‘années) | **05 ans** |  |
| 2 | Expérience en matière de sécurité informatique | **4 ans** |  |
| 3 | Nombre de Missions d’audit et conformes au décret N° 2004-1250 conduits sous sa gestion directe en Tunisie ou à l’étranger. | **05 missions** |  |
| 4 | le chef du projet est un auditeur parmi les cadres déclarés dans le cahier des charges pour l’exercice de l’activité d’audit déposé à l’ANSI, | **Oui** |  |
| 5 | Diplôme universitaire | Ingénieur Informatique ou Télécoms |  |
| 6 | Expérience du chef du projet en tant que membre dans des opérations d’audit (en nombre de missions) | **5** |  |

**Tableau 2.2**

**Qualité du personnel affecté à la mission**

|  |  |  |  |
| --- | --- | --- | --- |
| **Ordre** | **Sous-critère** | **Valeur minimale exigée** | **Réponse** |
| 1 | Nombre minimale des personnes affectées à la mission sans compter le chef de projet (couvrant l’ensemble des certifications cités au point 4) | 02 |  |
| 2 | Compétence du personnel affecté, en matière d’audit et sécurité | Voir sous-tableau  2.2**.1** |  |
| 3 | Nombre des membres auditeurs certifiés par l’ANSI (autres que le chef de projet) | A préciser |  |
| 4 | **Ensemble des Certificats exigés des personnes affectées au projet** | 1. **Linux Server ou Windows Server** 2. **CCNP ou équivalent** |  |

**Tableau 2.2.1 : Compétence du Personnel affectés**

**Pour chaque membre de l’équipe :**

|  |  |  |  |
| --- | --- | --- | --- |
| **Ordre** | **Sous-critère** | **Valeur minimale exigée** | **Réponse** |
| 1 | Nombre d’années d’Expérience générale | 3 |  |
| 2 | Expérience en matière de sécurité informatique | 2 |  |
| 3 | Nombre de Missions d’audit et conformes au décret N° 2004-1250 conduites durant les trois dernières années. | 3 |  |
| 6 | Diplômes universitaire | Maîtrise en Informatique ou Télécoms ou équivalent |  |

[1] Seules les missions justifiées par des P.V. de réception ou par des attestations du client seront considérées dans l’évaluation.

Présentation des offres LOT 02

**Critère 1 : Soumissionnaire**

|  |  |  |  |
| --- | --- | --- | --- |
| **Ordre** | **Sous-critère** | **Valeur minimale exigée** | **Réponse** |
| 01 | Spécialisation de l’entreprise dans l’activité de la sécurité Informatique (Intégration, Conseil, formation, ….) | Oui |  |
| 02 | Nombre total de références du soumissionnaire dans l’élaboration des plans de continuité des activités (PCA) et la politique de sécurité durant les cinq dernières années. | 02 Missions (attestation, PV de réception, ou autre document justifiant la bonne exécution). [1]. |  |
| 03 | Nombre total de références du soumissionnaire dans l’élaboration du politique de sécurité du système d’information durant les cinq dernières années. | 02 Missions (attestation, PV de réception, ou autre document justifiant la bonne exécution). [1]. |  |

Seules les missions justifiées par des P.V. de réception ou par des attestations du client seront considérées dans l’évaluation.

**Critère 2 - Qualité des Moyens humains mis à la disposition de la mission**

**Compétence du chef du projet**

|  |  |  |  |
| --- | --- | --- | --- |
| **Ordre** | **Sous-critère** | **Valeur minimale exigée** | **Réponse** |
| 1 | Expérience générale du chef du projet (en nombre d‘années) | **05 ans** |  |
| 2 | Expérience en matière de sécurité informatique | **4 ans** |  |
| 3 | Nombre de Missions élaboration PCA et PSSI | **02 missions** justifiées par des P.V |  |
| 4 | Diplôme universitaire | **Ingénieur Informatique ou Télécoms** |  |

**Qualité du personnel affecté à la mission**

|  |  |  |  |
| --- | --- | --- | --- |
| **Ordre** | **Sous-critère** | **Valeur minimale exigée** | **Réponse** |
| 1 | Nombre minimale des personnes affectées à la mission sans compter le chef de projet | 01 |  |
| 2 | Nombre d’années d’Expérience générale | 3 |  |
| 3 | Une mission de réalisation PCA (pour au moins un membre de l’équipe) | 01 justifiées par des P.V |  |
| 4 | Une mission de réalisation PSSI (pour au moins un membre de l’équipe) | 01 justifiées par des P.V |  |
| 5 | Diplômes universitaire | Maîtrise en Informatique ou Télécoms ou équivalent |  |

[1] Seules les missions justifiées par des P.V. de réception ou par des attestations du client seront considérées dans l’évaluation.

**ANNEXE 2**

**CV intervenants2**

Nom et Prénom : ..........................................................................................................................................................

Date de naissance : ........................................................................................................................................................ Situation familiale : ........................................................................................................................................................ Date de recrutement : .................................................................................................................................................... Dernier diplôme obtenu : …….………………………...…... Année : ........................................................................................ Nombre d'années d'expérience : ................................................................................................................................... Fonction à assurer : ........................................................................................................................................................ Profil et connaissances : .................................................................................................................................................

**Expérience professionnelle générale dans le domaine de l'informatique**

|  |  |  |  |
| --- | --- | --- | --- |
| **Période** | **Projet** | **Client** | **Période Projet Client Délai global** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Expérience professionnelle dans les projets de mise en place du produit offert**

|  |  |  |  |
| --- | --- | --- | --- |
| **Période** | **Projet** | **Client** | **Période Projet Client Délai global** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Signature et cachet du soumissionnaire**

ـــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــ

**2** Des copies des diplômes et des attestations des expériences professionnelles doivent être joint au CV de chaque intervenant.

**ANNEXE 3**

**Listes des références1**

Citer des références du soumissionnaire :

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **N°** | **Nom du client** | **Secteur d’activité** | **Nature d’intervention (Intégration/Support)** | **Période d’intervention** | **Description de intervention** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**Signature et cachet du soumissionnaire**

ـــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــ

**1** Seules les missions justifiées par des P.V. de réception ou par des attestations du client seront considérées dans l’évaluation.

**ANNEXE 4**

**Liste des intervenants**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Nom et Prénom | Diplôme | Date d’obtention | Certificats obtenues ou formation (Année/ Titre/Organisme) | les missions d’audit en tant que chef de projet (Année/nombre de jours/Organisme) [1] | Les missions d’audit en tant que membre (Année/nombre de jours /Organisme) |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**Signature et cachet du soumissionnaire**

Seules les missions justifiées par des P.V. de réception ou par des attestations du client seront considérées dans l’évaluation.

**ANNEXE 5**

Méthodologie de conduite du projet LOT 01

Présentation des éléments de la méthodologie de conduite du projet comme suit :

1. Périmètre de l’Audit :

* Critères d’échantillonnage pour chaque type de composante du système d’information à auditer, le cas échéant

1. Audit organisationnel & physique :

* Inspections à réaliser : types, description et résultats attendus,
* Structure du questionnaire à effectuer auprès des interviewés de l’audité, et les références d’adéquation des contrôles à vérifier à travers ce questionnaire avec [le référentiel d’audit](https://www.ansi.tn/sites/default/files/Referentiel_Audit%202.1_0.pdf) établi par l’ANSI,
* Echantillon du questionnaire à effectuer,
* les outils d’accompagnement utilisés pour le traitement des interviews, avec la liste des fonctionnalités et la documentation de chaque outil.
* Méthodologie d’Audit technique, incluant le type et l’objet des tests\* à réaliser pour chaque phase de l’audit technique suivant:
  + Audit de l’architecture
  + Audit de la configuration de chaque type de composantes du périmètre de l’audit présentées dans l’annexe A (Description volumétrique des structures à auditer)
  + Audit intrusif.
* Outils utilisés pour réaliser les tests pour chacune des phases de l’audit technique suscitées (voir Annexe 7 : présentation des outils techniques utilisés),
* La méthodologie d’analyse et de report des failles, selon leur gravité.

1. Analyse et évaluation des risques:

* Méthodologie d’Analyse et d’évaluation des risques, en précisant :
  + les critères de choix de la portée de l’analyse et de l’évaluation des risques,
  + les références d’adéquation de cette méthodologie avec les normes et les méthodologies connues à l’échelle internationale dans le domaine,
* les outils d’accompagnement pour effectuer l’analyse et l’évaluation des risques.

**ANNEXE 6**

Planning prévisionnel de la mission d’audit LOT 1

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Composant | | | Equipe intervenante | Durée en Hommes/jours pour chaque intervenant | | Logistique utilisée (Outils,…) | Livrable |
| Phase | | Objet de la sous phase | Sur Site | Totale |
| Audit | Audit Organisationnel et physique | 1: …………………... | Nom:…………………… |  |  |  |  |
| 2: ……………… | Nom:…………………… |  |  |  |  |
| Audit Technique | 1: …………………... | Nom:…………………… |  |  |  |  |
| 2: …………………… | Nom:…………………… |  |  |  |  |
| Elaboration du Plan de continuité d’activité | | 1: …………………... | Nom:…………………… |  |  |  |  |
| 2: …………………… | Nom:…………………… |  |  |  |  |
| Elaboration du Politique de sécurité du système d’information | | 1: …………………... | Nom:…………………… |  |  |  |  |
| 2: …………………… | Nom:…………………… |  |  |  |  |
| Durée Totale de la mission (en Homme/jour) | | | |  |  |  |  |

|  |  |
| --- | --- |
| Signature et cachet du soumissionnaire |  |
| Noms et signatures de(s) auditeur(s) certifié(s) | |

Délais de Réalisation PCA LOT 02

|  |  |
| --- | --- |
| Durée d’exécution (en nombre de jours) | Phases |
|  | Phase 1 : Etude de contexte |
|  | Phase 2 : Analyse des risques |
|  | Phase 3 : Analyse des impacts d'activité : Business Impact Analysis (BIA) |
|  | Phase 4 : Développement de la stratégie de continuité du système d'information et des processus métiers les plus critiques) |
|  | Phase 5 : Mise en œuvre des plans de continuité d'activité |
|  | Phase 6 : Test et simulation du plan de continuité d'activité |
|  | Délais global de réalisation des prestations requises dans le cadre de cette consultation |

Fait à ……..…. le………….

le soumissionnaire

Nom, prénom et qualité du signataire

Signature et Cachet du soumissionnaire

ANNEXE 7

Présentation des outils techniques utilisés

* Outils de …………………………………………………………[[1]](#footnote-1) :

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Outils | Référence | liste des fonctionnalités offertes ou à mettre en œuvre dans la mission | Utilité pour la mission | Lieu d’utilisation  (Planning, phase) | Référence de la documentation dans le dossier de l’offre  (éventuellement sous forme électronique : CD, ..) |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**ANNEXE 8**

**Engagement sur la confidentialité des données**

*(A remplir et à insérer obligatoirement dans les documents administratifs)*

Je soussigné ……………………………………………..………………………………………………………………

agissant en tant que ……………………………………….……............……………………………………………….………

de la société (ou entreprise) …………………………………………………………………………..…………………………………

Soumissionnaire de la consultation lancée par le Ministère des Domaines de l’Etat et des Affaires Foncières sous le N° 33/2022

M’engage à respecter et à faire respecter par ses employés et collaborateurs les obligations suivantes :

* Utiliser les Informations et Documents, quelles que soient leurs formes (notamment orale, papier, numérique,) ou leur contenu, qui me sont remis par le Ministère ou dont je prends connaissance, dans le strict cadre des prestations que je réalise pour le compte du Ministère des Domaines de l’état ; je m’interdis notamment toute utilisation des Informations et Documents pour mon compte personnel ou pour le compte de tiers ;
* Protéger les Informations et Documents et les garder strictement confidentiels ;
* Ne pas divulguer les Informations et Documents directement ou indirectement à tout tiers ;
* Maintenir les formules de copyright et autres insertions de droit de propriété figurant sur les documents communiqués, quelle que soient leur forme (papier, numérique...), qu’ils s’agissent d’originaux ou de copies ;
* Eviter que les Informations et Documents ne soient ni copiés ni reproduits ni dupliqués, en partie ou en totalité, sur quel que support que ce soit, lorsque de telles copies, reproductions ou duplications ne sont pas directement liées à l’exécution de mes engagements relatives au projet;
* Restituer immédiatement à première demande, ou à détruire après accord du Ministère, toutes les Informations et Documents et leurs éventuelles reproductions, duplications, copies.

Le présent engagement est pris par le Prestataire sans limite de durée.

**Signature et cachet du soumissionnaire**

**ANNEXE 9 : Description du système d’information de l’organisme (à remplir par l’auditeur)**

|  |  |  |  |
| --- | --- | --- | --- |
| **Postes de travail** | | | |
| Système d’exploitation | Nombre | Mentionné dans la description volumétrique (Article 8) (Oui/Non) | Inclus au périmètre d’audit (5) |
|  |  |  |  |
| … |  |  |  |

**Pour chaque site:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Applications** | | | | | |
| Nom (1) | Environnement de développement | Développée par /Année | Nombre d’utilisateurs | Mentionnée dans la description volumétrique (Article 8) (Oui/Non) | Incluse au périmètre d’audit (5) |
|  |  |  |  |  |  |
| … |  |  |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Serveurs** | | | | |
| Nom (1) | Système d’exploitation | Fonctionnalités (2) | Mentionné dans la description volumétrique (Article 8) (Oui/Non) | Inclus au périmètre d’audit (5) |
|  |  |  |  |  |
| … |  |  |  |  |

(1) : Veuillez respecter la même nomenclature utilisée au niveau du rapport d’audit.

(2) : Fonctionnalités : Base de données (MS SQL Server, Oracle, …), messagerie, application métier, Contrôleur de domaine, Proxy, Antivirus, etc.

Veuillez indiquer le(s) nom de (la) solutions métier au niveau de chaque serveur

(3): Nature : Switch, Routeur, Firewall, IDS/IPS, etc

(4) Observations : des informations complémentaires sur l’équipement par exemple niveau du switch

(5) : Oui/Non. Présenter les raisons de l’exclusion le cas échéant.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Infrastructure Réseau et sécurité** | | | | | |
| Nature (3) | Marque | Nombre | Observations (4) | Mentionné dans la description volumétrique (Article 8) (Oui/Non) | Inclus au périmètre d’audit (5) |
|  |  |  |  |  |  |
| … |  |  |  |  |  |

**الملاحق الإدارية والمالية**

**بطاقة إرشادات عامة حول المشارك**

الإسم واللقب أو الإسم الإجتماعي :....................................................................

الشكل القانوني :......................................................................................

عنوان المقر :.........................................................................................

رأس المال :.........................................................................................

الهاتف :..............................................................................................

مرسمة بالسجل التجاري تحت عدد ...................................................................

رقم المعرّف الجبائي :................................................................................

الشخص المفوض لإمضاء وثائق العرض (الإسم واللقب والخطة)......................................

حرر بـ ................في ................

## (إمضاء المشارك وختمه)

## تصريح على الشرف

## في عدم التأثير

### إنّي الممضى أسفله ( الاسم، اللقب، الصفة ) ............................................................................................

### ....................................................................................................................................................

### والمتعهد باسم ولحساب شركة ............................................................................................................

### ...................................................................................................................................................

### أصرح على الشرف بأن ألتزم بعدم القيام مباشرة أو بواسطة الغير بتقديم وعود أو عطايا أو هدايا القصد منها التأثير على مختلف إجراءات إبرام الصفقة ومراحل إنجازها بما يخدم مباشرة أو بصفة غير مباشرة مصلحتي وذلك في إطار الاستشارة عدد 33 لسنة 2022 لوزارة أملاك الدولة والشؤون العقارية.

### .............................. في .............................................

**العارض ( الاسم، اللقب، الصفة التاريخ والختم** **)**

## تصريح على الشرف بعدم العمل لدى الوزارة

إني الممضي أسفله ( الإسم واللقب والصفة ):...........................................................

ممثل شركة ( الإسم الإجتماعي والعنوان ) :..............................................……….......

المرسمة بالسجل التجاري بـ ................... .........تحت عدد.....................................

المعيّن محل مخابرته بـ ( العنوان بالكامل )..............................................................

...........................................................................المسمى فيما يلي "المشارك".

أصرح على شرفي بأني لم أعمل كعونا عموميا لدى وزارة أملاك الدولة والشؤون العقارية أو مضى على انقطاعي عن العمل بها مدة خمس سنوات على الأقل.

حرر بـ .................. في: .........................

**(إمضاء المشارك وختمه)**

الجمهورية التونسية

**وزارة أملاك الدولة والشؤون العقارية**

**(بالنسبة للحصص من 9 إلى 14 دون سواها)**

## وثيقــة التعهـد

## القسط ....

إني الممضي أسفله (2) : .................................................................................................. .........

الصفة : .................................................................................................... ............. .....

الاسم الاجتماعي للمؤسسة : .....................................................................................................

رقم الهاتف : .................................. رقم الفاكس : ...................... رقم التلكس : ..................... ........

رقم السجل التجاري للمؤسسة : ............................... ................................... .................... ......

رقم الانخراط في الصندوق القومي للضمان الاجتماعي : ............ ............................................... ..........

رقم الحساب الجاري للمؤسسة ....................................................................... ........................

أشهد بإطلاعي وبكامل مسؤوليتي على جميع المعلومات الضرورية لضمان حسن تنفيذ جميع التزاماتي المضمنة بكراس الشروط هذا والخاص بالإستشارة عدد 33 لسنة 2022 المـتعـلـقة بالقيام بمهمة التدقيق في مجال السلامة المعلوماتية وإنجاز سياسة أمن نظم المعلومات . وأصرح على الشرف أن كل البيانات التي تهمني والمذكورة سابقا هي صحيحة.

ـ القيمة الجملية للعرض المالي بدون إحتساب الأداءات H.T هي بالأرقام (3) ............................................... (وبلسان القلم) ..............................................................................................................................................

.........................................................................................................................................................

ـ قيمة الأداء على القيمة المضافة بالأرقام (3) ........................................................ (وبلسان القلم) ........................

.........................................................................................................................................................

- القيمة الجملية للعرض المالي باحتساب جميع الأداءات T.T.C هي بالأرقام (3) ............................................. (وبلسان القلم) ...........................................................................................................................................

........................................................................................................................................................

وأتعهد بتسليم جميع التجهيزات في أجل أقصاه .....................................................................................................

**حرر بـ** ...................... **في** .........................

(الاسم واللقب ـ التاريخ والإمضاء والختم)

1. هذا الالتزام المالي يجب أن يكون به تاريخ ثابت وممضى.
2. الاسم واللقب والصفة
3. يجب أن يقع ذكر القيمة الجملية للالتزام المالي وإلا فإن العرض يعتبر لاغيا.

|  |
| --- |
| **جدول الأسعار** |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ع.ر | **القسط** | **بيان المواد** | **الكميّة** | **السعر الفردي خال من الأداءات** | **الأداء على ق . م** | | **السعر الجملي** | |
| النسبة **%** | المبلغ | **السعر الجملي خال من الأداءات** | **السعر الجملي بإحتساب جميع الأداءات** |
| **01** | **القسط عدد 01** | **القيام بمهمة التدقيق لهياكل وزارة أملاك الدولة والشؤون العقارية في مجال السلامة المعلوماتية** | 1 |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  | **المجموع :** | |  |  |  |

المبلغ الجملي خال من الأداءات (بلسان القلم) :.......................................................................................................................................................................................................

المبلغ الجملي بإحتساب جميع الأداءات (بلسان القلم) :.....................................................................................................................................................................................................

**تونس في :..................**

**ختم وإمضاء العارض**

|  |
| --- |
| **جدول الأسعار** |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ع.ر | **القسط** | **بيان المواد** | **الكميّة** | **السعر الفردي خال من الأداءات** | **الأداء على ق . م** | | **السعر الجملي** | |
| النسبة **%** | المبلغ | **السعر الجملي خال من الأداءات** | **السعر الجملي بإحتساب جميع الأداءات** |
| **01** | **القسط عدد 02** | **القسط عدد 01إنجاز سياسة الأمن لتكنولوجيا المعلومات (Politique de sécurité de système d’information PSSI).** | 1 |  |  |  |  |  |
| **إنجاز خطة إستمرارية النشاط (Plan de continuité d’activité PCA)** |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  | **المجموع :** | |  |  |  |

المبلغ الجملي خال من الأداءات (بلسان القلم) :.......................................................................................................................................................................................................

المبلغ الجملي بإحتساب جميع الأداءات (بلسان القلم) :.....................................................................................................................................................................................................

**تونس في :..................**

**ختم وإمضاء العارض**

1. Mettre l’ensemble des types d’outils mentionnés lors de la phase IV- Conduite des activités d’audit  du Cahier de Clauses Techniques Particulières. [↑](#footnote-ref-1)