ФОНД „ВЪТРЕШНА СИГУРНОСТ“

Поставя се в плик №2

ОБРАЗЕЦ № 9А

ТЕХНИЧЕСКО ПРЕДЛОЖЕНИЕ

Уважаеми Дами и Господа,

След запознаване с документацията за участие в открита процедура с предмет **“Поддръжка и обновяване на програмното и техническо осигуряване на Националната визова информационна система и на визовата дейност в консулските служби на Р България”**,

Обособена позиция 1: „Поддръжка и осъвременяване на техническото осигуряване и инфраструктурата на НВИС“

Ние:

От ДЗЗД Ай Би Ес Индекс, София 1172, ул. Пимен Зографски 4,

с водещ съдружник Ай Би Ес – България ЕООД, ЕИК 131086564, София 1172, ул. Пимен Зографски 4 и

съдружник Индекс – България ООД, София 1784, ж.к. „Младост 1” блок 54, етаж 1,

предлагаме да изпълним поръчката съгласно документацията за участие при следните условия:

1. Приемаме да изпълним поръчката в срок от датата на сключване на договора до 31.12.2019 г.

2. Приемаме да изпълним поръчката съгласно всички изисквания на Възложителя, посочени в документацията за участие и техническата спецификация по настоящата обществена поръчка.

3. Декларираме, че ще изпълним поръчката съгласно всички изисквания на Възложителя, посочени в Техническата спецификация по настоящата обществена поръчка.

В допълнение прилагаме описание на тези дейности от Техническата спецификация, за които с нашето Техническо предложение ще надхвърлим изискванията на Възложителя.
- Не е приложимо.

4. Приемаме да изпълним поръчката на мястото, определено в Техническата

Този документ е създаден в рамките на проект „Поддръжка и обновяване на програмното и техническо осигуряване на НВИС и на визовата дейност в консулските служби на Р България“ по ДБФП с рег. № 812108-116, екз. 3/13.10.2015 г., финансиран по линия на фонд „Вътрешна сигурност“ 2014-2020, съфинансиран от Европейския съюз.

000001

спецификация -
гр. София, ул. „Ал. Жендов” № 2 и гр. София, ул. „Витошко лале” № 16.

5. Декларираме, че приемаме да извършим гаранционната поддръжка на доставеното хардуерно оборудване за срок до 31.12.2019.
6. Декларираме, че приемаме да извършим обучение на служители на Възложителя при условията на Техническата спецификация и Техническото ни предложение.

7. Други предложения и/или условия за изпълнение на доставката:

- Не е приложимо.

ПРИЛОЖЕНИЯ:
1. Приложение 1 - Съпътстваща техническа документация - Програма за обучения;
2. Приложение 2 - Техническо предложение за осъвременяването на оборудването по Компонент 2;
3. Приложение 3 - План - Програма за изпълнение на дейностите, съгласно изискванията на Техническата спецификация;
4. Приложение 4 -Подход и методика за управление на изпълнението на предмета на обществената поръчка;
5. Приложение 5 - Методология за управление на риска при изпълнение на проекта съгласно изискванията на Техническата спецификация;
6. Приложение 6 - Подход, методика и начин на изпълнение на дейностите по обслужване на инцидентите и механизма за управление на възникналите проблеми в периода на поддръжката на системите;

Дата: 25.05.2016
Представляващ ДЗЗД Ай Би Ес Индекс, съгласно Договор за консорциум от 19.05.2016,
Горан Ангелов, Управител на Водещ съдружник Ай Би Ес – България ЕООД:

(печат на Водещ съдружник, съгласно т. 3.5. от Договор за консорциум от 19.05.2016)

Този документ е създаден в рамките на проект „Поддръжка и обновяване на програмното и техническо осигуряване на НВИС и на визовата дейност в консулските служби на Р България“ по ДБФП с рег. № 812108-116, екз. 3/13.10.2015 г., финансиран по линия на фонд „Вътрешна сигурност“ 2014-2020, съфинансиран от Европейския съюз.

Приложение 1
Съпътстваща техническа документация
Програма за обучения
към
ТЕХНИЧЕСКА ОФЕРТА

за участие в открита процедура за възлагане на обществена поръчка с предмет: “Поддръжка и обновяване на програмното и техническо осигуряване на Националната визова информационна система и на визовата дейност в консулските служби на Р България”,
Обособена позиция 1: „Поддръжка и осъвременяване на техническото осигуряване и инфраструктурата на НВИС“

От КОНСОРЦИУМ ДЗЗД „Ай Би Ес Индекс”

Конфигурация и администриране на мрежовата и комуникационна инфраструктура от Компонент 1

За кого е предназначен този курс:

Курсът е предназначен за:

- Мрежови администратори
- Мрежови инженери
- Мениджъри на мрежи
- Системни инженери

Материали

Участниците в курса ще получат набор от учебни материали, необходими за провеждането на курса. Материалите ще бъдат на български и/или английски език.

Начин на провеждане на обучението

- Местоположение – Учебни зали на Изпълнителя или по искане на Възложителя в зали на МВнР.
- Продължителност – 3 дни
- Обучението ще се провежда по 5 учебни часа на ден

Обучението ще бъде на български език.

Съдържание на курса

Cisco ONS 15454E

- Запознаване с процедурата за Безопасност при работа и поддръжка
- Запознаване с най-добрите практики за поддръжка на оборудването
- Запознаване с необходимия набор от команди за откриване на софтуерни и хардуерни проблеми в устройствата
- Запознаване с различните видове хардуерни и софтуерни грешки
- Запознаване с основните процедури за откриване на различните типове грешки
- Запознаване с основните процедури за отстраняване на възникналите грешки
- Запознаване с процедурата за аварийно изключване на устройствата
- Запознаване с процедурата за привеждане в нормална робота на изключени устройства
- Запознаване с процедурите за монтаж и демонтаж на допълнителни модули, вентилатори и захранвания и др. компоненти
- Запознаване с процедурата за архивиране на конфигурации и операционни системи
- Запознаване с процедурите за възстановяване на софтуерната функционалност (Configuration Recovery, System Recovery, Password Recovery и др.)

- Практически упражнения

Cisco ASR 1006 VPN+FW Bundle w/ ESP-20G, RP2, SIP10, AESK9 License

- Запознаване с процедурата за Безопасност при работа и поддръжка
- Запознаване с най-добрите практики за поддръжка на оборудването
- Запознаване с необходимия набор от команди за откриване на софтуерни и хардуерни проблеми в устройствата
- Запознаване с различните видове хардуерни и софтуерни грешки
- Запознаване с основните процедури за откриване на различните типове грешки
- Запознаване с основните процедури за отстраняване на възникналите грешки
- Запознаване с процедурата за аварийно изключване на устройствата
- Запознаване с процедурата за привеждане в нормална работа на изключени устройства
- Запознаване с процедурите за монтаж и демонтаж на допълнителни модули, вентилатори и захранвания и др. компоненти
- Запознаване с процедурата за архивиране на конфигурации и операционни системи
- Запознаване с процедурите за възстановяване на софтуерната функционалност (Configuration Recovery, System Recovery, Password Recovery и др.)
- Практически упражнения

Cisco MDS 9513 Multilayer Director

- Запознаване с процедурата за Безопасност при работа и поддръжка
- Запознаване с най-добрите практики за поддръжка на оборудването
- Запознаване с необходимия набор от команди за откриване на софтуерни и хардуерни проблеми в устройствата
- Запознаване с различните видове хардуерни и софтуерни грешки
- Запознаване с основните процедури за откриване на различните типове грешки
- Запознаване с основните процедури за отстраняване на възникналите грешки
- Запознаване с процедурата за аварийно изключване на устройствата
- Запознаване с процедурата за привеждане в нормална робота на изключени устройства
- Запознаване с процедурите за монтаж и демонтаж на допълнителни модули, вентилатори и захранвания и др. компоненти
- Запознаване с процедурата за архивиране на конфигурации и операционни системи
- Запознаване с процедурите за възстановяване на софтуерната функционалност (Configuration Recovery, System Recovery, Password Recovery и др.)
- Практически упражнения

Cisco ASA 5580-20 Appliance with 4 GE, Dual AC, 3DES/AES

- Запознаване с процедурата за Безопасност при работа и поддръжка
- Запознаване с най-добрите практики за поддръжка на оборудването
- Запознаване с необходимия набор от команди за откриване на софтуерни и хардуерни проблеми в устройствата
- Запознаване с различните видове хардуерни и софтуерни грешки
- Запознаване с основните процедури за откриване на различните типове грешки

- Запознаване с основните процедури за отстраняване на възникналите грешки
- Запознаване с процедурата за аварийно изключване на устройствата
- Запознаване с процедурата за привеждане в нормална робота на изключени устройства
- Запознаване с процедурите за монтаж и демонтаж на допълнителни модули, вентилатори и захранвания и др. компоненти
- Процедури за мониторинг на Cisco ASA чрез Java базиран софтуер ASDM
- Процедури за инсталиране и надграждане на софтуера на ASA чрез TFTP
- Практически упражнения

Cisco Catalyst 3560 Switches

- Запознаване с процедурата за Безопасност при работа и поддръжка
- Запознаване с най-добрите практики за поддръжка на оборудването
- Запознаване с необходимия набор от команди за откриване на софтуерни и хардуерни проблеми в устройствата
- Запознаване с различните видове хардуерни и софтуерни грешки
- Запознаване с основните процедури за откриване на различните типове грешки
- Запознаване с основните процедури за отстраняване на възникналите грешки
- Запознаване с процедурата за аварийно изключване на устройствата
- Запознаване с процедурата за привеждане в нормална робота на изключени устройства
- Запознаване с процедурата за архивиране на конфигурации и операционни системи
- Запознаване с процедурите за възстановяване на софтуерната функционалност (Configuration Recovery, System Recovery, Password Recovery и др.)
- Практически упражнения

Cisco Catalyst 6500 WS-C6513

- Запознаване с процедурата за Безопасност при работа и поддръжка
- Запознаване с най-добрите практики за поддръжка на оборудването
- Запознаване с необходимия набор от команди за откриване на софтуерни и хардуерни проблеми в устройствата
- Запознаване с различните видове хардуерни и софтуерни грешки
- Запознаване с основните процедури за откриване на различните типове грешки
- Запознаване с основните процедури за отстраняване на възникналите грешки
- Запознаване с процедурата за аварийно изключване на устройствата
- Запознаване с процедурата за привеждане в нормална робота на изключени устройства
- Запознаване с процедурите за монтаж и демонтаж на допълнителни модули, вентилатори и захранвания и др. компоненти
- Запознаване с процедурата за архивиране на конфигурации и операционни системи
- Запознаване с процедурите за възстановяване на софтуерната функционалност (Configuration Recovery, System Recovery, Password Recovery и др.)
- ACE Модул за Cisco 6500 Switch – функционалност, диагностика, откриване и отстраняване на проблеми.
- Практически упражнения

Конфигурация и администриране на сървърната и лентова инфраструктура от Компонент 2 и новото оборудване

За кого е предназначен този курс:

Курсът е предназначен за:
- Системни администратори
- Мрежови инженери
- Мениджъри на сървери
- Системни инженери

Очаквани резултати в края на курса:

След завършване на курса участниците ще имат познания за работа с Blade и лентовите системи на IBM и Lenovo, което ще им позволи да лесно да диагностицират и оперативно да отстраняват възникнали проблеми със съществуващото оборудване, както и да наблюдават, конфугурират и управляват новодоставеното оборудвана.

Съдържание на курса

Тема 1: Запознаване с IBM/Lenovo Blade Center H
- Какво е Blade шасито и за какво служи
- Основни компоненти на шасито
  - Слотове за блейд сървъри
  - Слотове за разширителни модули
  - Захранващи блокове
  - Охлаждащи блокове
  - AMM управляващ модул
- Инсталация и конфигурация на IBM Blade Center H
- Управление на шасито чрез AMM модул
- Идентифициране и отстраняване на проблеми

Тема 2: Запознаване с Lenovo Flex System Enterprise Chassis
- Какво е Flex шасито и за какво служи
- Основни компоненти на шасито
  - Слотове за модулни сървъри
  - Слотове за комуникационни модули
  - Захранващи блокове
  - Охлаждащи блокове
  - CMM управляващ модул
- Инсталация и конфигурация на с Lenovo Flex System Enterprise Chassis
- Управление на шасито чрез CMM модул
- Идентифициране и отстраняване на проблеми

Тема 3: Запознаване с IBM/Lenovo BladeCenter HS22
- Какво представлява IBM/Lenovo BladeCenter HS22
- Основни компоненти на сървъра
  - Слотове за памет
  - Типове CPU
  - Слотове за HDD
- Инсталация и конфигурация на IBM/Lenovo BladeCenter HS22
- Идентифициране и отстраняване на проблеми

Тема 4: Запознаване с Lenovo Flex System x240 M5 Compute Node

- Какво представлява Flex System x240 M5 Compute Node
- Основни компоненти на сървъра
  - Слотове за памет
  - Типове CPU
  - Слотове за HDD
  - Комуникационни модули – LAN, SAN
- Инсталация и конфигурация на Flex System x240 M5 Compute Node
- Идентифициране и отстраняване на проблеми

Тема 5:

- Лентови библиотеки
- Общо описание на лентовата библиотека и спецификации
- Разширяване на лентовата библиотека
- Компоненти на предния панел
- Компоненти на задния панел
- Вътрешни компоненти
- Управление на лентовата библиотека
- Multipath архитектура
- Работа с логически библиотеки
- Запознаване със спецификите на новите TS3200 Tape Library

Програма за обучение IBM Tivoli Storage Manager
Курс съгласно официалната програма за IBM TSM Advanced administration, tuning and troubleshooting

Course #: TS623BG
IBM Tivoli Storage Manager 7.1 Advanced Admin, Tuning, Troubleshooting Training

Обучение за придобиване на задълбочени знания и развиване на експертни умения за администриране, настройка и решаване на проблеми в IBM Tivoli Manager 7.1.
Това е курс за напреднали, предназначен за опитни системни администратори и сторидж специалисти със съществени познания за IBM Tivoli Storage Manager.
Участниците ще бъдат обучени как да контролират и настройват Tivoli Storage Manager средата и какви стъпки да предприемат при възникване на проблем.
По време на предвидените лабораторни упражнения се изучават методите и вариантите за управление на бази данни DB2, посредством използване на план за възстановяване и SQL скриптове. Използват се множество сървъри, които да симулират среда на голяма организация.
Курсистите работят в групи за решаване на проблеми, за изпълнение на процеси по съхранение, възстановяване и оптимизация управлението, дедупликация на данни, както и за постигане на оптимална производителност при настройка на бекъп-архив клиент и Tivoli Storage Manager 7.1 сървър.
Обучението обхваща последните новости на продукта Tivoli Storage Manager с ново маркетингово име IBM Spectrum Protect V7.1.3 като дедупликейшън технология, подобрения в оперативния център и нови командни параметри.

Кратко съдържание на курса:

1. Tivoli Storage Manager 7.1 – концепции и общ преглед
2. Управление на бази данни и логове за напреднали
3. Управление на сторидж дискове за напреднали
4. Методологии за копиране, архивиране и възстановяване на данни
5. Автоматизация и скриптиране
6. Повишаване на производителността
7. Конфигуриране и управление на системите в организацията
8. Възстановяване от произшествия, инциденти и бедствия.
9. Управление на сигурността в Tivoli Storage Manager
10. Установяване на проблем
11. Tivoli Storage Manager и IBM Spectrum Protect 7.1.3 – разлики

Програма за обучение администриране на Steria Interconnection Box for VIS и Steria CompliTT

Тема 1
Администриране на Oracle Web Logic Application Servers и приложенията, работещи в тяхната среда и Сигурност на информацията

1. Oracle Fusion Middleware среда и компоненти
   - Oracle WebLogic Server;
2. Работа с инструменталните средства за управление
   - Работа с инструменталните средства за управление.
   - Конфигуриране на журналирането и използване на система за преглед на журнали Logviewer;
   - Операции за архивиране и възстановяване на сървъра за приложения.
3. Сигурност на информацията
   - Добри практики за сигурност на информационните системи.
   - Прилагане на политики и процедури за сигурност на информацията.
4. Практическа част – 2 учебни часа
   4.1. Администриране на Oracle Web Logic Application Servers
   - Конфигуриране на журналирането и използване на система за преглед на журнали Logviewer;
   - Операции за архивиране и възстановяване на сървъра за приложения.

Тема 2
Поддръжка и администриране на специализирания софтуер на Steria: SIB (Steria Interconnection Box for VIS) заедно с Administration User Interface (Admin UI), Steria CompliTT Testing Tool
1. Инсталация и конфигуриране
   - Инсталиране и пускане в експлоатация на програмните компоненти
   - Конфигуриране на файловете с параметри
   - Стартиране, спиране и рестарт на приложенията
   - Управление на потребители/потребителски роли за аутентикация и оторизация (Authentication and Autorization) създаване/премахване на роли, свързването им с потребители, промяна на пароли
2. Мониторинг на приложенията
   - Одит на лога със съобщения (MessageLog) в администраторския потребителски интерфейс (Admin UI)
   - Проверка на събития в системата
3. Практическа част – 2 учебни часа
   3.1. Мониторинг
   - Одит на лога със съобщения (MessageLog) в администраторския потребителски интерфейс (Admin UI)
   - Проверка на събития в системата
   3.2. Тестване на работоспособността
   - Работа с CompliTT
   - Търсене на грешки във файл със SIB лог
   - Проверка на XML отчет и как да се провери дали нотификацията за оповестяването е препратена коректно до Националната система

Тема 3
1. Тестване на работоспособността на приложението
   - Стартиране и разчитане на тестове с CompliTT
   - Проверка на логове и анализиране на случаи на неуспешно изпълнени тестове
   - Одит на лога със съобщения (MessageLog) в базата данни
2. Практическа част – 2 учебни часа

Програма за обучение администриране на СУБД IBM Informix
Informix database administration training

Course #: IX222BG

Informix Informix 11.7 Database Administration Training

Обучение за придобиване на знания и развиване на умения за администриране на сървъри за бази данни Informix 11.7
Курсът е предназначен да запознае обучаемите с базовите концепции на управлението на данни в Informix. Курсистите ще придобият знания как да определят точните типове данни; как да създават, управляват и поддържат таблици и индекси; ще бъдат запознати с начина на работа на оптимизатора в Informix; ще придобият умения за управление на данни и употреба на функцията SET EXPLAIN за определяне ефективността на заявките.

Кратко съдържание на курса:

1. Въведение в Informix терминологията
2. Типове данни в Informix
3. Създаване на бази данни и таблици
4. Промяна и изтриване на база данни и таблици
5. Създаване, промяна и изтриване на индекси
6. Управление и поддържане на индекси
7. Разпределение на таблици и индекси
8. Поддържане разпределението на таблици и индекси
9. Оптимизатор на заявки на база разход на ресурси
10. Обновяване на статистиките и разпределението на данните
11. Управление на оптимизатора
12. Цялост на връзките и интегритет
13. Управление на ограничения
14. Режими на работа и откриване на нарушения
15. Контрол на едновременния достъп
16. Сигурност на данните
17. Изгледи
18. Въведение в съхранените процедури
19. Тригери

Програма за обучение „Администриране и конфигуриране на Microsoft Windows Server и Active Directory, Администриране и конфигуриране на Microsoft System Center и Hyper-v, Администриране и конфигуриране на Microsoft Exchange Server"

Продължителност: 3 дни по 8 учебни часа дневно или 6 дни по 4 учебни часа дневно

Учебен ден: Обучението е целодневно, започва в 9:30 и приключва в 17:30 ч.

Метод на обучение: Присъствена (24 уч. часа) с включена теория и практика

Програма:

Ден 1:

- Инсталация и базова конфигурация на Windows Server 2012 R2
- Преглед на управлението на Windows Server 2012 R2
- Управление на инфраструктурните роли на Windows Server 2012 R2
- Управление на Active Directory Domain Services
- Създаване и управление на обекти на групови политики
- Наблюдение, бекъп и възстановяване на Windows Server 2012 R2 и Active Directory

Ден 2:

- Инсталация и базова конфигурация на Windows Server 2012 R2 Hyper-V роля
- Създаване и управляване на виртуални твърди дискове, виртуални машини и виртуални мрежи
- Конфигуриране и управление на failover клъстери с Hyper-V
- Конфигуриране и управление на Hyper-v клъстери и ресурси с Microsoft System Center 2012 R2 Virtual Machine Manager
- Конфигуриране и управление на Hyper-v сървъри и виртуални машини с Microsoft System Center Configuration Manager 2012 R2

Ден 3:

- Инсталация и базова конфигурация на Exchange Server 2013
- Управление на получатели
- Управление на клиентски достъп
- Управление на пренос на съобщенията
- Осигуряване на висока надеждност и наличност (DAG)
- Бекъп и възстановяване на бази и сървъри

Програма за обучение ITIL Foundation

За кого е предназначен:

ITIL Foundation е подходящ за всеки, който работи в областта на ИТ, който иска да придобие повече знания за най-добрите практики в управлението на ИТ процеси.

Съдържание на курса:

Service Strategy, която разглежда основните бизнес цели и очаквания за да се убеди, че ИТ стратегията е в унисон с бизнес стратегията на организацията
Service Design, който стартира с набор от нови бизнес изисквания и завършва с разработка на решение, проектирано да посрещне бизнес нуждите на организацията
Service Transition, отговорен за управлението на промените, рисковете и осигуряване на качеството и има за цел да внедри услугите в експлоатационната среда планирано и с минимално прекъсване на услугите
Service Operation, обхващащ ежедневните дейности в работата на услугите
Continual Service Improvement, който обхваща всички останали елементи и търси начини за подобрение на услугите и осигуряване на процесите

Очаквани резултати:

Усвояване на добрите практиките и теорията за подобряване на работата в ИТ отделите.ITIL обхваща практиките, дейностите, структурите и отговорностите в целия цикъл на създаване на ИТ услуги. Покриване на 100 % изискванията за успешно преминаване на изпит ITIL Foundation.

Програма:

Ден 1:

- Въведение
- Практическо управление на услуги
- Стратегия на услуги (Service Strategy)
- Изграждане на услуги (Service Design)

Ден 2:

- Кратък преглед на Ден 1
- Промяна на услуги (Service Transition)
- Изпълнение на услуги (Service Operation)

Ден 3:

- Кратък преглед на Ден 2
- Подобрение на услуги (Continual Service Improvement)
- ITIL квалификационна схема
- Преговор и проверка на знанията
- Оценка на курса

Дата: 25.05.2016
Представляващ ДЗЗД Ай Би Ес Индекс, съгласно Договор за консорциум от 19.05.2016,
Горан Ангелов, Управител на Водещ съдружник Ай Би Ес – България ЕООД:

(печат на Водещ съдружник, съгласно т. 3.5. от Договор за консорциум от 19.05.2016)

Приложение 2

Техническо предложение за осъвременяването на оборудването по Компонент 2

към

ТЕХНИЧЕСКА ОФЕРТА

за участие в открита процедура за възлагане на обществена поръчка с предмет: “Поддръжка и обновяване на програмното и техническо осигуряване на Националната визова информационна система и на визовата дейност в консулските служби на Р България”,

Обособена позиция 1: „Поддръжка и осъвременяване на техническото осигуряване и инфраструктурата на НВИС“

От КОНСОРЦИУМ ДЗЗД „Ай Би Ес Индекс”

Предложението ни е базирано на най-новото поколение блейд шасита на Lenovo - **Lenovo Flex System Enterprise Chassis**. В основновния и в резервния дейта център предвиждаме инсталиране на по едно блейд шаси с инсталирани съответно 14 и 10 броя блейд сървъри - **Flex System x240 M5 Compute Node**.

Блейд сървърите предвиждаме да са с по 2 броя 16 ядрени процесори и по 256GB RAM, като по този начин ще успеем да консолидираме съществуващите 4 броя блейд шасита с 35 броя сървъри в основния център и 3 броя блейд шасита с 20 броя в резервния център.

При тази конфигурация ще се получи многократно оптимизиране на ресурсите, консумацията на електроенергия, място в сървърните шкафове, управлението на оборудването.

Лентовите библиотеки за архивиране също са базирани върху най-новите технологии - **TS3200 Tape Library** с инсталирани LTO Ultrium 7 устройства. Предвиждаме инсталиране на по една библиотека в основния и в резервния сайт, като тази в основния е с 4 LTO Ultrium 7 устройства, а тази в резервния – с 2 LTO Ultrium 7. Капацитета за запис на една касета без компресия е 6TB, а скоростта на трансфер е 300Mbs.

При тази конфигурация се намалява броя на устройствата и броя на касетите необходими за архивиране.

Предложеното оборудване ще е ново, неупотребявано и в текущата производствена листа на производителя Lenovo.

Предлаганото оборудване ще бъде произведено съгласно прилагането на стандарта за качество ISO 9001:2000. Приложен е сертификат ISO 9001:2000 на съответния производител - Lenovo.

Електрическо захранване – цялото оборудване ще е пригодно за работа с електрическо захранване в Република България – 220 V / 50 Hz

Шаси за модулни сървъри – 2 бр. Lenovo Flex System Enterprise Chassis,; Part. No: 8721ALG	
Капацитет за модулни сървъри:	Има възможност за добавяне до 14 модулни сървъра
Капацитет за комуникационни модули:	Има възможност за добавяне до 4 комуникационни модула.
Размери:	10U, подходящо за монтаж в сървърен шкаф
Захранвания:	N+1 (при пълно със сървъри шаси) резервирани заменяеми по време на работа захранващи модули, където N е 5. Общ максимален брой захранващи модули – 6.
Охлаждане:	N+1 (при пълно със сървъри шаси) резервирани, заменяеми по време на работа вентилатори, способни да поемат охлаждането на шасито при пълно натоварване, където N е 9. Общ максимален брой охлаждащи модули – 10.
Поддържани процесорни архитектури:	Поддържа 2 вида процесорна архитектура на модулните сървъри в шасито – x86 и IBM Power. Поддържа инсталиране на еднопроцесорни, двупроцесорни, четирипроцесорни и осемпроцесорни модулни сървъри.
Ethernet свързаност:	Ще се инсталират подходящи модули, които да осъществят свързаност между новите модулни блейд сървъри и съществуващата LAN инфраструктура. Модулите ще са резервирани – 2 броя
SAN свързаност:	Ще се инсталират подходящи модули, които да осъществят свързаност между новите модулни блейд сървъри и съществуващата SAN инфраструктура. Модулите ще са резервирани – 2 броя
Управление:	Шасито разполага с 2 броя резервирани модули за отдалечено управление и наблюдение на всички компоненти на шасито, сървърите и модулите за свързаност - Lenovo Flex System Redundant Chassis Management Module 2; Part. No: 00FJ669 Вид на мрежата за управление - 1Gb
Диагностика:	Възможност за записване на генерирани грешки.
Резервираност:	Всички компоненти в шасито са сменяеми по време на работа и максимално резервирани, за да се избегне съществуването на единична точка на отказ
Поддръжка	3 години на място

Модулни сървъри – 24 бр. Lenovo Flex System x240 M5 Compute Node; Part. No: 9532	
Размери:	Напълно съвместими с предлаганото блейд шаси
Процесори:	2 бр. Intel Xeon със следните параметри: Архитектура – x86; Брой ядра – мин 16 физически ядра на процесор без използване на Hyper-threading; Номинална честота на процесора – мин 2.1GHz L3 кеш на процесор – мин 40 MB Брой на QPI интерфейсите – 2 Скорост на QPI интерфейсите – 9.6 GT/s
Памет:	Инсталирани 256GB Registered мин 2133MHz DDR4, 24 слота (по 12 за процесор), има свободни 8 слота за бъдещо разширение. Максимална поддържана памет до 1.5 TB с 24x 64 GB LRDIMM.
Дисков контролер:	Вграден SAS/SATA RAID контролер, с поддръжка на RAID 0,1
Инсталирани дискове:	2 броя с капацитет 300GB и скорост на въртене 15 000 оборота в минута.
Мрежови адаптер:	Инсталиран мрежови адаптер с 2 порта. Всеки порт поддържа 10Gbit Ethernet - Flex System EN4172 2-port 10Gb Ethernet Adapter; Part. No: 00AG530.
Оптичен адаптер:	Инсталиран Fiber Channel адаптер с 2 порта. Всеки порт да поддържа 16Gbps Fibre Channel - Flex System FC5172 2-port 16Gb FC Adapter; Part. No: 69Y1942
Управление:	Вграден чип за отдалечено управление/наблюдение интегриращ се с модулите за управление на шасито - Integrated Management Module 2 (IMM2) with Renesas SH7758 controller, .
Диагностика:	Светлинна диагностика при възникване на проблем (light path diagnostics panel), софтуер за наблюдение (remote presence), вградена диагностика, софтуер за събиране на сервизна информация (Predictive Failure Analysis).

Лентова библиотека тип 1 – 1 брой TS3200 Tape Library Model L4U; Part. No: 61734UL	
Шаси	Поддържа до 4 броя Half-High LTO 5, 6, 7 лентови устройства
Инсталирани лентови устройства	Инсталирани 4 броя LTO лентови устройства LTO Ultrium 7 Half High Fibre Drive Sled; Part. No: 00WF769
Интерфейс на лентовите устройства	Наличен по 1 брой Fibre Channel интерфейс на всяко инсталирано лентово устройство
Трансфер на данни	Всяко устройство поддържа до 300 MBps трансфер на данни (при LTO 7) без използване на компресия.
Включени лентови касети	Включени 50 броя лентови касети с капацитет 6TB без компресия
Лентова библиотека тип 2 – 1 брой TS3200 Tape Library Model L4U; Part. No: 61734UL	
Шаси	Поддържа до 4 броя Half-High LTO 5, 6, 7 лентови устройства
Инсталирани лентови устройства	Инсталирани 2 броя LTO лентови устройства LTO Ultrium 7 Half High Fibre Drive Sled; Part. No: 00WF769
Интерфейс на лентовите устройства	Наличен 1 брой Fibre Channel интерфейс на всяко инсталирано лентово устройство
Трансфер на данни	Всяко устройство поддържа минимум 300 MBps трансфер на данни (при LTO 7) без използване на компресия.
Включени лентови касети	Включени 50 броя лентови касети с капацитет 6TB без компресия

Услуги, които ще извършим след доставката на оборудването:

Целият хардуер, компоненти, модули, части и софтуерни продукти ще се инсталират и тестват, за да се валидира тяхната функционалност, в работните помещения на Възложителя.

Изпълнителят ще свърже логически и физически доставеното оборудване към наличната SAN среда.

Изпълнителят ще подготви документация за изграденото решение, която да съдържа логическата и физическата свързаност на устройствата към SAN и LAN мрежата.

Оборудването ще бъде доставено в рамките на 2 месеца след приемане на първоначалния доклад

Оборудването ще бъде инсталирано и пуснато в експлоатация до 1 месец след неговата доставка. Инсталацията ще бъде направена в основния и резервния център за управление на данни.

Изпълнителят ще мигрира системите към ново инсталираните изчислителни мощности съгласно приетия план за дейностите от Възложителя, но не по-късно от 3 месеца след неговата инсталация.

Гаранционният срок от производителя на новодоставеното оборудване ще бъде до 31.12.2019 г.

Дата: 25.05.2016

Представляващ ДЗЗД Ай Би Ес Индекс, съгласно Договор за консорциум от 19.05.2016,

Горан Ангелов, Управител на Водещ съдружник Ай Би Ес – България ЕООД:

(печат на Водещ съдружник, съгласно т. 3.5. от Договор за консорциум от 19.05.2016)

Приложение 3

План - Програма за изпълнение на дейностите съгласно изискванията на Техническата спецификация

КЪМ

ТЕХНИЧЕСКА ОФЕРТА

за участие в открита процедура за възлагане на обществена поръчка с предмет: "Поддръжка и обновяване на програмното и техническо осигуряване на Националната визова информационна система и на визовата дейност в консулските служби на Р България",

Обособена позиция 1: „Поддръжка и осъвременяване на техническото осигуряване и инфраструктурата на НВИС“

От КОНСОРЦИУМ ДЗЗД „Ай Би Ес Индекс"

1. Анализ на текущото състояние на всички компоненти на системата - до 30 календарни дни след сключване на договора за поддръжка и след това веднъж годишно до края на договора – 31.12.2019 г
   1.1. Анализ на мрежовата инфраструктура и комуникациите
2. Планиране на дейностите по поддръжка и обновяване на системите - до 7 календарни дни след извършване на анализа от т. 1. и след това веднъж годишно до края на договора
3. Осигуряване 24/7 техническа поддръжка – през целия срок на договора
4. Ремонт на дефектирали хардуерни устройства - до 15 работни дни след извършване на анализа от т. 1., а след това спрямо нивото на критичност на устройството/ компонента за срока на договора – 31.12.2019 г
5. Профилактика на оборудването - До 30 дни след сключване на договора за възлагане на поръчката, а след това веднъж годишно до края на договора – 31.12.2019 г
6. Поддръжка на Компоненти 1, 2 и 3 - мрежова, сървърна, лентова и дискова инфраструктури – За целия срок на договора или извеждане на оборудването от употреба
7. Поддръжка на Компонент 4 - Софтуер за архивиране и възстановяване, софтуер за наблюдение и софтуер за управление - За целия срок на договора или извеждане на системните инструменти от употреба
8. Поддръжка на Компонент 5 - Специализиран софтуер SIB (Steria Interconnection Box for VIS), Oracle Database Servers, Oracle Weblogic Application Servers и специализиран софтуер CompliTT - За целия срок на договора или извеждане на специализирания софтуер от употреба
9. Поддръжка на Компонент 6 - Приложен софтуер на НВИС и система за управление на базата от данни IBM Informix, използвана от централната компонента на НВИС - За целия срок на договора или извеждане на приложния софтуер от употреба
10. Поддръжка на Компонент 7 - Системен софтуер на Microsoft (Windows Server 2012/ 2012 R2, Microsoft Exchange Server 2013, Microsoft System Center 2012 R2 Virtual Machine Manager и Microsoft System Center 2012 R2 Configuration Manager) - За целия срок на договора или извеждане на системния софтуер от употреба
11. Осъвременяване на оборудването по Компонент 2
    11.1. Доставка – до 2 месеца след приемане на първоначалния доклад по т.1
    11.2. Инсталация и пускане в експлоатация - 1 месец след доставката
    11.3. Мигриране на системите към ново инсталираните изчислителни мощности – до 3 месеца след инсталацията
12. Обучение
    12.1. Конфигурация и администриране на мрежовата и комуникационна инфраструктура от Компонент 1 – 3 дни
    12.2. Конфигурация и администриране на сървърната и лентова инфраструктура от Компонент 2 и новото оборудване – 3 дни
    12.3. IBM Tivoli Storage Manager - Курс съгласно официалната програма за IBM TSM Advanced administration, tuning and troubleshooting – 5 дни

12.4. Администриране на Steria Interconnection Box for VIS и Steria CompliTT – 3 дни
12.5. Администриране на СУБД IBM Informix - Informix database administration training – 4 дни
12.6. Администриране и конфигуриране на Microsoft Windows Server и Active Directory, Администриране и конфигуриране на Microsoft System Center и Hyper-v, Администриране и конфигуриране на Microsoft Exchange Server – 3 дни
12.7. ITIL Foundation – 3 дни

Задача	Q3-16	Q4-16	Q1-17	Q2-17	Q3-17	Q4-17	Q1-18	Q2-18	Q3-18	Q4-18	Q1-19	Q2-19	Q3-19	Q4-19
Анализ на текущото състояние на всички компоненти на системата														
Планиране на дейностите по поддръжка и обновяване на системите														
Осигуряване 24/7 техническа поддръжка														
Ремонт на дефектирали хардуерни устройства														
Профилактика на оборудването														
Поддръжка на Компоненти 1, 2 и 3														
Поддръжка на Компонент 4														
Поддръжка на Компонент 5														
Поддръжка на Компонент 6														
Поддръжка на Компонент 7														
Осъвременяване на оборудването по Компонент 2														
Обучение:														
Компонент 1														
Компонент 2														

IBM Tivoli Storage Manager				[redacted]										
Steria		[redacted]												
Informix			[redacted]											
Microsoft				[redacted]										
ITIL Foundation	[redacted]													

Дата: 25.05.2016
Представляващ ДЗЗД Ай Би Ес Индекс, съгласно Договор за консорциум от 19.05.2016,
Горан Ангелов, Управител на Водещ съдружник Ай Би Ес – България ЕООД:

(печат на Водещ съдружник, съгласно т. 3.5. от Договор за консорциум от 19.05.2016)

Приложение №4

Подход и методика за управление на изпълнението на предмета на обществената поръчка

към

ТЕХНИЧЕСКА ОФЕРТА

за участие в открита процедура за възлагане на обществена поръчка с предмет: "Поддръжка и обновяване на програмното и техническо осигуряване на Националната визова информационна система и на визовата дейност в консулските служби на Р България",

Обособена позиция 1: „Поддръжка и осъвременяване на техническото осигуряване и инфраструктурата на НВИС“

От КОНСОРЦИУМ ДЗЗД „Ай Би Ес Индекс”

СЪДЪРЖАНИЕ

ИЗПОЛЗВАНИ ТЕРМИНИ И СЪКРАЩЕНИЯ

Съкращение / Термин	Значение
PMI	Project Management Institute
Възложител	Министерство на външните работи
Изпълнител	ДЗЗД „Ай Би Ес Индекс”
ИТ	Информационни технологии
ТС	Технически спецификации по обществената поръчка

1. ВЪВЕДЕНИЕ

Настоящият документ е разработен възоснова на поставените изисквания в документацията за участие в открита процедура с предмет "Поддръжка и обновяване на програмното и техническо осигуряване на Националната визова информационна система и на визовата дейност в консулските служби на Р България", Обособена позиция 1: „Поддръжка и осъвременяване на техническото осигуряване и инфраструктурата на НВИС“.

Целта на този документ е да се опише реализация на поръчката, като се представят организацията и методологията за изпълнение на поръчката, както и подходът за изпълнение на дейностите по поръчката.

2. ОРГАНИЗАЦИЯ И МЕТОДОЛОГИЯ ЗА РЕАЛИЗАЦИЯ НА ПОРЪЧКАТА

2.1. Подход, методология и планирани действия

Специалистите на Изпълнителя разполагат със значителен опит и ноу-хау в решения за големи организации с комплексна инфраструктура и работни процеси.

Множеството реализирани проекти, както и сертификациите ни по ISO9001:2008, ISO 20000:2011 и ISO27001:2005 гарантират за качеството на предоставяните услуги. Визията на Изпълнителя за реализация на този проект включва адаптирането на най-добрите практики при доставката на оборудване и софтуерни лицензи, услуги по инсталация, конфигурация и миграция на комплексни ИТ системи, поддръжка и профилактика на инфраструктурни и софтуерни системи.

2.1.1. Общи положения

Изпълнителят предлага използването на методологията на PMI (Project Management Institute) за цялостното управление на проекта. По-долу са описани принципите на тази методология, базирана на Project Management Body of Knowledge (PMBOK).

Project Management Body of Knowledge (PMBOK) е сбор от процеси и сфери на знание, широко приети като най-добра практика в дисциплината —Управление на проекти. Този международно признат стандарт (IEEE Std 1490-1998) е основата на управлението на проекти. Според PMBOK съществуват 5 основни групи процеси (стартиране, планиране, изпълнение, проследяване и контрол, приключване) и 9 сфери на знание (управление на интеграцията на проекта, на обхвата, на времето, на разходите, на качеството, на човешките ресурси, на комуникациите, на риска и на доставките). Във всеки проект или фаза процесите се застъпват и си взаимодействат. Те се описват от гледна точка на вход (документи, планове, проекти), инструменти и техники (механизми, прилагани върху входящите данни) и изход (документи, продукти, резултати).

Основните цели на методологията на PMI са:

- Контролиране на обхвата, графика, разходите и качеството;
- Намаляване и управляване на риска;
- Управление на ресурсите;
- Идентифициране на дейностите по проекта;

- Координиране на комуникациите между заинтересованите страни;
- Съобразяване на работата с бизнес целите на Възложителя.

За постигане на горните цели методологията е съсредоточена върху следните 9 сфери на знание:

- Управление на интеграцията;
- Управление на обхвата;
- Управление на времето;
- Управление на разходите;
- Управление на качеството;
- Управление на човешките ресурси;
- Управление на комуникациите;
- Управление на риска;
- Управление на доставките;

2.1.2. Фази

Проследяването и контролът се извършва през целия проект и включва процесите, необходими за стартирането, планирането, изпълнението и приключването на проекта в съответствие с целите, зададени в обхвата и плана за управление на проекта.

Всяка група процеси се състои от един или повече управленски процеси. Групите са свързани – често изходът на даден процес се превръща във вход на друг. При централните групи процеси има итерация на връзките — планирането осигурява на изпълнението първоначален документиран план на проекта, след което осигурява актуализации на плана в хода на работата.

Процесите по управление на проекта са организирани в следните групи:

2.1.2.1. Фаза 1: Анализ на текущото състояние (веднъж годишно)

Анализ на текущото състояние и планиране на доставките и всички дейности, необходими за реализация на спецификацията. Дейността завършва с доклад, който включва:

- Описание на съществуващите конфигурации и практики;
- Анализ на откритите проблеми и препоръки за тяхното отстраняване;
- Подробен план за реализация на необходимите дейности по проекта.

2.1.2.2. Фаза 2: Извършване на доставки (за целия срок на договора)

Извършване на всички доставки за подмяна на оборудване при необходимост съгласно предварително одобрен план от Възложителя. Дейността завършва с доклад, който включва:

- Протоколи за извършените доставки;
- Договорите за гаранционна поддръжка със съответните доставчици, съгласно изискванията на Техническата спецификация.

2.1.2.3. Фаза 3: Извършване на дейности по инсталация, конфигурация, отстраняване на проблеми, реализиране на възложени промени (за целия срок на договора)

Извършване на всички дейности по инсталация конфигурация, отстраняване на проблеми, реализиране на възложени промени на хардуер и софтуерни продукти. Дейността завършва с доклад, който включва:

- Протоколи за приемане на извършените промени и/или нови инсталации;

- Подробно описание на промените.

2.1.2.4. Фаза 4: Провеждане на обучения (за целия срок на договора)

Провеждане на обучения. Дейността завършва с доклад, който включва:

- Присъствени списъци, анкетни карти и протокол за провеждането на всяко обучение;
- Описание на проведените обучения и анализ на постигнатите резултати.

2.1.2.5. Фаза 5: Систематизиране и актуализация на съществуващата документация (за целия срок на договора)

Систематизиране и актуализация на съществуващата документация, както и изготвяне на липсващи документи и ръководства. Новите документи трябва да включват: инсталационна инструкция, инструкция за експлоатация, инструкции за архивиране и възстановяване на средите.Дейността завършва с доклад, който включва:

- Каталог на съществуващите документи;
- Описание на направените промени;
- Описание на изготвените нови документи.

2.1.3. Сфери на управление

Следва описание на деветте сфери на управление съгласно стандарта на PMI:

2.1.3.1. Управление на интеграцията

Процесите по управление на интеграцията гарантират правилната координация на различните елементи на проекта. Те включват балансиране на целите и алтернативите с оглед на нуждите и очакванията на заинтересованите страни. Описаните в тази глава процеси са предимно интегративни.

Разработване на план на проекта

При разработването на плана на проекта се използват резултатите от други планиращи процеси, включително стратегическо планиране, за да се създаде един ясен и последователен документ, който да насочва и изпълнението, и контрола на проекта. Този процес минава през няколко итерации. Сборът от всички интегрирани планове за управленски контрол съставлява обхвата на проекта.

Изпълнение на плана на проекта

Изпълнението на плана на проекта е основен процес при осъществяването на плана – преобладаваща част от бюджета и усилията по проекта се изразходват при извършването на този процес. Чрез него ръководителят на проекта и неговия екип координират и насочват техническите и организационните интерфейси. В рамките на този процес фактически се създава продуктът на проекта. Изпълнението постоянно ще се сравнява с основния план на проекта, за да се вземат своевременни корективни мерки. В подкрепа на анализа ще се правят периодични прогнози за окончателните разходи и резултати.

Интегриран контрол на промените

Интегрираният контрол на промените се занимава с факторите, които влияят върху пораждането на промени, грижи се за съгласуването на промените, констатира наличието на промени и ги управлява, когато възникнат.

Първоначално дефинираният обхват и интегрираният основен план на проекта се поддържат чрез постоянно управление на възникналите промени чрез приемане или

отхвърляне на промените и включването им в актуализираната версия на основния план. Интегрираният контрол на промените изисква:

- Поддържане интегритета на базовите измерители на изпълнението.
- Отразяване на промените в обхвата на продукта във вече дефинирания обхват.
- Координиране на промените във всички сфери на знание.

2.1.3.2. Управление на обхвата

Управлението на обхвата на проекта включва процесите, които гарантират, че проектът включва цялата необходима работа и само необходимата работа за успешното осъществяване на проекта. То се занимава най-вече с определянето и контролирането на това какво е включено и какво не е включено в проекта.

- Стартирането е процесът на официалното възлагане на проект. Официалното възлагане на този проект ще бъде подписването на договор, което ще свърже проекта с работата на изпълнителя.
- Планирането на обхвата е процесът на детайлизиране и документиране на работата по проекта (обхвата на проекта). Описанието обхващо изискванията, които отразяват съгласуваните нужди на клиента. Резултатите от планирането на обхвата са Дефиниция на обхвата и План за управление на обхвата. Дефиницията на обхвата е основата за постигане на споразумение между възложителя и изпълнителя, чрез идентифициране на целите и резултатите по проекта. След стартирането на проекта екипите разработват множество дефиниции на обхвата, в съответствие с нивото на детайлизиране на работата (напр. Системен анализ, подробен график и др.).
- Определянето на обхвата включва разбиването на основните резултати, посочени в Дефиницията на обхвата, на по-малки, по-управляеми елементи. Целта е:
  - Подобряване на прогнозите за разходи, продължителност и ресурси.
  - Определяне на основни параметри за измерване на изпълнението и контрол.
  - Ясно разпределяне на отговорностите
- Потвърждаването на обхвата е процесът по официално приемане на обхвата на проекта от заинтересованите страни. Той изисква преглед на резултатите от работата и потвърждение, че всичко е свършено както трябва. Ако проектът се прекратява преждевременно, потвърждението на обхвата трябва да документира нивото и степента на завършеност.
- Контролът на промените в обхвата се занимава с факторите, които влияят върху пораждането на промени, грижи се за съгласуването на промените, констатира наличието на промени и ги управлява, когато възникнат.

2.1.3.3. Управление на времето

Управлението на времето по проекта включва следните процеси, необходими за навременното приключване на проекта:

- Определяне на дейностите – идентифициране и документиране на конкретните дейности, необходими за постигане на набелязаните резултатите и под-резултати. Определянето на дейностите се съгласува с Дефиницията на обхвата и включва детайлизиране, предположения и ограничения.
- Последователност на дейностите - идентифициране и документиране на логическите взаимозависимости. Дейностите трябва да бъдат в правилна последователност, за да спомогнат за разработването на реалистичен и

постижим график. Последователността може да следва критичната пътека. В резултат се определя график със съответните контролни точки и зависимости.

- Продължителност на дейностите – определя се въз основа на информацията за обхвата на проекта и ресурсите. Предварителната оценка ще се детайлизира в хода на работата, предвид наличието и качеството на входящите данни. Оценката се прави по методологията на критичната пътека.
- Определяне на график – задава се началната и крайната дата на дейностите по проекта. Процесът преминава през няколко итерации преди окончателното определяне на графика на проекта.
- Контрол на графика – занимава се с факторите, които влияят върху пораждането на промени, грижи се за съгласуването на промените, констатира наличието на промени и ги управлява, когато възникнат.

2.1.3.4. Управление на разходите

- Планирането на ресурсите включва определяне на количеството и качеството на необходимите ресурси (хора, техника, материали), както и сроковете на тяхното използване. То е тясно свързано с оценката на разходите.
- Оценката на разходите включва прогнозно определяне на разходите за необходимите ресурси. Взимат се предвид причините за отклонение от окончателната прогноза, за да се осигури по-добро управление на проекта.
- Бюджетирането на разходите включва разпределяне на общите прогнозни разходи по отделни дейности или групи дейности, за да се установи базовата цена, спрямо която ще се измерва изпълнението. Действителността може да наложи изготвяне на прогнози след одобрението на бюджета, но по възможност те трябва да се правят предварително.
- Контролът на разходите се занимава с факторите, които влияят върху пораждането на промени, грижи се за съгласуването на промените, констатира наличието на промени и ги управлява, когато възникнат. Контролът на разходите включва:
  - Проследяване изпълнението на бюджета, за да се открият и разберат разминаванията с плана.
  - Точно отразяване на необходимите промени в базовата цена.
  - Предотвратяване на включването на ненужни или неразрешени промени в базовата цена.
  - Информиране на съответната страна за одобрени промени.
  - Осъществяване на очакваните разходи в приемливи граници.

2.1.3.5. Управление на качеството

Целта на процесите по управление на качеството е да бъдат задоволени нуждите, заради които е предприет проекта. Тези процеси включват всички дейности от цялостното управление на проекта, които определят политиката, целите и отговорностите по качеството и ги осъществяват чрез планиране на качеството, гарантиране на качеството, качествен контрол и подобряване на качеството в рамките на системата за качество.

- **Планиране на качеството –** идентифициране на стандартите за качество за конкретния проект и начините за спазването им. Това е един от ключовите процеси при планиране на качеството и ще се извършва редовно, успоредно с останалите процеси по планиране на проекта.

- **Гарантиране на качеството –** всички планирани и систематични действия в рамките на системата за качество, които дават увереност, че проектът ще отговаря на съответните стандарти. Ще се извърша в хода на целия проект от вътрешни Специалисти по качеството.
- **Качествен контрол –** проследяване на конкретни резултати, за да се определи дали отговарят на зададените стандарти и да се набележат начини за отстраняване на причините за незадоволителните резултати. Ще се извърша в хода на целия проект. Резултатите включват както доставката на конкретен резултат/продукт, така и резултати от управлението на проекта (изпълнение на бюджета и графика). Би било полезно да се знае разликата между:
  - Предотвратяване (недопускане на грешки в процеса) и проверка (недопускане на грешки от страна на клиента).
  - Изпробване на атрибути (резултатът отговаря или не отговаря) и изпробване на променливи (резултатите се измерват по прогресивна скала за степен на съответствие).
  - Специални причини (необичайни събития) и случайни причини (нормално отклонение от процеса).
  - Допустимост (резултатът е приемлив, ако попада в посочения обхват на допустимост) и контролни граници (процесът е под контрол, ако резултатът е в рамките на контролните граници).

В рамките на проекта ще се приложи утвърдена в изпълнитеял методология за управление на качеството, основана на осемте принципа за управление на качеството, съгласно ISO 9001:2008.

Управлението на проекти се управлява електронно в Lotus база данни, наречена Leads&Projects. В нея се регламентира, кой е Manager на Проекта, кои са участниците - екипът, дава се прогноза и оценка за реализацията на развието на проекта, както и има възможност за отчет, както от участните, така и от мениджърите на проекта.

Въз основа на входната информация Operating manager/ Manager на проекта планира реализацията на проекта чрез генериране на Проектна Карта - Leads&Projects с информация за: дейности, кореспонденция, етапи, срокове, отговорности, проектен мениджър, планирани ресурси, междинни контроли, бюджет, приоритет.

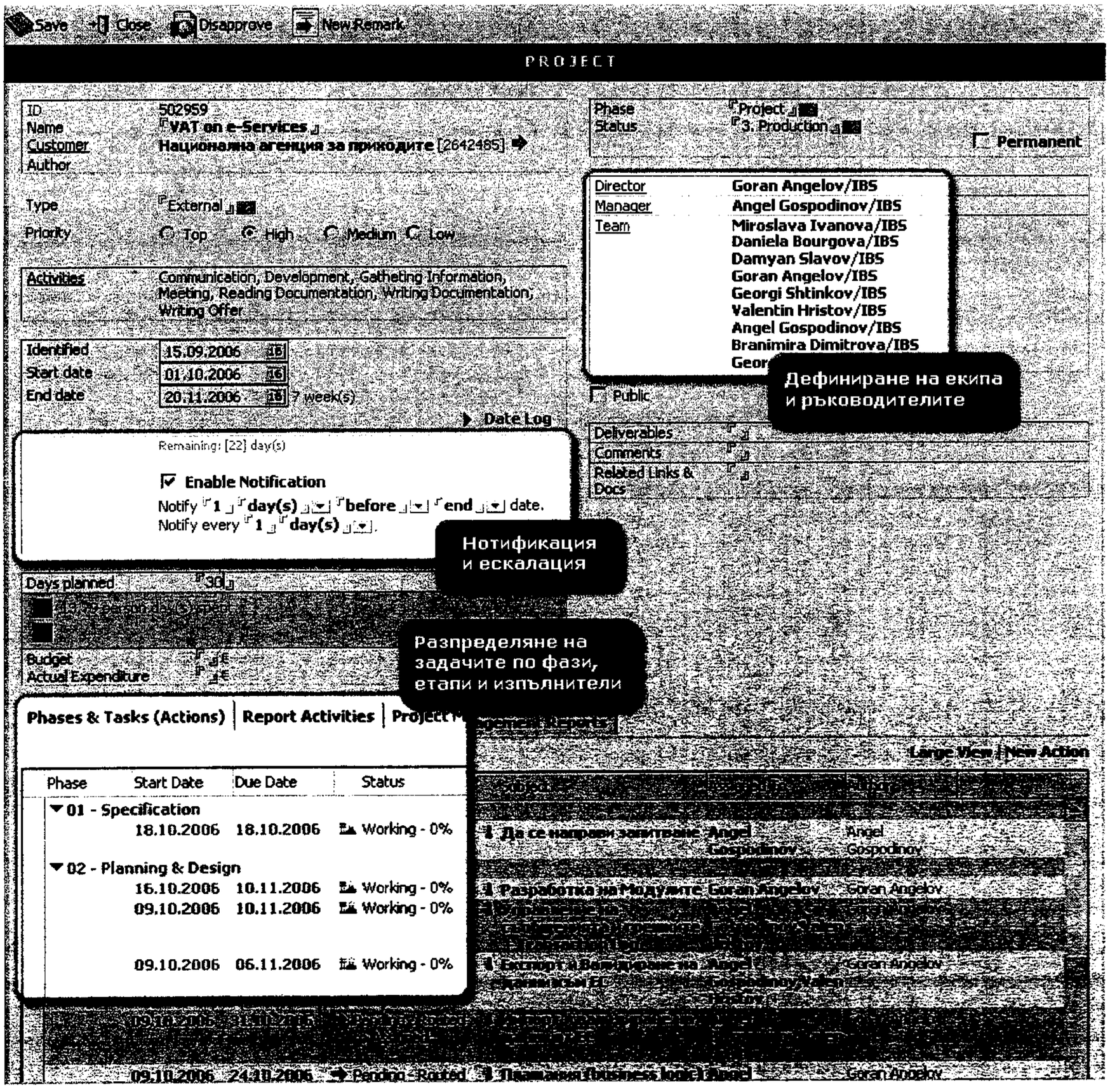
Базата Leads&Projects се архивира и в момента на приключването си всички проекти се запазват. Посредством архива се съставя и регистъра на Проектите, като търсенете в него се извършва по следните дейности:

- По вид;
- По статус;
- По мениджър на проекта;
- По участници – екип.

В базата Leads&Projects достъпът е ограничен и единствено предварително уточнените участниците и мениджърите на проекти могат да достъпват и коригират документите.

ERM Projects (управление на проекти) - приложението управлява процесите на дефиниране, планиране и проследяване и отчитане по проектите. Координацията на екипите по отделните проекти в цялата компания както вътрешни, така и външни. Поради това, че работи с *готова* информация от другите модули и потребителите *само* допълват, тяхната производителност се увеличава, от там планирането на проектите и

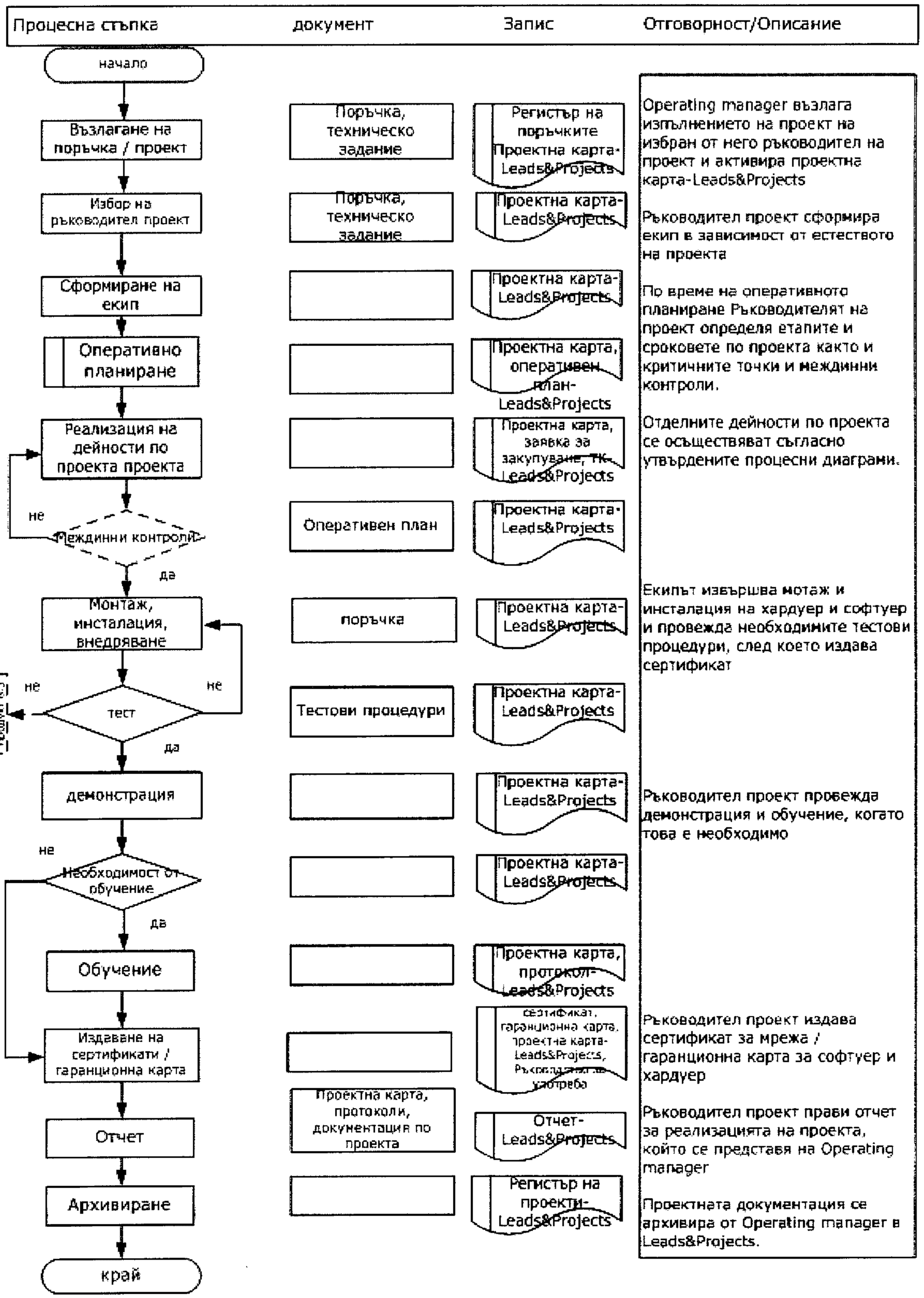
Всички проекти, които са регистрирани в системата се проследяват по всички предефинирани стъпки от техния цикъл на живот, съгласно най-добрите практики в индустрията:



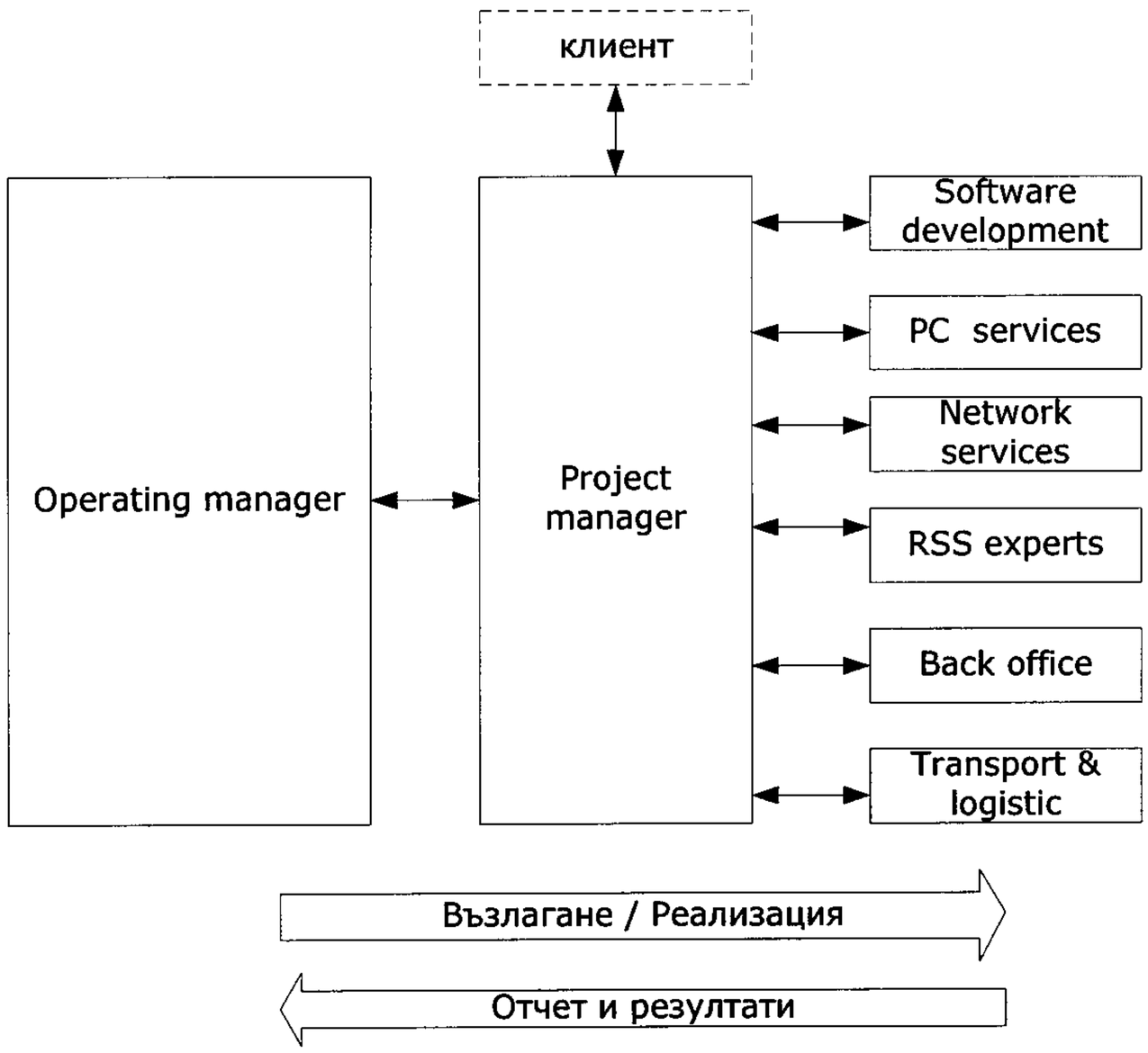
Всички проекти се описват и следят в единен регистър. Всеки има достъп до проектите в зависимост от своята роля във всеки един от тях, като отчитането на работата по проекта става с ERM Activities – тоест с функционалност, която вече е добре позната на повечето потребители на системата.

Продукта има вграден механизъм за планиране на ресурсите във времето и заедно с това да се сравнява реално изпълненото до момента. Всичко това дава допълнителен стимул за екипната работа, като системата се грижи за спазването на сроковете и отчитането на задачите.

Управление на проекти



Функционалните връзки между отделните звена в процеса на реализация на проекти са представени в следната функционална диаграма



Потвърждаване на качеството

За гарантиране качеството на продукта се осъществява междинен контрол на определени критични точки по време на процесите на реализация, както и краен качествен контрол на продукта. Организацията е определила критерии за преглед и одобряване на процесите, както и специфични методи за контрол. Организацията използва международно утвърдени методики за тестване и окачествяване на информационни системи.

2.1.3.6. Управление на човешките ресурси

Управлението на човешките ресурси включва процесите, които осигуряват най-ефективното използване на хората, участващи в проекта. То обхваща всички заинтересовани страни. Състои се от:

- Организационно планиране — идентифициране, документиране и определяне на роли, отговорности и канали за отчитане.
- Създаване на екипа — осигуряване на необходимите човешки ресурси и включването им в работата по проекта.
- Развитие на екипа — развиване на индивидуални и групови умения, с цел подобряване на изпълнението.

2.1.3.7. Управление на комуникациите

Процесите по управление на комуникациите осигуряват навременното и адекватно генериране, събиране, разпространение, съхранение и унищожаване на информацията по проекта. Те осъществяват критичната за успеха връзка между хора, идеи и данни. Всеки участник в проекта трябва да е готов да изпраща и приема комуникации и трябва да разбира как каналът на комуникация, в която участва, се отразява на целия проект.

- Планиране на комуникациите – определяне на нуждите на заинтересованите страни от информация и комуникации: кой от каква информация се нуждае, как ще я получи и от кого. Нуждата от предоставяне на информация за проекта е общовалидна, но информационните нужди и методите на разпространение са различни за всеки проект. Идентифицирането на нуждата от информация и разпространяването й по подходящ начин е важен фактор за успех на проекта.
- Разпространение на информацията – своевременното достигане на информацията до заинтересованите страни. Включва прилагането на Плана за комуникация и откликването на неочаквани искания на информация.
- Отчитане на изпълнението – събиране и разпространение на данни за изпълнението, показателни за използването на ресурсите за постигане на целите на проекта. Този процес включва:
- Отчитане на състоянието — описва докъде е стигнал проектът в дадения момент,
- Отчитане на напредъка — описва какво е постигнал екипът по проекта,
- Прогнозиране — предполага бъдещото състояние и напредък по проекта.
- Отчитане на изпълнението – данни за обхвата, графика, разходите и качеството.
- Административно приключване: след постигане на целите или след прекратяване по други причини, проектът или фазата трябва да приключи. Административното приключване се състои от документиране на резултатите, с цел официалното приемане на продукта от страна на клиента. То включва събиране на проектната документация, която отразява окончателните спецификации, анализ на успеха и ефективността на проекта и на извлечените поуки, и архивиране на тази информация за бъдещо ползване. Дейностите по административното приключване не се отлагат до приключването на проекта. Всяка фаза трябва да бъде надлежно приключена, за да не бъде загубена тази важна и полезна информация.

2.1.3.8. Управление на риска

Методологията за управление на риска е представена подробно в приложение №5 към техническото предложение.

Изпълнителят ще поддържа през целия период на изпълнение на проекта целия списък, описан по-долу.

Списък на рисковете представлява структурирано описание на известните и реално стоящи рискове пред проекта, подредени по реда на тяхното идентифициране. Към всеки риск се привързват мерки за ограничаване на последствията или действия при настъпване на риска. Списъкът на рисковете трябва да отразява критичните и сериозни рискове.

Регистърът на рисковете се изготвя и поддържа през целия проект в следния табличен вид:

№	Категория	Описание	Въздействие върху проекта	Собственик (Отговорник)	Приоритет	Степен на влияние	Вероятност	Индикатор	Стратегия за смекчаване

№	Категория	Описание	Въздействие върху проекта	Собственик (Отговорник)	Приоритет	Степен на влияние	Вероятност	Индикатор	Стратегия за смекчаване
1	Управленски рискове	Недостиг на компетентности и умения в рамките на проектния екип	Забавяне на целия проект	Възложител Изпълнителя	4	Значителна	Минимална (1 - 20%)	Неизпълнени срокове и липсващи одобрения на ключови дейности	

Рискът се идентифицира с пореден номер, който се записва в първата колона. Втората колона съдържа описание на риска, а третата – резюме на възможните последствия. В колона "Собственик (Отговорник)" се посочва(т) лицето или организацията (лицата или организациите), което отговаря (които отговарят) за противодействието на съответния риск. Скалата на приоритетите е от 1 до 8, като 1 е с най-нисък приоритет, а 8 е с най-висок.

2.1.3.9. Управление на доставките

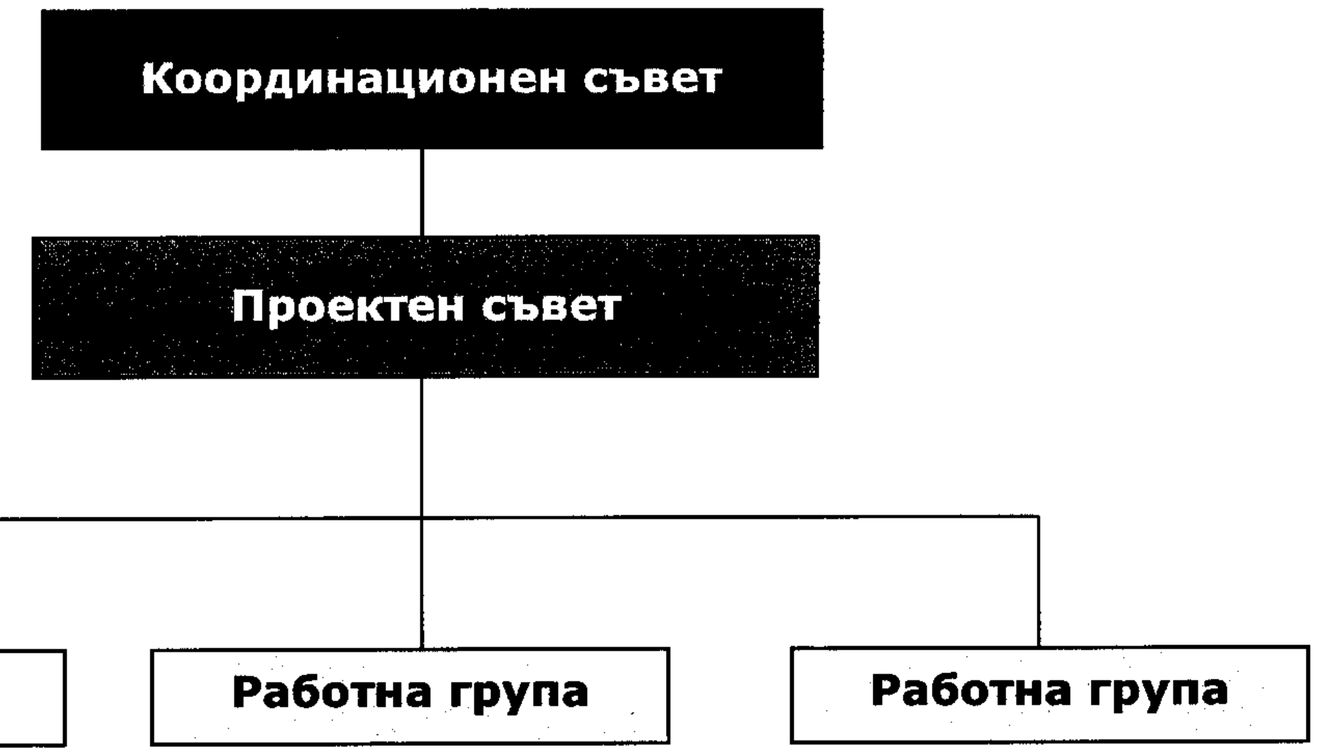
Управлението на доставките от трети лица се занимава с придобиването на стоки и услуги от външни за изпълнителя организации. Този процес се състои от:

- Планиране на доставките;
- Планиране на търсенето;
- Търсене;
- Избор на източник;
- Администриране на договори;
- Приключване на договори.

2.1.4. Структура на управление на проекта

За да осигури успех на проекта, изпълнителя използва следната структура за неговото управление на три нива:

1. Координационен съвет
2. Проектен съвет
3. Работни групи



Координационният съвет е главния орган за управление на проекта. Състои се от представители на ръководствата на изпълнителя и възложителя. Осигурява успешното развитие на проекта чрез вземане на стратегически решения по неговото управление и осъществява контрол над сроковете за изпълнение и плащанията по етапи.

Проектният съвет е оперативния орган за управление на проекта. Състои се от ръководителите на проекта от страна на изпълнителя и възложителя. Ръководителите на проекта:

- планират, организират и контролират изпълнението на всички задачи;
- организират и осигуряват присъствието на ключовите потребители на срещите на работните групи;
- осигуряват наличието на данните, необходими за настройка и преход към новата система;
- осигуряват техническите средства, необходими за изпълнение на отделните задачи и работните срещи по тях;
- отговаря за решаването на текущите проблеми, възникнали в хода на внедряването.

Ръководителите на проекта комуникират с Координационния съвет, когато е необходимо да се вземе стратегическо решение (заповед, промяна на работен процес и други).

Работните групи се създават от служители двете организации. Те извършват същинската работа по планиране, детайлизиране, тестване и изпълнение на решението в съответствие с одобрените планове.

2.2. Детайлен план-график

Всички дейности ще се планират и координират съвместно с Възложителя.

Подробният план-график за изпълнение на дейностите ще се изработи и съгласува съвместно с Възложителя. В Приложение 3 към техническата оферта е приложена План - Програма за изпълнение на дейностите съгласно изискванията на Техническата спецификация

2.2.1. Основни дейности

Изпълнителя предвижда следните базови стъпки за работа по проекта:

1. **Планиране** – тази стъпка започва с провеждането на встъпителна среща, на която изпълнителя ще представи документи свързани с методологията, която ще бъде приложена при управлението на проекта, организация на проекта - формиране на комуникационна карта с роли и отговорности, ключови роли и експерти, методите за планиране, контрол, управление на качеството, управление на промените, управление на риска.
2. **Детайлизиране на изискванията** – Проучване, документиране и представяне пред Възложителя на подробен план и график за дейностите по проекта.
3. **Анализ на текущото състояние на всички компоненти на системата**.
4. **Ремонт на дефектирали хардуерни устройства**
5. **Профилактика и поддръжка на оборудването и системите**
6. **Осъвременяване на оборудването**
7. **Изготвяне на подробен технически доклад за направените хардуерни и софтуерни инсталации**
8. **Провеждане на обучения**

3. ПОДХОД ЗА ИЗПЪЛНЕНИЕ НА ДЕЙНОСТИТЕ ПО ПОРЪЧКАТА

Изпълнителят ще се погрижи да се извършат всички дейности по проекта за да се достигне основният резултат - непрекъснато и безпроблемно функциониране на НВИС в Национален Визов Център (НВЦ) и Резервен визов център (РВЦ), както и осигуряване на непрекъсната връзка с ВИС на ЕС и поддържане на постоянен обмен на информация между системите.

Конкретни дейности по осигуряване на техническата поддръжка

3.1. Осигуряване 24/7 техническа поддръжка

Изпълнителят ще осигури техническа поддръжка 24/7 (24 часа/ 7 дни в седмицата) на наличното техническо оборудване и програмно осигуряване, като това включва текущи ремонти, заменяне на повредено оборудване, ъпгрейд или подобряване на наличните хардуерни и софтуерни средства, и техническа поддръжка 8/5 (8 часа в работни дни) на конкретното техническо оборудване и програмно осигуряване.

Изпълнителят ще осигури поддръжка на цялостното техническо оборудване за целия срок на договора, включително в случаите, когато официалната поддръжка на оборудването бъде спряна от производителя. При подмяна на оборудване с ново от Възложителя техническата поддръжка ще бъде съобразена с гаранционния срок на новодоставеното за срок не по-малък от 3 години или до 31.12.2019 (което настъпи по-късно)

В случай на подмяна на инфраструктурни компоненти, Изпълнителят ще осигури миграцията и продължи да осигурява софтуерна поддръжка на мигрираните върху новото оборудване съществуващи услуги.

3.1.1. Анализ на текущото състояние на всички компоненти на системата.

Изпълнителят внимателно ще анализира състоянието всички компоненти и ще предостави доклад, който ще включва в себе си изискванията за одит разписани в отделните компоненти. Докладът ще съдържа минимум:

- Съответствие на действителното състояние на компонентите с описанието им в наличната документация – характеристики, серийни номера, количества и др.;
- Оценка на техническото им състояние – съществуващи проблеми, потенциални проблеми и др.;
- Обща оценка за цялостното състояние на системата.

Продължителност: до 30 календарни дни след сключване на договора за поддръжка и след това веднъж годишно до края на договора – 31.12.2019 г.. Изпълнителят ще изготвя доклад с анализ на състоянието на инфраструктурата ежегодно – в срок от 30 дни след завършване на всяка година от проекта.

Приемане на дейността: с доклад за изпълнение на дейността.

Приложимост:

Таблица 1. Приложимост на дейностите

Компонент	Система	Периодичност	Резултат	Забележка
Всички, както са описани в т. 3.1. на ТС	Всички	Веднъж годишно	Доклад за оценка техническото състояние на доставеното оборудване и програмно осигуряване. Наличие на актуална документация за състоянието на системите.	

3.1.1.1.1. Анализ на мрежовата инфраструктура и комуникациите

- Проверка на функционирането на мрежата като цяло:
  - вътрешни комуникации между НВЦ и РВЦ;
  - маршрутни протоколи;
  - криптиране на трафика;
  - комуникация с външни мрежи (МВР, ДАНС, Европейска визова система, МВнР);
  - свързаност на сървърите с мрежовите устройства;
  - резервираност на комуникациите;
- Преглед на сигурността на мрежата.
  - Достъпа до устройствата да става по сигурни протоколи. Смяна на паролите.

3.1.2. Планиране на дейностите по поддръжка и обновяване на системите

Продължителност: до 7 календарни дни след извършване на анализа от т. 3.1.1 след подписване на договора и след това веднъж годишно до края на договора – 31.12.2019г.

Приемане на дейността: с доклад за изпълнение на дейността.

3.1.3. Ремонт на дефектирали хардуерни устройства.

Ремонтът на дефектирали устройства и/ или компоненти ще се извършва спрямо тяхната критичност за функционирането на всички системи. Нивата на критичност се дефинират както следва:

Ниво на критичност	**Време за възстановяване**
Високо (Заплаха за спиране на НВИС или основни инфраструктурни системи)	4 часа
Средно (Заплаха за липса на резервираност)	8 часа
Ниско (Потенциална заплаха за инцидент)	24 часа

Сроковете в таблицата започват да текат от официалното заявяване от Възложителя към Изпълнителя за дефектирало устройство или компонент.

Определянето на нивото на критичност ще се съгласува писмено между Възложителя и Изпълнителя.

Продължителност: до 15 работни дни след извършване на анализа от т. 3.1.1, а след това спрямо нивото на критичност на устройството/ компонента за срока на договора – 31.12.2019 г.

Приемане на дейността: с приемо-предавателен протокол.

Приложимост:

Таблица 2. Приложимост на дейностите

Компонент	**Система**	**Периодичност**	**Резултат**	**Забележка**
Компонент 1 както е описан в т. 3.1.1.**Error! Reference source not found.** на ТС	Всички	За целия срок на договора или извеждане на оборудването от употреба	Безпроблемна и надеждна работа на мрежовата подсистема.	
Компонент 2 както е описан в т. 3.1.2 на ТС	Всички	За целия срок на договора или извеждане на оборудването от употреба	Безпроблемна и надеждна работа на сървърната подсистема и лентови библиотеки.	

Компонент	Система	Периодичност	Резултат	Забележка
Компонент 3 както е описан в т. 3.1.3 на ТС	Всички	За целия срок на договора или извеждане на оборудването от употреба	Безпроблемна и надеждна работа на дисковата подсистема.	

3.1.4. Профилактика на оборудването

Продължителност: До 30 дни след сключване на договора за възлагане на поръчката към Изпълнителя, а след това веднъж годишно до края на договора – 31.12.2019 г.

Приемане на дейността: с доклад за изпълнение на дейността.

Отстраняване на установени неизправности, дефекти и функционални откази.

Профилактика на оборудването, включваща отстраняване на прах и други замърсители от повърхността и вътрешността на оборудването.

Контролирано рестартиране на всеки от мрежовите и сървърни компоненти с цел проверка работоспособността на резервираността на системите, както и установяване на възможностите за автоматично възстановяване след сривове.

Приложимост:

Таблица 3. Приложимост на дейностите

Компонент	Система	Периодичност	Резултат	Забележка
Компонент 1 както е описан в т. 3.1.1.**Error! Reference source not found.** на ТС	Всички	По план съгласуван с Възложителя	Безпроблемна и надеждна работа на мрежовата подсистема.	
Компонент 2 както е описан в т. 3.1.2 на ТС	Всички	По план съгласуван с Възложителя	Безпроблемна и надеждна работа на сървърната подсистема и лентови библиотеки.	
Компонент 3 както е описан в т. 3.1.3 на ТС	Всички	По план съгласуван с Възложителя	Безпроблемна и надеждна работа на дисковата подсистема.	Без контролирано рестартиране

3.1.5. Поддръжка на Компоненти 1, 2 и 3 - мрежова, сървърна, лентова и дискова инфраструктури.

Продължителност: За целия срок на договора или до извеждане на оборудването от употреба.

Приемане на дейността: с приемо-предавателен протокол и доклад за изпълнение на дейността.

Изпълнителят ще извърши корекционни дейности съгласно препоръките, описани в изготвените доклади за състояние на инфраструктурата. До 30 дни след приемане на доклада и възлагане от страна на Възложителя

За целия срок на договора Изпълнителят ще извършва, по заявка от Възложителя, конфигурации и преконфигурации по инфраструктурата, които са свързани с нейните разширение и нормално функциониране и не представляват промени в архитектурата й.

Приложимост:

Таблица 4. Приложимост на дейностите

Компонент	Система	Периодичност	Резултат	Забележка
Компонент 1 както е описан в т. 3.1.1.**Error! Reference source not found.** на ТС	Всички	При необходимост	Безпроблемна и надеждна работа на мрежовата подсистема.	
Компонент 2 както е описан в т. 3.1.2 на ТС	Всички	При необходимост	Безпроблемна и надеждна работа на сървърната подсистема и лентови библиотеки.	
Компонент 3 както е описан в т. 3.1.3 на ТС	Всички	При необходимост	Безпроблемна и надеждна работа на дисковата подсистема.	

3.1.6. Поддръжка на Компонент 4 - Софтуер за архивиране и възстановяване, софтуер за наблюдение и софтуер за управление

Продължителност: За целия срок на договора или до извеждане на системните инструменти от употреба.

Приемане на дейността: с приемо-предавателен протокол и доклади за изпълнение на дейността.

В поддръжката на IBM Tivoli Storage Manager (IBM Spectrum Protect) ще са включени минимум следните дейности:

- Отстраняване на проблеми свързани с невъзможността за създаване на резервни копия (Backup)/архив. Тук се включват следните услуги:
    - Специфично конфигуриране на Решението на място при ВЪЗЛОЖИТЕЛЯ по предварително съгласувани политики;
    - Допълнителен анализ на системните логове/записи на Решението във връзка с конкретно направено конфигуриране;
    - Помощ при възстановяване на информация архивирана чрез Решението
- Управление на достъпа до средите за архивиране на данни, чрез създаване и/или промяна на потребители или промяна на параметри в IBM Tivoli Storage Manager сървър с подходящи права за достъп.
- Конфигуриране на лентови библиотеки за работа с IBM Tivoli Storage Manager сървър.
- Конфигуриране съществуващи и/или създаване на нови политиките за съхранение на данни
- Конфигуриране съществуващи и/или създаване на нови контейнери за съхранение на данни
- Конфигуриране съществуващи и/или създаване на нови графици (schedules), за изготвяне на резервни копия (backup) или архиви.
- Превантивна поддръжка на Решението, чрез наблюдение на поведението му и предупреждение за необходимост от възстановяване в случаите на нарушено функциониране (включително следене на процеса на архивиране в системната база данни на Решението). Изпращане на ежедневен оперативен доклад за състоянието на Решението.
- Тестово възстановяване на данни до два пъти в рамките на дванадесет месеца с хардуер предоставени от ВЪЗЛОЖИТЕЛЯ.
- Ежемесечен анализ на системните записи/отчети, на производителността и натоварването на Решението. Изготвяне на ежемесечен доклад за състоянието на Решението.
- Анализ на проблеми свързани със съвместимостта, операционната система и хардуерната среда на Решението.
- Препоръки за оптимизиране работата на внедреното Решение, базирани на извършените анализи.
- Телефонни и e-mail консултации относно въпроси, свързани с функционалността на внедреното Решение.

В поддръжката на IBM Tivoli Monitoring ще са включени минимум следните дейности:

- Ежеседмична проверка на Депата (Agent Depots) за консистентност в цялата IBM Tivoli Monitoring Инфраструктура
- Ежеседмична проверка/конфигуриране на Agent Application поддръжката е валидна и коректна.
- Ежеседмична проверка и конфигуриране наличността на всички ключови компоненти на IBM Tivoli Monitoring инфраструктурата – IBM Tivoli Enterprise Portal Server, IBM Tivoli Monitoring Server, IBM Tivoli Warehouse Proxy Agent и Summarization & pruning agent.

- Ежеседмична проверка за Off-line агенти за наблюдение и отстраняване на причините за това.
- Ежеседмична проверка за регулярно изпращане и съхранение на данните от Tivoli Monitoring агентите в системата за историческо съхранение на данните (IBM Tivoli Monitoring Data Warehouse)
- Ежемесечна проверка за IBM Tivoli Monitoring Data Warehouse по отношение на капацитет и производителност.
- Инсталиране и конфигуриране на нови агенти за наблюдение на инфраструктурата и правилното им визуализиране в IBM Tivoli Portal Server.
- Конфигуриране съхранението на исторически данни в IBM Tivoli Data Warehouse за нови или съществуващи агенти за наблюдение.
- Създаване на нови и конфигуриране на съществуващи плотове за визуализиране на данните (Dashboard) от IBM Tivoli Monitoring инфраструктурата.
- Създаване на ново и пренастройка на специализирани агенти за наблюдение създадени с IBM Tivoli Monitoring Agent Builder.
- Управление на достъпа до средите за архивиране на данни, чрез създаване и/или промяна на потребители или промяна на параметри в IBM Tivoli Storage Manager сървър с подходящи права за достъп.
- Ежемесечен анализ на производителността и натоварването на Решението. Изготвяне на доклад за състоянието на Решението.
- Анализ на проблеми свързани със съвместимостта, операционната система и хардуерната среда на Решението.
- Препоръки за оптимизиране работата на внедреното Решение, базирани на извършените анализи.
- Телефонни и e-mail консултации относно въпроси, свързани с функционалността на внедреното Решение.

Таблица 5. Приложимост на дейностите

Компонент	**Система**	**Периодичност**	**Резултат**	**Забележка**
Компонент 4 както е описан в т. 3.1.4 на ТС	Софтуер за архивиране и възстановяване Софтуер за мониторинг	Ежеседминчен анализ и месечни доклади. Промени и корективни действия само при необходимост	Инфраструктурата на IBM Tivoli Storage Manager и IBM Tivoli Monitoring да са оптимизирани според нуждите и изискванията на НВИС.	

3.1.7. Поддръжка на Компонент 5 - Специализиран софтуер SIB (Steria Interconnection Box for VIS), Oracle Database Servers, Oracle Weblogic Application Servers и специализиран софтуер CompliTT.

Продължителност: За целия срок на договора или извеждане на специализирания софтуер от употреба.

Приемане на дейността: с приемо-предавателен протоколи и доклади за изпълнение на дейността.

В поддръжката трябва ще са включени минимум следните дейности:

- Одит на техническото състояние на доставеното софтуерно оборудване, оценка на състоянието му и изготвяне на писмен встъпителен доклад.
- Осигуряване на поддръжка, нови версии, update, upgrade, patches от производителя Steria Benelux S.A. за продуктите SIB (Steria Interconnection Box for VIS) и Steria CompliTT;
- Инсталация, преинсталация, конфигурация на нови версии на продуктите SIB (Steria Interconnection box for VIS) и специализиран тестов инструмент Steria CompliTT;
- Комуникация с производителя Steria при открити програмни грешки, липса на функционалност и неочаквано поведение на софтуера;
- Изграждане и конфигуриране на бази данни за осигуряване работата на SIB (Steria Interconnection box for VIS) с Oracle Database;
- Проверка на логовете на Oracle Database Real Application Cluster и отстраняване на открити проблеми.
- Проверка за коректно функциониране на услуги по репликация на данни от основе в резервен център;
- Проверка за успешно изпълнени архиви и тестово възстановяване.
- Изграждане и конфигуриране на сървъри за приложения за осигуряване на работата на SIB (Steria Interconnection box for VIS)с Oracle WebLogic;
- Извършване на специализирани тестове на SIB (Steria Interconnection box for VIS) с Steria CompliTT;
- Изготвяне, зареждане, валидиране на тестови сценарии за тестове с Steria CompliTT;
- Тестване за оперативна съвместимост с европейската мрежа. Тестовете следва да се провеждат по време на специално дефиниран времеви прозорец и място, определено от Възложителя. По време на тестовете трябва да бъде осигурен сертифициран от Steria специалист на място, който да изпълни тестовете и да изготви предварително дефиниран доклад. Тестовете се изпълняват чрез сертифициран от производителя Steria инструментален софтуер.
- Проактивен мониторинг: Оптимизиране на системата за проактивен мониторинг, осигуряваща непрекъсваемост и бързо отстраняване на евентуални технически проблеми;
- Администриране на специализиран софтуер SIB (Steria Interconnection Box for VIS), Steria CompliTT, Oracle Database Servers и Oracle WebLogic Application Servers - интеграция, анализ, извършване на тестове и др. свързани с работата на описания софтуер;

Изпълнителят ще предостави услугите с техническите и функционални показатели, съответстващи на параметрите, заложени в т. 3.4 "Техническа спецификация".

Приложимост:

Таблица 6. Приложимост на дейностите

Компонент	Система	Периодичност	Резултат	Забележка

Компонент	Система	Периодичност	Резултат	Забележка
Компонент 5 както е описан в т. 3.1.5.**Error! Reference source not found.** на ТС	SIB for VIS CompliTT Oracle Database Servers Oracle WebLogic Application Servers	При необходимост за целия срок на договора. Дейностите следва да се изпълняват в рамките на 14 дни след възлагане от Възложителя, освен ако не е посочено друго в заявката.	Модулите на SIB for VIS, Steria CompliTT, Oracle Database и Oracle WebLogic да адаптирани според изискванията на ЕС.	

3.1.8. Поддръжка на Компонент 6 - Приложен софтуер на НВИС и система за управление на базата от данни IBM Informix, използвана от централната компонента на НВИС

Продължителност: За целия срок на договора или до извеждане на приложния софтуер от употреба.

Приемане на дейността: с приемо-предавателен протоколи и доклади за изпълнение на дейността.

В поддръжката ще са включени минимум следните дейности:

- Консултантски услуги за свързване и работа на Националната визова информационна система с Визовата информационна система на ЕС, Шенгенската информационна система и специализираната система за обмен на информация за консулско сътрудничество и съгласуване на визи VIS Mail.
- Съдействие при свързване и настройка на Националната визова информационна система за работа с Визовата информационна система на ЕС, Шенгенската информационна система и специализираната система за обмен на информация за консулско сътрудничество и съгласуване на визи VIS Mail. Участие в подготовката и провеждането на тестове за свързаност и съвместимост.
- Поддържане на функционалните възможности и информационния обхват на НВИС в съответствие с изискванията и измененията на Визовата информационна система на ЕС.
- Предоставяне и инсталиране на нови версии /update/ на Националната визова информационна система, отстраняващи възникнали проблеми и оптимизиращи нейната работа. Изграждане на нови таблици и индекси в базата данни. Поддръжка на кодовите таблици на системата, изграждане на нови номенклатури за избор на кодови значения.

- Инсталация и преинсталация на приложното програмно осигуряване на компонентите на системата, работещи в Националния визов център на МВнР (централни компоненти) върху съществуващо или ново техническо оборудване.
- Настройка на конфигурационните и експлоатационни параметри на системата, работеща в Националния визов център.
- Възстановяване работата на системата в Националния визов център след повреда на технически ресурси.
- Консултантски услуги, свързани с оптимизиране на бизнес процесите на НВИС в консулските служби. Посещение на поне три консулски служби и при необходимост - изготвяне на препоръки и план за развитие.
- Съдействие при избора на биометрични устройства и технологии.
- Интеграция на нови биометрични и други специализирани устройства към НВИС.
- Консултации и съдействие при администриране на НВИС;
- Анализ и отстраняване на проблеми, възникващи при обработка на постъпващите данни от външни доставчици на услуги. вкл. при постъпване на некоректни или непълни данни, дублиране на данни и др.;
- Анализ и отстраняване на проблеми, възникващи при работата на системата в консулските служби на Република България;
- Оптимизиране на времето за достъп до информацията в базата данни при необходимост, след натрупването на големи количества биометрични данни;
- Осигуряване сервизна софтуерна поддръжка на СУБД IBM Informix:
  - Помощ при отстраняване на възникнали проблеми и извършване на консултации по телефона в работно и извънработно време - целогодишно и денонощно (24x7)
  - Консултации на място и реакция при възникнал проблем - целогодишно и денонощно (24x7).
  - Време за реакция при възникнал проблем – до 4 ч. (времето се измерва от момента на официално регистриране на заявка за проблем; неизпълнението на сроковете подлежи на санкциониране съгласно клаузите на договора за изпълнение)

Таблица 7. Приложимост на дейностите

Компонент	Система	Периодичност	Резултат	Забележка

Компонент	Система	Периодичност	Резултат	Забележка
Компонент 6 както е описан в т. 3.1.6. на ТС	Приложен софтуер на НВИС и система за управление на базата от данни IBM Informix	При регистриране на проблем; при заявка за промяна;	Приложният софтуер на НВИС и системата за управление на базата от данни IBM Informix да са адаптирани според изискванията на ЕС и процесите за издаване и обработка на визи.	

3.1.9. Поддръжка на Компонент 7 - Системен софтуер на Microsoft (Windows Server 2012/ 2012 R2, Microsoft Exchange Server 2013, Microsoft System Center 2012 R2 Virtual Machine Manager и Microsoft System Center 2012 R2 Configuration Manager)

Продължителност: За целия срок на договора или до извеждане на системния софтуер от употреба.

Приемане на дейността: с приемо-предавателен протоколи и доклади за изпълнение на дейността.

Изпълнителят ще приложи следната методика за поддръжката на Microsoft инфраструктурата:

1. Детайлно документиране на текущите услуги, базирани на продукти от Microsoft
2. Оценка на текущото състояние и анализ на изискванията към отделните Microsoft компоненти
3. Дефиниране на дейностите, необходими за осигуряване на оперативна поддръжка, и изготвяне на план за ежедневни, седмични, месечни и годишни активности в зависимост от критичността на компонентите спрямо цялостната наличност и надеждност на системата
4. Изпълнение на съответните дейности
5. Извършване на промени в Microsoft инфраструктурата в следствие на нови или променени изисквания на Възложителя относно НВИС
6. Извършване на ъпгрейди, миграции и конфигурации при подмяна на сървърни, мрежови и дискови компоненти
7. Цялостна оптимизация на Microsoft инфраструктурата по отношение на капацитет, производителност, надеждност и сигурност на информацията

В поддръжката на Microsoft Windows Server 2012/ 2012 R2 ще бъдат включени следните дейности:

- Ъпгрейд към последна актуална версия при поискване от Възложителя
  - Ъпгрейдите ще се съгласуват с версиите на другите компоненти с цел гарантиране на официалната поддръжка от производителя, както и

намаляване на възможностите за инциденти или негативен ефект върху работата на НВИС или поддържащи системи
- Ъпгрейдите ще се валидират предварително в тестова среда за съвместимост с текущата конфигурация
- След извършването на ъпгрейд ще се тества функционално и оперативно работата на всички променени и свързани компоненти, както и работоспособността на поддържащите системи за архивиране, наблюдение, отказоустойчивост и т.н.
- При установяване на нормално функциониране на системата след ъпгрейд ще се обновява документацията на променените компоненти и конфигурации
- При установяване на некоректно функциониране системата ще бъде възстановена към предишното стабилно състояние

- Осигуряване на съдействие при подмяна на хардуер
  - Извършване на оценка на потенциалните рискове в следствие на планираната подмяна
  - Изготвяне на план на дейностите за подмяната
  - Допълнително архивиране на системата преди подмяната
  - Валидиране на работоспособността на Microsoft компонентите с подменения хардуер
- Проверка на бекъпите и извършване на тестово възстановяване
  - Ежедневна проверка на лог файловете и конзолата на софтуера за бекъп с цел установяване на успешно преминал дневен бекъп
  - Седмична проверка след преминал пълен бекъп
  - Конфигуриране на нотификации към администраторите за известяване при неуспешно преминала бекъп дейност
  - Изготвяне на план за тестово възстановяване
  - Извършване на тестово възстановяване – веднъж месечно
- Проверка на хард дисковете за свободно пространство, темпове на запълване и производителност
  - Конфигуриране на отчет в системата за наблюдение, даващ справка за наличното свободно пространство по различните сървърни системи
  - Конфигуриране на нотификации за администраторите при спадане на свободното пространство под определен праг
  - Проверка за грешки, свързани със закъснение при четене или запис от дисковите дялове, и при наличие на такива – изпълнение на процедура за тестване на производителността, препоръчана от Microsoft за съответния компонент и приложение
- Проверка на дефинициите на Антивирус и Антиспайуеър софтуерите, тяхното състояние и регистрирани проблеми
  - Ежедневна проверка на лог файловете и конзолата на софтуера за Антивирус и Антиспайуеър
  - Конфигуриране на нотификации към администраторите за известяване при регистриран вирус или потенциална заплаха
  - Анализиране на проблема и стартиране на процедура по отстраняване на вируса, препоръчана от доставчика на Антивирусния софтуер

- Оценка на предпоставките за активиране на вируса или заплахата и извършване на превантивни промени по всички потенциално атакуеми компоненти
- Проверка относно и инсталиране на актуални ъпдейти за приложенията и операционната система
  - Анализиране на предлаганите ъпдейти и тяхната приложимост към инфраструктурата на НВИС
  - Инсталиране на ъпдейтите и валидиране на компонентите и системата в тестова среда
  - При успешно валидиране ъпдейтите ще се дистрибутират към всички системи, за които са приложими
  - Изготвяне на справка от Widows Software Update Services или Microsoft System Center Configuration Manager за успешното инсталиране на ъпдейтите
  - Диагностика и анализ на грешките в следствие на невъзможността или некоректното инсталиране на ъпдейт
- Проверка на резултатите от мониторинг за открити грешки и проблеми
  - Ежедневна проверка на лог файловете и конзолата на софтуера за наблюдение
  - Филтриране на важните събития
  - Извършване на корелация между събитията в различните компоненти и анализ на ситуацията
  - Конфигуриране на нотификации за администраторите при регистриране на конкретни грешки или възникнали събития
  - При наличие на инцидент или съмнение за проблем се стартират процедура от инцидент или проблем мениджмънт процесите
- Проверка на Windows Event Logs за грешки и предприемане на съответните мерки
  - Ежедневна проверка на Windows Event Logs от конзолата на софтуера за наблюдение
  - Изготвяне на предефинирани справки, даващи информация за всички или специфични грешки
  - При липса на връзка с конкретен сървър се извършва проверка на Windows Event Logs от конзолата на сървъра и се установява причината за липса на свързаност и други грешки, ако има такива
  - При наличие на инцидент или съмнение за проблем се стартират процедура от инцидент или проблем мениджмънт процесите
- Цялостна проверка на хардуерните и софтуерните компоненти, с фокус върху процесори, памет, хард дискове, сторидж и мрежови контролери
  - Изготвяне на план за седмични и месечни проверки
  - Изготвяне на чеклисти и процедура за проверка
  - Извършване на тестове за производителност и надеждност
  - Извършване на проверки след подмяна на компоненти, миграция към нов хардуер или нова версия на софтуерен продукт
  - Извършване на проверки след миграция към нов, различен хардуер
- Тестване на функционалността на основни услуги: DNS, DHCP и Hyper-V
  - Проверка на функционалността при отпадане на физически DNS или DHCP сървър – тест за надеждност

- Проверка на функционалността при отпадане на виртуална машина, DNS или DHCP сървър – тест за надеждност
- Проверка на коректността на съдържанието на отделните сървъри, тестване на резолюция на имена и получаване на адреси
- Проверка за консистентността на данните и интеграцията между DNS и DHCP услугите
- Тестване на Hyper-V услугите – изключване на сървър и преместване на виртуални машини на друг сървър – тест на клъстер за надеждност
- Тестване на Hyper-V услугите – мигриране на виртуални машини на друг сървър или миграция на дисковата подсистема, създаване на нови виртуални машини
- Възстановяване на виртуална машина от бекъп и възстановяване на аварирал Hyper-V сървър

В поддръжката на Microsoft Windows Active Directory ще са включени следните дейности:

- Преглед на потребителски акаунти и премахване на ненужни акаунти
  - Веднъж месечно
  - След проекти по миграция или обновяване, за нуждите на които са създавани временни акаунти
  - Анализ на необходимостта от акаунтите и нивата на достъп, и реорганизация ако е необходимо
  - Изготвяне на отчет за използването на акаунтите за определн период
- Стартиране на Microsoft's Domain Controller Diagnostics - от команден ред, се стартира dcdiag.exe (само на ДК). Ако командите са неразбираеми, трябва да се инсталира Windows Support Tools
  - Скриптиране на командата
  - Автоматично изпълнение всеки ден или веднъж седмично
  - Изготвяне на отчет и изпращане към администратора
  - Анализ на грешките и предприемане на мерки за отстраняването им
- Потвърждаване дали политиката за пароли е активирана
  - Тестване на политиката с тестови акаунти
  - Преглед на Security Log в Windows Event Viewer за грешки и заключени акаунти
  - Анализ на параметрите: интервал на смяна на паролата, минимална и максимална история, комплексност и дължина, както и връзка с политиката за заключване на акаунтите
- Преглед на дисковото пространство на домейн контролера
  - Като част от поддръжката на Windows Server 2012
- Проверка на бекъпите - бекъп на активната директория включващ състоянието на системата, информация свързана с базата данни на активната директория, логове, регистри, файлове за стартиране, SYSVOL и други системни файлове
  - Изготвяне на процедура за възстановяване
  - Тестово възстановяване на домейн контролер
  - Възстановяване на Активна Директория в ситуация, в която няма изправно бекъп копие
  - Тестово възстановяване на изтрит акаунт или група
  - Тестово възстановяване на групова политика

- Проверка за правилната работа на репликацията на активната директория
  - С използване на Microsoft's Domain Controller Diagnostics
- Проверка на логовете за "persistent" грешки
  - Създаване на справка от системата за наблюдение за специфични грешки
  - При доказване на определени симптоми се инициира процедурата за инцидент или проблем мениджмънт
- Стартиране на дефрегментация за увеличаване на производителността. При дълго време на работа големите директории стават по-големи и се налага дефрагментация
  - След анализ с помощта на Ntdsutil (ntdsutil.exe) се преценява дали има такава необходимост
  - Ако има – инициира се промяна, извършва се бекъп и се извършва дефрагментацията в предварително съгласувано време

В поддръжката на Microsoft Exchange Server 2013 ще са включени следните дейности:

- Ъпгрейд към последна актуална версия при поискване от Възложителя
  - Подготовка за ъпгрейд
  - Проверка за съвместимост
  - Обновяване на Windows Server и Exchange Server 2013 до нужното ниво
  - Бекъп на Active Directory, бази и конфигурация
  - Подготовка на Active Directory – схема и конфигурация
  - Конфигуриране на Windows Server клъстери
  - Инсталация на нови Exchange 2016 сървъри, конфигурирани в DAG
  - Преместване на пощенските кутии
  - Преконфигурация на SMTP трафика и клиентския достъп
  - Премахване на старите Exchange 2013 сървъри от конфигурацията
- Инсталиране на ъпдейти и фиксове
  - Анализиране на предлаганите ъпдейти и тяхната приложимост към Exchange инфраструктурата
  - Инсталиране на ъпдейтите и валидиране на компонентите и системата в тестова среда
  - При успешно валидиране ъпдейтите ще се дистрибутират към всички системи, за които са приложими
  - Диагностика и анализ на грешките в следствие на невъзможността или некоректното инсталиране на ъпдейт
- Проверка на физическото оборудване
  - Проверка на физическите сървъри, върху които работят Exchange Server виртуални машини за грешки, производителност, свободно дисково пространство, утилизация на оперативната памет и мрежовите интерфейси
  - Анализ на резултатите и изготвяне на план за отстраняване на проблеми и оптимизиране на конфигурацията
  - Прилагане на промените след оценка и одобрение
- Проверка и мониториране на бекъпите
  - Ежедневна проверка на лог файловете и конзолата на софтуера за бекъп с цел установяване на успешно преминал дневен бекъп
  - Седмична проверка след преминал пълен бекъп

- Конфигуриране на нотификации към администраторите за известяване при неуспешно преминала бекъп дейност
- Изготвяне на процедура за възстановяване
- Извършване на тестово възстановяване – веднъж месечно
- Тестово възстановяване на пощенска кутия
- Тестово възстановяване на Exchange mailbox база
- Тестово възстановяване на Exchange сървър
- Възстановяване на Активна Директория в ситуация, в която няма изправно бекъп копие
- Тестово възстановяване на изтрит акаунт или група
- Тестово възстановяване на групова политика

• Проверка на използваното дисково пространство
  - Конфигуриране на отчет в системата за наблюдение, даващ справка за наличното свободно пространство по различните дялове, използвани от Exchange Server – за бази от данни, transaction log файлове, опашки на SMTP услугите, индекси на услугите за търсене и т.н.
  - Конфигуриране на нотификации за администраторите при спадане на свободното пространство под определен праг
  - Проверка за грешки, свързани със закъснение при четене или запис от дисковите дялове, и при наличие на такива – изпълнение на процедура за тестване на производителността, препоръчана от Microsoft за съответния компонент и приложение
• Проверка на Event viewer
  - Част от проверката на Windows Event Viewer за Windows Server 2012
• Мониториране на работата на сървърите
  - Част от наблюдението на Windows Server 2012
• Мониториране на операционните системи
  - Част от наблюдението на Windows Server 2012
• Мониториране на мрежовата производителност
  - Част от наблюдението на Windows Server 2012
• Тестване на NLB за client access сървъри
  - Изготвяне на процедура за тестване
  - Веднъж месечно
  - С различни клиенти – Outlook и Outlook Web Access
  - При наличие на проблем – анализ и извършване на нужните корекции
• Тестване на DAG – отказоустойчивостта на отделните бази
  - Изготвяне на процедура за тестване
  - Веднъж месечно
  - С различни клиенти – Outlook и Outlook Web Access
  - Тестване на SMTP трафика
  - Тестване на бекъпа в случай на промяна в активната конфигурация
  - При наличие на проблем – анализ и извършване на нужните корекции

В поддръжката на Microsoft System Center 2012 R2 Virtual Machine Manager ще бъдат включени следните дейности:

- Осигуряване на централизирана администрация с управление на всички Hyper-V хост сървърни машини и на всички виртуални машини посредством инсталирани агенти
  - Ще се използва съществуващия Microsoft System Center 2012 R2 Virtual Machine Manager
  - Към инструмента за управление ще се добавят всички новоинсталирани Hyper-v сървъри, клъстери и виртуални машини
  - Инструментът ще се използва за конфигуриране на:
    - Настройки, свързани с хардуерните параметри на хостове и машини
    - Промяна и миграция на виртуалното дисково пространство на виртуалните машини
    - Промяна и миграция на виртуалната мрежова конфигурация на виртуалните машини
    - Инсталиране на нови виртуални машини
    - Подготовка на библиотеки с образци на машини и дистрибутиви на софтуер
- Конфигуриране и администриране на основни елементи: Фабрики, Мрежи, Управление на услуги. Управление на споделен масив от ресурси, които са присъединени към съответни хостове и/или цели услуги – композиция от фабрика и прилежащата й ИТ инфраструктура, които изградени като колекция от виртуални машини, представляват конкретна цялостна услуга
  - Първоначално ще бъде верифицирана конфигурацията на инструмента за управление:
    - Определяне на броя VMM сървъри и SQL бази към тях
    - Анализ на VMM инфраструктурата за управление
    - Определяне локацията на всеки един компонент
    - Анализ на текущата отказоустойчивост - сървър и SQL база
    - Оценка на хардуерна конфигурация - сървър и SQL база
    - Планиране на VMM библиотека - локация, отказоустойчивост и хардуерна конфигурация
    - Анализ на инфраструктура за софтуерни ъпдейти
  - Първоначално, а след това периодично, ще бъде верифицирана работоспособността на инструмента за управление:
    - комуникация с Hyper-V сървъри
    - комуникация с виртуални машини
    - статус на Виртуални Библиотеки
    - наличие на образци за виртуални машини
    - конфигурация на виртуални мрежи
    - конфигурация на виртуални дискови масиви
  - Конфигурация на отделните компоненти на инструмента при подмяна или миграция на хардуера:
    - VMM сървър за управление
    - VMM база от данни
    - VMM конзола
    - VMM библиотека
- Динамична Оптимизация – Осъществяване на балансиране на натоварването на хостове и виртуални машини на клъстерно ниво, посредством динамичен анализ и преместване на набор от виртуални машини към различни Hyper-V хостове,

чрез използване на специфичната функционалност за продукта: Live Migration – миграция на виртуални машини в реално време, без прекъсване (или с минимално) на тяхната наличност
    - Ще се извършва на база анализ на текущото натоварване на Hyper-v сървърите и изискванията за производителност на съответните виртуални машини
    - Ще се извършва ръчно или автоматично
- Оптимизация на изразходваната електрическа енергия - Като допълнение от горната функционалност, посредством динамична миграция на виртуални машини да се реализира гасенето на ненатоварени хостове и консолидация на виртуални машини
    - Ще се извършва на база анализ на текущото използване на виртуалните машини и услугите, които работят върху тях, броят използвани сървъри и текущата консумация на електроенергия
    - След изготвяне на отчет и анализ ще бъдат определени машини, подходящи кандидати за спиране – машини, които не се използват в извънработно време и които не са критични за работата на компоненти, работещи 24x7
    - Самото спиране на неизползваните машини и мигриране на работещите към други сървъри с цел консолидация ще се извършва автоматично
- Изграждане на правила за автоматизирано провизиране на нови виртуални машини (създаване, инсталиране, администриране) и поставянето им в оптималните хостове
    - Изготвяне на образци (темплейти) за виртуални машини – хардуерни и софтуерни, в зависимост от нуждите на различните системи, поддържащи НВИС
    - Анализ и изготвяне на препоръки за оптимално разположение на машините по съответните Hyper-v Клъстери
    - Изготвяне на процедура за провизиране на нова виртуална машина
    - Изготвяне на чеклисти за конфигурация на машините в зависимост от приложението им
- Bare-Metal Hyper-V провизиране – с развиването на тази функционалност да се реализира инсталиране на Hyper-V Хост върху нова, празна физическа сървърна машина
    - Изготвяне на процедура за провизиране на нови Hyper-v сървъри
    - Изготвяне на необходимите имиджи за дистрибуция
    - Конфигуриране на нужната функционалност в инструмента за управление
    - Тестово инсталиране на нов Hyper-v хост

В поддръжката на Microsoft System Center Configuration Manager (MS-SCCM 2012 R2) трябва да са включени минимум следните дейности:

- Администриране и конфигуриране на продукта и неговите роли:
    - Сайт сървър
    - База данни на сайта
    - Компонентен сървър
    - Точка за управление
    - Точка за дистрибуция
    - Точка за отчетност (reporting)

- Осигуряване на централизирана администрация с управление на всички клиентски машини, посредством инсталирани агенти:
  - Валидиране на текущата конфигурация и база с клиентска информация
  - Проверка за и отстраняване на грешки
- Следене за актуално състояние на софтуерното ниво на клиентските машини:
  - Изготвяне на отчет за текущите версии на използваните операционни системи продукти
  - Анализ на нови изисквания
  - Иницииране на нужните промени
- Автоматизирано осъвременяване на операционни системи с необходими и определени ъпдейти (пач мениджмънт):
  - Валидиране на текущата конфигурация
  - Отстраняване на грешки
  - Изготвяне на отчет за текущото ниво на ъпдейти на физически сървъри, виртуални машини приложения
  - Изготвяне на политика за софтуерно обновяване на различните системи в зависимост от препоръките на производителя и текущата конфигурация
- Създаване и прилагане на „Базова“ конфигурация – спазване и придържане към определено софтуерно ниво:
  - Дефиниране на базова конфигурация (baseline) за сървъри и приложения
  - Изготвяне на процедура за поддръжка и обновяване
  - Периодичен одит и изготвяне на отчети за несъответствия
- Инсталиране на операционни системи, напълно автоматизирано, посредством предефинирани шаблони:
  - Изготвяне на стандартни имиджи на операционни системи
  - Дефиниране на нужните колекции от клиенти – физически сървъри и виртуални машини, в зависимост от версията на операционната система
  - Изготвяне на процедура за провизиране на операционна система
- Инсталиране на софтуерни приложения на база на колекции, които са машинно или потребителски насочени
  - Изготвяне на стандартни пакети на приложения
  - Дефиниране на нужните колекции от клиенти – физически сървъри и виртуални машини, в зависимост от версията на приложението
  - Изготвяне на процедура за провизиране на приложението
- Динамично прилагане на платформени и инфраструктурни промени
  - Конфигуриране на интеграция между Microsoft System Center Configuration Manager и Microsoft System Center 2012 R2 Virtual Machine Manager
  - Конфигурация на WSUS сървъра
  - Настройка на динамични ъпдейти по фабриката

Таблица 8. Приложимост на дейностите

Компонент	Система	Периодичност	Резултат	Забележка

Компонент	Система	Периодичност	Резултат	Забележка
Компонент 7както е описан в т. 3.1.7 на ТС	Системен софтуер на Microsoft (Windows Server 2012/ 2012 R2, Microsoft Exchange Server 2013, Microsoft System Center 2012 R2 Virtual Machine Manager и Microsoft System Center 2012 R2 Configuration Manager)	При необходимост	Версиите на системния софтуер на Microsoft (Windows Server, Microsoft Exchange Server, Microsoft System Center Virtual Machine Manager и Microsoft System Center Configuration Manager) да са най-актуалните според изискванията на приложното програмно осигуряване на НВИС, системите за управление на бази от данни и всички останали софтуери за управление и поддръжка	

3.1.10. Изготвяне на документация

Продължителност: За целия период на договора.

Приемане на дейността: с приемо-предавателен протокол.

Изпълнителят ще изготви подробна техническа документация на всички промени в подсистемите на ИТ средата и взаимовръзките и зависимостите между тях: мрежова, сървърна и дискова инфраструктура, операционни системи, бази данни, сървъри за приложения и приложения.

Изпълнителят ще изготви и актуализира инвентарни списъци на наличните оборудване и програмно осигуряване в електронен вид и ще ги обновява при промени, възникнали по времето на изпълнение на договора.

Техническата документация и списъците, съдържащи всички направени промени по ИТ средата, ще бъдат предадени на Възложителя при приключване изпълнението на задълженията по договора.

Приложимост:

Таблица 9. Приложимост на дейностите

Компонент	Система	Периодичност	Резултат	Забележка

Компонент	Система	Периодичност	Резултат	Забележка
Всички, както са описани в т. **Error! Reference source not found.** на ТС	Всички	За целия период на договора	Наличие на актуална документация за състоянието на ИТ средата.	

3.2. Осъвременяване на оборудването по Компонент 2

Изпълнителят ще достави на техника за осъвременяване на Компонент 2 – подробно описана в Приложение 2 към Техническата оферта - Техническо предложение за осъвременяването на оборудването по Компонент 2

Услуги, които Изпълнителят ще извърши след доставката на оборудването:

Целият хардуер, компоненти, модули, части и софтуерни продукти ще се инсталират и тестват, за да се валидира тяхната функционалност, в работните помещения на Възложителя.

Изпълнителят ще свърже логически и физически доставеното оборудване към наличната SAN среда.

Изпълнителят ще подготви документация за изграденото решение, която да съдържа логическата и физическата свързаност на устройствата към SAN и LAN мрежата.

Оборудването ще бъде доставено в рамките на 2 месеца след приемане на първоначалния доклад по т.3.1.1

Оборудването ще бъде инсталирано и пуснато в експлоатация до 1 месец след неговата доставка. Инсталацията ще е направена в основния и резервния център за управление на данни.

Изпълнителят ще мигрира системите към ново инсталираните изчислителни мощности съгласно приетия план за дейностите от Възложителя по т.3.1.2, но не по-късно от 3 месеца след неговата инсталация.

Гаранционният срок от производителя на новодоставеното оборудване ще бъде минимум до 31.12.2019г.

3.3. Обучение

3.3.1. Обхват

Изпълнителят ще организира и провежда ежегодни работни семинари за поне 2-ма служители на Възложител. Семинарите ще включват обзор на цялостната среда и инструментите за нейното администриране и наблюдение.

Програмата за обученията е подробно описана в Приложение 1 към Техническата оферта.

3.3.2. Курсове

Изпълнителят ще осигури адаптирани за Възложителя курсове на обучение, от обучаващи, сертифицирани от производителя на съответния компонент, покриващи следните области:

Таблица 10. Списък на курсове и обучения

Курс	Времетраене (минимум)	Бр. участници	Забележка
Конфигурация и администриране на мрежовата и комуникационна инфраструктура от Компонент 1	3 дни	поне 2	
Конфигурация и администриране на сървърната и лентова инфраструктура от Компонент 2 и новото оборудване	3 дни	поне 2	
IBM Tivoli Storage Manager Курс съгласно официалната програма за IBM TSM Advanced administration, tuning and troubleshooting	5 дни	поне 2	Официално сертифицирано обучение
Администриране на Steria Interconnection Box for VIS и Steria CompliTT	3 дни	поне 2	
Администриране на СУБД IBM Informix Informix database administration training	4 дни	поне 2	Официално сертифицирано обучение
Администриране и конфигуриране на Microsoft Windows Server и Active Directory, Администриране и конфигуриране на Microsoft System Center и Hyper-v, Администриране и конфигуриране на Microsoft Exchange Server	3 дни	поне 2	
ITIL Foundation	3 дни	поне 2	Официално сертифицирано обучение.

Обученията ще се водят от сертифицирани за продуктите, обект на обучение, лектори. Лекторите ще са сертифицирани съгласно сертификационна програма за обучение на производителите на съответния компонент, като сертификатите ще са валидни към дата на провеждане на обучението.

Обученията ще се организират в зали на МВнР или в зали на Изпълнителя.

Обученията ще бъдат на български език или с осигурен превод; и ще се провеждат до 5 учебни часа на ден.

Учебните материали ще бъдат на български или на английски език.

Обученията ще осигурят на служителите на Възложителя знания и умения за осигуряване на първото ниво на поддръжка на оборудването.

3.3.3. Протоколи и сертификати

Дейността приключва с подписване на протоколи за проведено обучение и сертификати за успешно завършен курс на обучение за всеки служител на Възложителя. Всеки протокол се подписва от Изпълнителя и Възложителя. Окончателният протокол за проведените обучения се подписва от Изпълнителя и Възложителя..

3.4. Поддръжка при инциденти и проблеми.

Всички дейности ще се изпълняват при следните условия:

3.4.1. Обхват на предоставяните дейности по поддръжката

Всички дейности ще се предоставят така, че да осигурят наличност на услугите, предоставяни от визовия център 24 часа в денонощието, без почивен ден. Услугите по поддръжка ще се предоставят в работни дни от 8 до 18 часа на следните адреси:

Таблица 11. Визови центрове

N	Център	Адрес
1	Национален визов център	гр. София, ул. „Ал. Жендов“№ 2
2	Резервен визов център	гр. София, ул. „Витошко лале“№ 16
3	Колеж по телекомуникации	гр. София, ул. „Акад. Стефан Младенов“ № 1

Изпълнителят е отговорен за поддръжката, администрирането, диагностиката и ремонта на системата, която се състои от софтуерните и хардуерните компоненти.

Изпълнителят гарантира наличността на резервни части и модули, необходими за поддръжката.

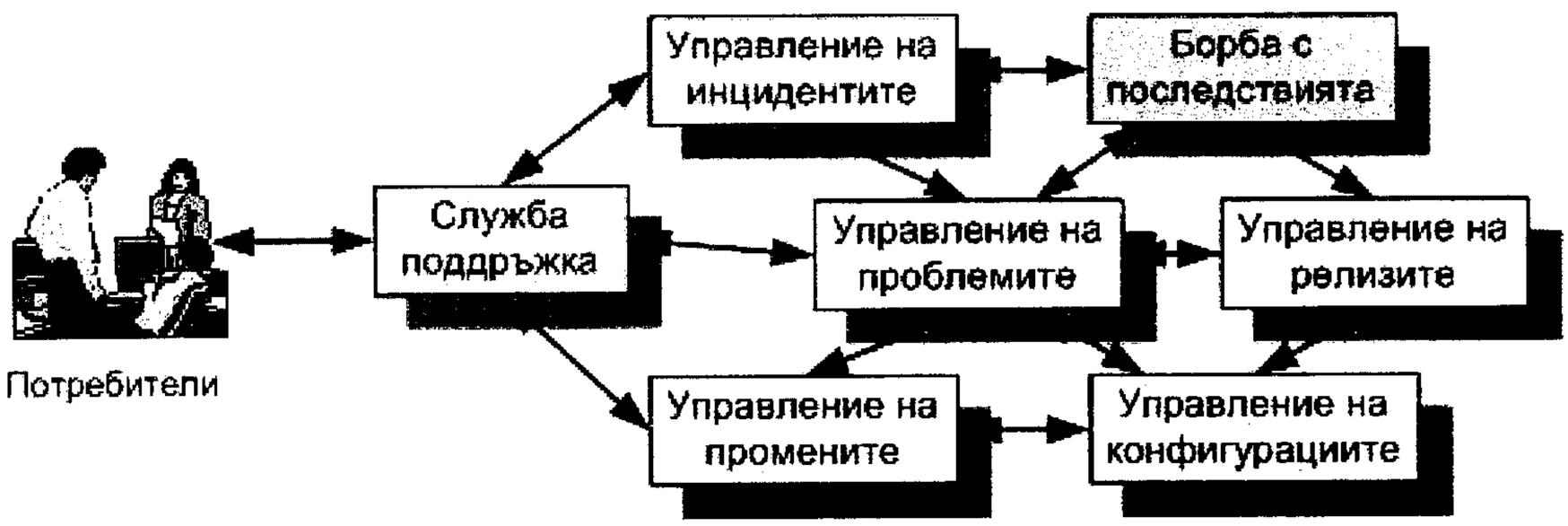
3.4.2. Планова поддръжка и профилактика

Планова поддръжка ще се осъществява по съгласуван (поне две седмици предварително) с Възложителя план-график.

Процедура за управление на възникналите проблеми и организация за реакция при възникнал проблем

Всички процеси по Планова поддръжка и профилактика ще са съгласно най-добрите практики при обслужването на ИТ системи в съответствие с ITIL книга Поддръжка на услуги (Service Support) част от методологията ITSM версия 2, състояща се от следните части:

- Служба Поддръжка (Service Desk)
- Процес за управление на инцидентите (Incident Management)
- Процес за управление на проблемите (Problem Management)
- Процес за управление на конфигурациите (Configuration Management)
- Процес за управление на промените (Change Management)
- Процес за управление на релизите (Release Management)



Служба за поддръжка (Service Desk)

Създава се за осигуряване на ефективна поддръжка на потребителите и взаимовръзка на процесите от операционното ниво.

Задача

Откриване на проблемните участъци в ИТ инфраструктурата и ефективността от работата на ИТ службите.

Осъществява техническа поддръжка за решаване проблеми на потребителите с компютрите, апаратните и програмни средства

Схема на работа

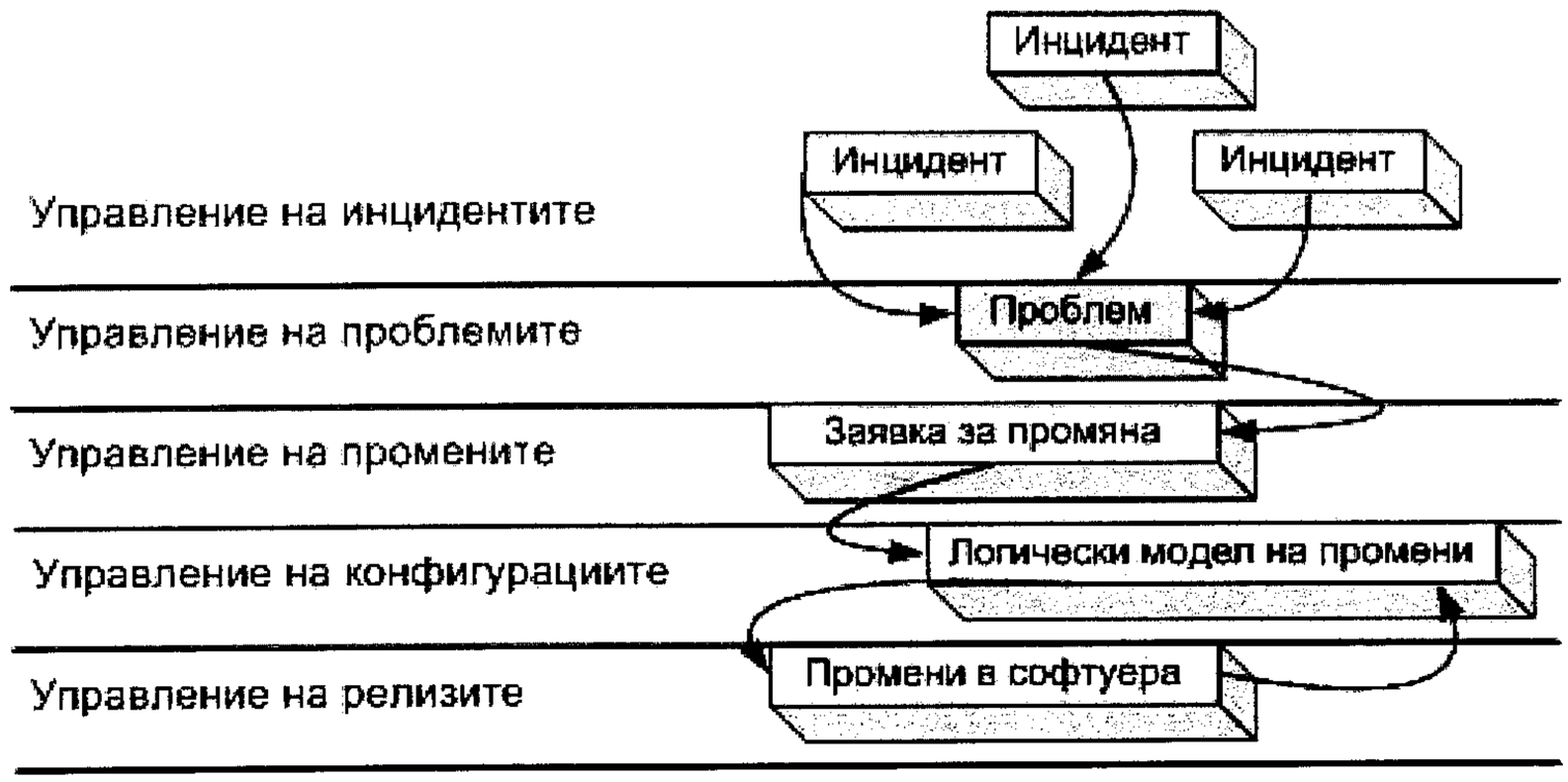
Представител на Възложителя или краен потребител прави заявка за инцидент → Оператора категоризира заявката и при възможност помага на потребителя да реши проблема с помощта на база знания → Координатора назначава специалист за решаване на заявката и фиксира изпълнението и → Специалистът решава проблема или го връща на координатора.

Логически компоненти

- Модул за регистрация заявките за инциденти;
- База данни за заявки;
- Система за проследяване статуса на заявките и известяване;
- База знания;
- Панел за администриране.
- Модул за отчетност.

Управление на инциденти (Incident Management)

Осигурява непрекъснато предоставяне на услуги.



Основна задача - скоростно възстановяване на услугите на съгласувано ниво в случай на повреда (или заплаха за повреда).

Характерни особености

- Залага се на скоростта на възстановяване, като след това се обръща внимание на надеждността, универсалността или системността на решението;
- Отделя се като процес "борбата с последствията", което позволява да осигури непрекъснато предоставяне на услуги и да се създаде база за разследване и отстранение на причините за повреди в рамките на процеса.

Управление на проблеми (Problem Management)

Минимизиране на прекъсванията при предоставяне на услуги, като за целта се решават задачи по идентификация, разследване и отстранение на причините за възникване на повреди.

Характерни особености

- Анализира инфраструктурата и формира предложения по нейното изменение с цел повишаване на стабилността;
- Предложенията, формализирани Заявки за изменения (Request For Change), служат като входна информация за процеса Управление на промените.

Профилактика на инсталираното оборудване ще се извършва при запазване функционалността на системите и ще включва като минимум:

- **Тестване на всички функционалности на системите**:
- Тестването на функционалности на системи се заключава в извършването на проверка на коректното функциониране на системите като цяло или на отделни техни компоненти.
- Сравняват се предварително известни и очаквани стойности на различни параметри с реално измерени / проверени стойности.

- В зависимост от характера на тестваната система се допуска проверка на функционалността ѝ чрез подаване на входни данни /или въздействие на вход/, като изходните данни /или резултат на изход/ се сравняват с очакваните данни или резултати при нормално функциониране на системите.
- Получените данни се анализират, като се проверява дали съвпадат с очакваните резултати.
- Ако получените стойности / резултати съвпадат с предварително очакваните или са в рамките на допустимо отклонение, съгласно експертна оценка, съответният тест се приема за успешен.
- Провеждането на тестове за функционалност на системи се документира, като се описват:
    - Тествана система
    - Обхват на теста
    - Параметри
    - Процедури, които ще се изпълнят по време на теста
    - Получени резултати, стойности и т.н.
    - Критерии за приемане
    - Общ резултат от теста
    - Имена и длъжност на провеждащите теста лица
    - Имена и длъжност на проверяващо лице

- **Преглед на хардуерната част за установени дефекти:**
- Дейностите по преглед на хардуерна част на система се извършват съгласно плана за профилактика на оборудването.
- Наблюдават се светлинни индикатори на устройствата за индикации за грешки, съгласно спецификациите в документацията на производителя.
- Наблюдават се дисплеи на устройствата (напр. front panel) за изведени съобщения за грешки .
- Проверява се хардуера за нехарактерен шум при работа.
- В случай на открити грешки в работата на хардуера, същите се регистрират в протокола от извършения преглед и се отваря ЗСУ за отстраняване на регистрирания проблем.
- **Отстраняване на прах и други замърсители от повърхността и вътрешността на оборудването**:
    - Преглеждат се повърхността и вътрешността на оборудването за прах и замърсители и същите се отстраняват.
    - Специално внимание се обръща на местата около въртящи се части, вентилатори, охладители и други, в околност на които традиционно се отлагат прах и замърсители.
    - При отстраняване на прах и други замърсители от вътрешността на оборудването, когато ситуацията го налага, се извършва:
        - Изваждане на охлаждания / вентилатори
        - Почистване на прашните радиатори и вентилатори

- Почистване на останалия прах в оборудването
- Монтиране на охладителните модули и вентилатори

Изпълнителят уведомява Възложителя поне две седмици предварително за всички промени в графика за планирани ремонти и планирани профилактични прегледи.

3.4.2.1. Докладване на инциденти

Всички заявки и съобщения се считат за направени, след като Възложителят ги е изпратил на Изпълнителя на посочени от Възложителя телефон/факс или e-mail адрес.

Изпълнителят ще осигури гореща телефонна линия, достъпна 24 часа в денонощието, без почивен ден.

3.4.2.2. Време за реакция

Таблица 12. Времена за реакция

N	Тип на дейността	Време за реакция
1	Дистанционни дейности	До 15 минути след докладване на инцидент съгласно т. 3.4.2.1 от ТС
2	При необходимост от "ремонт на място"	До 18:00 часа на следващия работен ден, считано от времето на докладване на инцидент съгласно т. 3.4.2.1 от ТС

Дистанционните дейности ще могат да се прилагат в много ограничен обхват. Системата не позволява достъп извън територията на НВЦ и РВЦ.

3.4.2.3. Време за разрешаване на инцидент

Ниво на критичност	Време за намиране на временно решение (заобикаляне на проблема)	Време за пълно разрешаване на инцидента
Високо (Заплаха за спиране на НВИС или основни инфраструктурни системи)	4 часа	До 18:00 часа на следващия работен ден (ако не е станало автоматично)
Средно (Заплаха за липса на резервираност)	8 часа	В рамките на два работни дни
Ниско (Потенциална заплаха за инцидент)	24 часа	В рамките на пет работни дни

Ако възникнал проблем блокира цялостната работа на системата, но позволява активирането на Резервния център и ако времето за заобикаляне/отстраняване на

проблема надвишава 1 час, то се пристъпва към активиране на Резервния център, съгласно подробно разписан при Възложителя план за работа при критични ситуации.

3.4.3. Структуриране на поддръжката

Предвижда се поддръжката да се осъществява на следните две нива:

3.4.3.1. Първо (Базово) ниво

Това е нивото на поддръжка от страна на Възложителя. Извършва се първоначално диагностициране на възникналите проблеми от служителите на Възложителя, преди да бъде отправено официално искане за извършване на сервизно обслужване. Това включва: събиране на нужната информация, базово диагностициране на проблема, както и дейности за неговото отстраняване при възможност.

3.4.3.2. Второ (Разширено) ниво

Позволява решаване на проблема, в зависимост от неговата специфика и сложност, като се извършва от Изпълнителя, съгласно неговата вътрешна организация и вътрешни процедури на работа и се съгласува с Възложителя.

3.4.4. Ред за извършване на техническото обслужване

Заявката за отстраняване на възникнал проблем с оборудването се подава от упълномощен представител на Възложителя на посочен от Изпълнителя телефон, електронен адрес или факс. Отбелязва се датата и часа на подаване на заявката. Заявката трябва да съдържа информация за: проблема; часа и датата, когато е констатиран проблема; вероятния характер на повредата.

3.4.4.1. Тримесечни доклади за възникнали проблеми и повреди

Изпълнителят изготвя 3 месечни доклади за изпълнение с пълен запис на всички заявки и извършени дейности.

3-месечните доклади се изготвят до 5-то число на следващия месец след изтичане на предходното тримесечие. Докладите подлежат на съгласуване и одобрение от Възложителя.

3.4.4.2. Специални условия

Достъпът на Изпълнителя до помещенията, в които се намира оборудването, обект на договора, ще се извършва по начина и във времето, допустими съгласно правилата и инструкциите за организация на охраната и пропускателния режим в двата визови центъра на Възложителя (НВЦ и РВЦ).

Дата: 25.05.2016

Представляващ ДЗЗД Ай Би Ес Индекс, съгласно Договор за консорциум от 19.05.2016,

Горан Ангелов, Управител на Водещ съдружник Ай Би Ес – България ЕООД:

(печат на Водещ съдружник, съгласно т. 3.5. от Договор за консорциум от 19.05.2016)

ФОНД „ВЪТРЕШНА СИГУРНОСТ“

Приложение 5

Методология за управление на риска при изпълнение на проекта съгласно изискванията на Техническата спецификация

към

ТЕХНИЧЕСКА ОФЕРТА

за участие в открита процедура за възлагане на обществена поръчка с предмет: "Поддръжка и обновяване на програмното и техническо осигуряване на Националната визова информационна система и на визовата дейност в консулските служби на Р България",

Обособена позиция 1: „Поддръжка и осъвременяване на техническото осигуряване и инфраструктурата на НВИС“

От КОНСОРЦИУМ ДЗЗД „Ай Би Ес Индекс”

МЕТОДИ ЗА УПРАВЛЕНИЕ НА РИСКА

Съдържание

1. ВЪВЕДЕНИЕ

Анализът на риска има за цел да идентифицира всички рискове свързани с експлоатацията на Визовата Система, да оцени потенциалното им влияние, както и вероятността съответните рискове да се случат. На тази база ще бъдат предложени мерки за справяне критичните рискове. Използвана е методология за анализ на риска описана в "ISO 31000 – Risk Management", както и "BS 31100 - Risk management – Code of practice and guidance for the implementation of BS ISO 31000". Тези стандарти описват подробно как се извършва анализ на рисковете и как да се прилага методологията за анализ на рисковете. Принципите залегнали в тези стандарти са следните:

- Управлението на риска създава и запазва добавена стойност
- Управлението на риска трябва да бъде интегрална част от всички организационни процеси
- Управлението на риска играе важна роля при взимане на решения
- Управлението на риска адресира несигурността
- Управлението на риска е систематичен, структуриран и периодичен подход
- Управлението на риска се базира на достъпната информация в рамките на организациите
- Управлението на риска взима под внимание човешкия фактор в организацията, както и нивото на зрялост
- Управлението на риска се извършва посредством процес за идентифициране и управление на риска

По време на изпълнението на проекта екипът на изпълнитля ще поддържа списък на рисковете - структурирано описание на известните и реално стоящи рискове пред проекта, подредени по реда на тяхното идентифициране. Към всеки риск ще бъдат идентифицирани мерки за ограничаване на последствията и евентуални действия при настъпване на риска. Планът за действие ще бъде изпълняван към рисковете попадащи в категорията критичните и сериозни рискове.

Регистърът на рисковете се изготвя и поддържа през целия проект в следния табличен вид:

№	Категория	Описание	Действие върху проект	Собственик (Отговорник)	Приоритет	Степен на влияние	Вероятност	Индикатор	Стратегия за смекчаване
1	Управленски рискове	Недостиг на компетентност и умения в рамките на проектния екип	Забавяне на целия проект	Възложител Изпълнителя	4	Значителна	Минимална (1 - 20%)	Неизпълнени срокове и липсващи одобрения на ключови дейности	

Рискът се идентифицира с пореден номер, който се записва в първата колона. Втората колона съдържа описание на риска, а третата – резюме на възможните последствия. В колона "Собственик (Отговорник)" се посочва(т) лицето или организацията (лицата или организациите), което отговаря (които отговарят) за противодействието на съответния риск. Скалата на приоритетите е от 1 до 8, като 1 е с най-нисък приоритет, а 8 е с най-висок.

2. ПРОЦЕДУРА ЗА УПРАВЛЕНИЕ НА РИСКА

Процедурата има за цел да осигури и поддържа ефективно управление на рисковете свързани с дейността на Визовата Система.

Процедурата се прилага за оценка на риска на активите (информационни системи или други активи), които са включени в обхвата на Визовата Информационна Система.

2.1 Термини и съкращения

Сигурност на информацията	Запазване на поверителност, цялостност и наличност на информацията.
Събитие, свързано със сигурността на информацията	Идентифицирана проява на състояние в система, услуга или мрежа, показваща възможно нарушаване на политиката по сигурност на информацията, пробив на защити или неизвестна до момента ситуация, засягаща сигурността.
Актив	Всяко нещо, което има стойност за организацията.
Информационен актив	Материалните и нематериалните активи, свързани с информационна система, които имат полезна стойност за организацията.
Наличност на информацията	Свойството за достъпност и използваемост на информацията при заявка от упълномощено лице.
Поверителност на информацията	Свойството на информацията да не се предоставя или разкрива пред неупълномощени лица, служители или процеси.
Цялостност на информацията	Свойството за опазване на точността и целостта на активите.
Заплаха	Потенциална причина за нежелан инцидент, който може да навреди на система или организация.
Уязвимост	Слабост на актив или група активи, която може да бъде използвана от една или повече заплахи.
Риск	Комбинация от вероятността на дадено събитие и неговото последствие.
Анализ на риска	Систематично използване на информация с цел да се идентифицират източниците и да се прецени рискът.
Преценяване на риска	Цялостен процес на анализ и оценяване на риска.

Оценяване (оценка) на риска	Процес на сравняване на оценения риск с дадени критерии за риск, за да се определи неговата значимост.
Остатъчен риск	Рискът, който остава след въздействието върху риска.
Приемане на риска	Решение да се приеме рискът.
Управление на риска	Координирани действия за насочване и контролиране на организацията по отношение на риска.
Риск за сигурността	Фактическо състояние, което създава заплахи за уязвяване на един или няколко информационни актива, което да предизвика тяхното повреждане или унищожаване.
Въздействие върху риска	Процес на подбор и прилагане на мерки с цел изменение на риска.
Остатъчен риск	рискът, който остава след въздействието върху риска
Приемане на риска	решение да се приеме рискът
Анализ на риска	систематично използване на информация с цел да се идентифицират източниците и да се прецени рискът
Преценяване на риска	цялостен процес на анализ и оценяване на риска
Оценяване на риска	процес на сравняване на оценения риск с дадени критерии за риск, за да се определи неговата значимост
Управление на риска	координирани действия за насочване и контролиране на организацията по отношение на риска
Въздействие върху риска	процес за подбор и прилагане на мерки с цел изменение на риска

2.2 Отговорности

Ръководител контрол на риска

- Контролира цялата дейност по оценката на риска като одобрява процедурите и инструкциите от Системата за управление;
- Одобрява извършената оценка на риска като утвърждава Протокола за неговата оценка;
- Разрешава промените (придобиването или отписването) с цел определяне на риска на активите, включени в Системата за управление по отношение на сигурността на информацията.

Мениджърите/Ръководителите на функционални направления управляващи съответната дейност:

- Участват в разработването на процедурите и инструкциите от Системата за управление на сигурността на информацията;
- Предлагат за закупуване или отписване на активи, свързано с необходимостта за правилното и безопасно функциониране на направленията / дейностите, които управляват;

- Отговарят за организацията на правилното използване на активите, които се намират в ръководените от тях направления /дейности по отношение на сигурността на информацията;
- Предлагат на Управителя да наложи по съответния ред дисциплинарни наказания на служителите, които нарушават настоящата процедура или инициира съдебна процедура в зависимост от нарушението.
- Участват в оценката на значимостта на активите и техният риск за сигурността на информацията.

Ръководител по информационна сигурност:

- Организира и контролира цялостната дейност по осигуряване на защитата и оценката на риска на активите, включени в обхвата на Системата за управление по отношение на сигурността на информацията;
- Участва в разработването на процедурите и инструкциите от Системата за управление, свързани със сигурността на информацията;
- Предлагат за закупуване или отписване на активи, свързано с необходимостта за правилното и безопасно функциониране на Системата за управление по отношение на Визовата Информационна Система;
- Контролира своевременното вписване на новите активи в съответните регистри и тяхното отписване при изваждането им от употреба;
- Определя отговорници за съответните активи, като контролира изпълнението на задълженията им;
- Изготвя отчетите, свързани със сигурността на информацията и оценката на риска като част от отчетите на Визовата Информационна Система;
- Предлага на ръководството да наложи по съответния ред дисциплинарни наказания на служителите, които нарушават настоящата процедура или инициира съдебна процедура в зависимост от нарушението;
- Организира изпълнението на предписаните превантивни и коригиращи действия от проведени вътрешни и външни одити

Собственик на актив:

- Изпълнява изискванията на всички процедури и инструкции по отношение на сигурността на информацията и свързани с активите, за които отговарят или имат разрешен достъп;
- При забелязване на инциденти със сигурността на информацията, свързани с активите, след изясняване на проблема и евентуалната причина, незабавно информира Ръководител по сигурността на информацията;
- Участва в дейностите по оценка на риска на активите, свързани с обработката и съхранението на класифицираната информация;

2.3 Управление на риска

2.3.1 Изисквания

Управлението на риска за Визовата Информационна Система включва следните етапи

- избор на обектите за оценка на риска;
- идентифициране на информационните активи, свързани с Визовата Информационна Система;

- идентифициране на заплахите за тези активи и уязвимостите, които могат да бъдат използвани от тях;
- избор на методология за оценка на риска;
- оценка и приемане на риска;
- избор на защитни мерки и въздействие върху риска;
- реализация и проверка на избраните мерки;
- оценка на остатъчния риск;
- оценка на ефективността на приложените мерки;

2.3.2 Избор на обектите за оценка на риска

В оценката на риска на Визовата Информационна Система се включват тези активи (информационни системи или други активи), при които са възможни последствия като загуба на поверителност, на цялостност и наличност на информацията; пропуснати ползи, както и потенциални щети или неблагоприятно влияние върху бизнеса вследствие на инцидент, свързан с тях.

За целите на оценката на риска, активите може да бъдат групирани по:

- дейности (информационни системи, процеси);
- информационни активи (т.е. хардуер, софтуер, бази данни, записи с информация),
- хора (т.е. персонал, клиенти, доставчици и др.),
- обкръжаваща среда (т.е. сгради, офиси, съоръжения).

2.3.3 Идентифициране на заплахите и уязвимостите за активите

Примерен списък на заплахите за сигурността на активите в обхвата на информацията и уязвимостите, които могат да бъдат използвани от тях е даден в Приложение 1

Списъкът не е напълно изчерпателен и за определени активи при необходимост може да се идентифицират други заплахи или уязвимости.

2.3.4 Методика за оценка на риска

Целта на методиката е да оцени рисковете, на които са изложени активите, за да се установят и изберат подходящи защити на тяхната сигурност. Рисковете са функция на значимостта на активите в опасност, вероятността от поява на заплахи, които да причинят потенциални неблагоприятни бизнес влияния, уязвимостите на установените заплахи и всички съществуващи или планирани защити, които могат да намалят риска.

Какъвто и метод да се приеме, за да се прецени мярката на риска, резултатът от този етап трябва да е списък на установените рискове за сигурността на услугите.

За оценка на риска на активите за сигурността на информацията, свързана с дейността на Визовата Система се прилага метод, основан на експертната оценка на всички заплахи и свързаните с тях уязвимости за даден актив.

Риск = Вероятност X Влияние

В използваната методика рисковете са функция на:

- значимостта на активите;
- възможните заплахи и свързаната с тях вероятност за появата им, която може да застраши съответните активи;
- свързаните с активите уязвимости и потенциални нежелани въздействия върху активите;
- съществуващите или планирани защити, които трябва да намалят тежестта на нежеланите въздействия на уязвимостите и свързаните с тях заплахи.

Значимостта на активите е дадена по-долу:

Поради разнообразния характер на активите, възможно е някои от тях да бъдат оценени количествено директно по тяхната финансова стойност, но за други това е невъзможно. Прилагането на качествена оценка на значимостта на активите има универсален характер, като определените стойности могат да варират – например от „много ниска” до „много висока” с произволен брой стъпки между тях.
При оценка на значимостта на активите на Визовата Система се прилага следната 3-степенна скала:

ЗНАЧИМОСТ	СТОЙНОСТ
Ниска	1
Средна	2
Висока	3

Оценяването на значимостта на активите се извършва под ръководството на Ръководител по сигурността с участието на отговорниците на съответните активи. При необходимост може да се потърси съдействието на служителите, които ползват активите или участват в дейностите по бизнес планиране, финансиране или поддържане на активите.

Оценяване на значимостта на активите се извършва експертно в зависимост от вида на актива. В зависимост от вида на актива при оценяването му се отчитат възможните последствия от загуба на поверителност, на цялостност и наличност на информацията, свързана с него или на пропуснатите ползи; потенциалните щети или неблагоприятното влияние върху бизнеса вследствие на инцидент. Ако е приложимо, при определяне на значимостта на актива се използва и неговата първична цена, стойността му при замяна и възпроизвеждане, а също и значението му за доброто име и репутация на дружествата.

За окончателната стойност на значимостта на актив се приема максималната от всички възможни стойности на неговата значимост.

Оценяването на значимостта на активите на Визовата Система се извършва с помощта на следните критерии, с които се определя големината на възможните щети в резултат на загуба на поверителност, цялостност или наличност на информацията:

- нарушаване на законовите и други нормативни изисквания;
- загуба на клиенти;
- отрицателен ефект върху репутацията на дружествата;
- инциденти, свързани с личната информация;
- излагане на опасност на личната сигурност;
- инциденти с поверителността на търговските дейности;
- нарушаване на обществения ред;
- финансови загуби;
- влошаване на бизнес дейностите;
- излагане на опасност на сигурността на околната среда.

На оценка на риска се подлагат активи със средна и висока значимост за компанията

За реална оценка на заплахата се взема предвид вероятността за нейната поява, която зависи от:

- привлекателността на актива, свързан със заплахата за преднамерена човешка намеса;

- лесното получаване на облаги от преднамерената човешка намеса;
- техническите възможности на реализация на заплахата от преднамерена човешка заплаха;
- периодът от време, в което активът се използва и има нужда от защита.

Вероятността се оценява в съответствие с **Таблица 1**

Вероятност	**Обяснение**	**Оценка**
Незначителна	много малко вероятно да се случи	0
Много ниска	2-3 пъти за 5 годишен период	1
Ниска	До 1 път годишно	2
Средна	До 2 пъти годишно	3
Висока	До 1 път месечно	4
Много висока	Повече от 1 път месечно	5
Изключително висока	Няколко пъти в рамките на седмица или ден	6

Таблица 1

Влиянието на свързаните с активите уязвимости (технически и нетехнически) върху сигурността на информацията се оценява, като се използват качествени критерии. Критериите се оценят в съответствие с **Таблица 2**:

Ниво на влияние	**Обяснение**	**Оценка**
Незначителна	Никакво влияние	0
Минимално	Не е необходимо усилие/средства за да се възстанови или поправи	1
Значително	Реални щети, необходимо е усилие/средства за да се възстанови или поправи	2
Увреждащо	Щети на репутация или конфиденциалност. Значителни разходи на усилие и/или средства за да се възстанови или поправи	3
Сериозно	Продължително отпадане на актив/услуга и/или загуба на свързаност Компрометирани големи обеми от данни или услуги	4
Изключително	Отпадане на част от бизнес процес. Невъзможност да се възстанови актив/услуга.	5

Таблица 2

При определяне на критериите за уязвимост се отчитат всички въведени мерки за защита на оценявания актив, както и адекватността на мерките.
За оценката на риска, съответният актив (или група от активи) се съпоставя с възможната за него заплаха и отговарящата й уязвимост, като се отчитат присъщата му уязвимост.
Заплахите могат да бъдат:

- Форс мажорни събития
- Организационни проблеми
- Управленски

- Човешки грешки
- Технически грешки
- Преднамерени, злоумишлени деяния

Заплахите могат да бъдат случайни или предумишлени. И случайните и предумишлените източници на заплаха трябва да бъдат отчетени и да бъде оценена вероятността за тяхната поява.
Ако за един актив са възможни няколко заплахи или няколко уязвимости, свързани с определена заплаха, то рискът се оценява поотделно за всеки отделен случай.
Наличието на уязвимост само по себе си не причинява вреда, а трябва да има налична заплаха, която да я използва. Уязвимост, за която няма съответстваща й заплаха, не изисква прилагането на защита, но трябва да бъде разпозната и да се наблюдава за промени. Трябва да се отчете, че неправилно въведените, нефункциониращите или неправилно използваните защити могат сами по себе си да бъдат уязвимост.
Нивото на риска се изчислява във скалата на **Таблица 3**

Ниво на Риск	**Скала**
Нулево	0
Ниско	1 до 3
Средно	4 до 8
Високо	9 до 14
Критично	15 до 19
изключително	20 до 30

Таблица 3

Резултатите от оценката на риска се нанасят в Протокол за оценка на риска.
Процесът на управление на риска е цикличен процес. Крайният етап се явява начало на нов цикъл на оценка на риска. Новият цикъл се провежда когато:
а) Остатъчният риск не удовлетворява ръководството;
б) Са настъпили съществени изменения в структурата на активите или са въведени нови информационни системи или активи;
в) След изтичане на срока, определен в процедурата

2.3.5 Оценка и приемане на риска

Началната оценка за рисковете се прави от работна група под ръководството на Ръководител по сигурността.
Входящите данни за оценката на риска се получават от отговорницита на активите или техните потребители, от специалистите, които планират активите и ги поддържат, както и от хора, отговорни за охраната на сградите и офисите. Друг източник на информация за оценка на рисковете са приложимите за дейността на Визовата Система, законови и други нормативни актове.
Оценката на риска за активите (информационни системи или други активи), които са включени в обхвата на Визовата Система по отношение на сигурността на информацията се прави по определена методика.
Ако за един актив са възможни няколко заплахи или няколко уязвимости, свързани с определена заплаха, то рискът се оценява поотделно за всеки отделен случай.

Резултатите от оценката на риска се нанасят в Протокол за оценка на риска. Съветът по сигурност на информацията разглежда и обсъжда Протокола и го предлага за одобрение от ръководството.

Въвеждат се следните нива на приемливост на риска:

За приемливи рискове на активите (информационни системи или други активи), свързани със сигурността на информацията се приемат тези със стойност до средно ниво включително. За активите с оценка на риска над средно ниво се въвеждат нови мерки за защита и се прави повторна оценка на риска.

Този цикъл се повтаря, докато се получат приемливи стойности на риска за съответния актив. Нова оценка се прави и когато настъпят съществени изменения в структурата на активите или са въведени нови информационни системи или активи.

Всяка година под ръководството на Ръководител по сигурността оценката на риска се преразглежда, като се изготвя съответния Протокол.

При всяка оценка на риска трябва да се използват еднакви критерии и стойности за съответната заплаха или уязвимост, за да има възпризводимост и повторяемост на резултатите.

Резултатите от анализа на риска водят до избор и въвеждането на защитни мерки (защити), които да бъдат използвани за намаляване на оценените рискове до приемливо ниво. Защитните мерки се описват в детайли в План за третиране на риска.

2.3.6 Избор на защити и тяхното прилагане

При установяване на риск над приемливия трябва да се предприемат ефективни и икономични мерки за неговото снижаване и оценка дали резултативният риск е в приемливи граници.

При идентифициране на риск над приемливия, се предприема едно от следните действия:

а) ликвидиране на риска (например чрез отстраняване на причиняващите го обстоятелства);

б) намаляване на риска (например чрез използване на допълнителни защитни средства);

в) приемане на риска и разработване на план за действия в обстановка на риск;

г) преадресиране на риска (например чрез сключване на договор с друга организация за изпълняване на съответната дейност с приемлив риск или за съответната застраховка).

Защитите, въведени след прегледа на анализа на риска трябва да бъдат допълнение на вече съществуващите, за да се избегне излишното дублиране на защити.

Проверява се дали избраните защити са съвместими със съществуващите и планираните защити, т.е. избраните и съществуващите защити трябва да бъдат съвместими, тъй като защитата, която не функционира правилно, е източник на възможна уязвимост.

За изпълнение на Защитните мерки се назначава съответен отговорник, изпълнител както и предварителен срок за изпълнение. Разработва се съответния План за третиране на риска, в който се адресират всички остатъчни рискове над приемливото ниво за рискове на Визовата Система.

Когато се установи, че вече съществуващите защити не изпълняват своите функции, Ръководителят по сигурността прави аргументирано предложение на Съвета по

сигурност на информацията съответната защита да бъде премахната, заменена с друга по-подходяща или да бъде усъвършенствана.
Оценката на ефективността за предприетите мерки за свеждане на рисковете до приемливи нива за министерството и се провежда при повторния анализ на рисковете.
В планът за третиране на риска за всяка мярка (или комплекс от мерки) се прилага оценка на остатъчния риск след прилагането на мярката. Оценката на риска се провежда по методологията дадена по-горе в текущия документ.
В оценката на риска се сравнява планирания остатъчен риск от плана за третиране на риска с реално отчетения. Ако резултантния риск е по-малък или равен на планирания остатъчен риск се счита че мярката е ефективна. В случай на избор на не-ефективна мярка се прави допълнителен анализ за причините за не-ефективността и се докладва на ръководството.

2.4 Оценка на риска

Предназначение

Протоколът има за цел да опише резултатите от проведения анализ на заплахите, потенциалните уязвимости и риска който те имат за Визовата Информационна Система.

Целта на протокола за оценка на риска е да гарантира, че всички значими за Визовата Информационна Система рискове са разгледани и адресирани по рационален начин, водещ до намаляване на влиянието на заплахите или тяхното влияние върху бизнеса, както и за постепенно подобряване на достъпността на услугите.

Приложимост

Протоколът се прилага при управлението на риска, а така също и при управлението на информационните активи и ресурси, при контрола и защитата на корпоративната мрежа, при управлението и контрола на задаваните привилегии.

Процедура

За целите на оценката на риска, активите може да бъдат групирани.

В следствие на утвърдената стратегия за управление на риска се извърши анализ на риска на следните групи активи:

Активи
Сървърни Помещения
Сървърна Инфраструктура
Мрежово оборудване
Договори
Персонал

Идентифицирани и анализиране потенциални заплахи

За всеки един актив, система или услуга се идентифицират заплахи и уязвимости от следните типове:

Заплахи
Форс мажорни събития
Организационни проблеми
Човешки грешки
Технически грешки
Преднамерени, злонамерени деяния

Определените нива на заплахите и уязвимост са в съответствие с текущото, действително състояние на системите.

Оценка на риска

Приложената методология за оценка е в съответствие с процедурата за оценка на риска и приетото базово на приемане на риска описани в точка 2 от настоящата процедура.

При оценката на рисковете са идентифицирани влиянията, които биха имали рисковете, ако те се случат по време на изпълнение на проекта. Вероятността ще бъде идентифицирана и периодично одитирана по време на изпълнение на проекта. Риска = Вероятност x Влияние

Актив	Заплаха	Вероятност	Влияние	Риск
Персонал	Липса или неадекватно документиране		4	
Сървърна инфраструктура	Липса и/или неадекватна поддръжка		5	
Персонал	Неправилно администриране на ИТ системите		5	
Персонал	Грешки в конфигурацията и експлоатацията		5	

Оценка на ефективността на вече приложени мерки в плана за третиране на риска

Актив	Заплаха	Уязвимост	Планиран остатъчен риск	Отчетен остатъчен риск	Ефективен (Да/Не)
Няма данни от предишен план	Няма данни от предишен план	Няма данни от предишен план	Няма данни от предишен план	Няма данни от предишен план	Няма данни от предишен план

3. МЕРКИ ЗА НАМАЛЯНЕ ВЛИЯНИЕТО НА РИСКОВЕТЕ

Критично ниво на риска

Актив	Заплаха	Вероятност	Влияние	Риск
Персонал	Липса или неадекватно документиране		4	

Анализ:

В следствие на липсата на процедури за управление на IT Service Management процесите може да доведе до проблеми в експлоатацията с ИТ услугите и тяхната стабилност.

Подобрение и причина за избор на мерките:

Създаване на писани правила и най-вече запознаването на персонала с тях ще увеличи познаването на ИТ системите с които ежедневно ще помогне за правилното използване на ИТ системите.

Повишаване на осведомеността на персонала за ИТ системите и техните функции.

Използването на специализирано звено Хелпдеск, може да доведе до събиране на информация за най-типични липси на знания или насоки за такива.

Мерки за минимизирани и отстраняване на рисковете

Мерки за минимизиране на рисковете	Отговорник	Изпълнителя на промяната	Срок за прилагане на мерките	Планиран Остатъчен Риск	Приоритет
Въвеждане на процедури за управление на процесите				4	Среден

. Високо ниво на риска

Актив	Заплаха	Вероятност	Влияние	Риск
Сървърна инфраструктура	Липса и/или неадекватна поддръжка		5	
Персонал	Неправилно администриране на ИТ системите		5	

Персонал	Грешки в конфигурацията и експлоатацията		5	

Анализ:

В следствие на проектния принцип за постигане на договори за поддръжка може да се стигне до ситуация на липса на поддръжка на сървърната и мрежовата инфраструктура. Липсата на формализирани процеси за управление на промените и тестови среди за всички конфигурации може да доведе до грешки в конфигурации и неработоспособност на ИТ услугите.

Подобрение и причина за избор на мерките:

Създаване на писани правила и най-вече запознаването на персонала с тях ще увеличи познаването на ИТ системите с които ежедневно ще помогне за правилното използване на ИТ системите.

Повишаване на осведомеността на персонала за ИТ системите и техните функции.

Използването на специализирано звено Хелпдеск, може да доведе до събиране на информация за най-типични липси на знания или насоки за такива.

Мерки за минимизирани и отстраняване на рисковете

Мерки за минимизиране на рисковете	**Отговорник**	**Изпълнителя на промяната**	**Срок за прилагане на мерките**	**Планиран Остатъчен Риск**	**Приоритет**
Повишена проактивност при процедурите за поддръжка (увеличаване на сроковете за подготовка)				5	Среден
Въвеждане на процедури за управлвение на процесите				5	Среден

Списък на рисковете при изпълнение на проект

В таблицата по-долу са дадени списък на примерните рискове при изпълнение на проект по категории

Категория риск	**Риск - описание**
Поддръжка от ръководството	Ръководството не успява да укаже нужната подкрепа на проекта
Поддръжка от ръководството	Ръководството не е ангажирано с проекта
Поддръжка от ръководството	Конфликт между ключови стекхолдери в проекта

Категория риск	**Риск - описание**
Поддръжка от ръководството	Ключов ръководител напуска проекта
Обхват	Обхвата е лошо дефиниран
Обхват	Промяна на обхвата в движение (по време на изпълнение)
Обхват	Обещания на проектните мениджъри от името на екипа
Обхват	Оценката на работата не е направена коректно
Обхват	Зависимости между различните задачи не са коректно определени
Обхват	Дейности, липсващи в обхвата
Управление на промяната	Голямо количество промени в кратки срокове
Управление на промяната	Несъгласие на основните участници относно промените
Управление на промяната	Липса на умения за упраление на промените
Управление на промяната	Липса на мениджмънт за упралвение на промените
Управление на промяната	Неправилна приоритизация на промените
Управление на промяната	Ниско качество на извършените промени
Участници в проекта	Участниците в проекта не са ангажирани с неговто изпълнение
Участници в проекта	Основни участници напускат
Участници в проекта	Участниците не успяват да подкрепят проекта
Участници в проекта	Конфликт на участниците
Комуникация	Екипа грешно разбира изискванията
Комуникация	Голямо количество информация се комуникира за кратко време
Комуникация	Липса на комуникация
Комуникация	Потребителите имат грешни очаквания
Комуникация	Потребителите не са информирани
Екип	Недостиг на хора в екипа
Екип	Недостатъчна квалификация на ключовите експерти
Екип	Екипа е претоварен с други задачи
Екип	Слаба мотивация на екипа
Дизайн	Дизайна е неприложим
Дизайн	Дизайна не е гъвкав
Технически	Техническите компоненти не са скалируеми
Технически	Нестабилни технически компоненти
Технически	Недостатъчна интеграция
Решения и действия при проблеми	Забавени решения
Решения и действия при проблеми	Решенията са неясни
Решения и действия при проблеми	Решенията са непълни

Категория риск	**Риск - описание**
Организационни	Разминаване в организационната култура
Организационни	Смяна на спонсор на проекта
Управление на проекта	Липса на контрол
Управление на проекта	Липса на организационни умения

ПРИЛОЖЕНИЕ 1 – АНАЛИЗ НА РИСКОВЕТЕ

В това приложение са посочени някои от най-често срещаните рискове при управление на ИТ услугите. Периодичната оценка на вероятността ще даде възможност за се определи нивото на риск във всеки един момент за определените заплахи. Следвайки методиката за оценка на рисковете ще могат да се определят рисковете, както и мерките за управление на рисковете.

Актив	Заплаха	Вероятност	Влияние	Риск
	Форс Мажорни ситуации			
Персонал	Загуба на персонал		5	
Сървърна Инфраструктура	Отпадане на ИТ система		5	
Сървърни Помещения	Мълнии		5	
Сървърни Помещения	Пожар		5	
Сървърни Помещения	Наводняване		5	
Сървърни Помещения	Горящи Кабели		5	
Сървърни Помещения	Недопустими температури и влажност		4	
Сървърни Помещения	Прах, твърди частици		4	
Сървърна Инфраструктура	Загуба на данни при наличие на силни магнитни полета		4	
Мрежово оборудване	Отпадане/сриване на глобална мрежа		4	
Сървърни Помещения	Последици от природни катаклизми		5	
Сървърни Помещения	Мащабни публични прояви		3	
Сървърни Помещения	Бури		4	
Сървърни Помещения	Загуба на информация поради силна светлина		3	
Сървърни Помещения	Поражение в резултат от промелнива приложна среда		4	
	Заплахи свързани с организационни слабости			
Персонал	Липса на, или недостатъчни, правила		4	
Персонал	Недостатъчно познаване на правилата и процедурите		4	
Персонал	Липса на адекватни, или неподходящи, ресурси		3	
Персонал	Недостатъчно наблюдение върху мерките по ИТ сигурност		4	
Сървърна Инфраструктура	Липса на, или неподходяща, поддръжка		5	

Актив	Заплаха	Вероятност	Влияние	Риск
Сървърни Помещения	Неоторизиран достъп до помещения, изискващи защита		5	
Сървърна Инфраструктура	Неоторизирано ползване на права		4	
Сървърна Инфраструктура	Неконтролирано ползване на ресурси		3	
Сървърна Инфраструктура	Лоша нагласа към промените при работата на ИТ		4	
Сървърни Помещения	Информационните носители не са налични, когато е необходимо		3	
Персонал	Понижаване на ИТ работоспособността вследствие на вредни работни условия		3	
Персонал	Неконтролирана промяна на ползвателите на преносими компютри		2	
Сървърни Помещения	Неадекватно маркиране на информационни носители		2	
Сървърни Помещения	Неправилно доставяне на информационни носители		2	
Мрежово оборудване	Некоректно управление на ключоветее за криптиране		2	
Сървърна Инфраструктура	Неподходящо или некоретно предоставяне на консумативи		3	
Сървърна Инфраструктура	Загуба на поверителността на чувствителни данни в защитавана мрежа		4	
Сървърна Инфраструктура	Липса на, или неподходящи, тестови и внедрителни процедури		4	
Персонал	Липса на, или неадекватно документиране		4	
Персонал	Нарушаване на авторските права		2	
Персонал	Тестване на софтуер с продукционни данни		2	
Сървърна Инфраструктура	Неадекватна защита на Windows системите		4	
Мрежово оборудване	Недостатъчна честотна лента на канала		3	
Персонал	Неподходящо ограничаване на потребителската среда		3	
Мрежово оборудване	Неконтролирано използване на комуникационни канали		3	
Сървърна Инфраструктура	Липса на или неподходящо прилагане на защитните механизми за БД		4	
Сървърна Инфраструктура	Сложност на Системата за Управление на База Данни		2	
Сървърна Инфраструктура	Сложност на достъпа до базите данни		2	
Персонал	Лоша организация на потребителската работа с базите данни		3	
Мрежово оборудване	Неподходящи активни и пасивни мрежови компоненти		4	

Актив	Заплаха	Вероятност	Влияние	Риск
Мрежово оборудване	Концептуални недостатъци на мрежата		4	
Мрежово оборудване	Достигане на максимално-позволените кабелни дължини или размери на ринговете		3	
Сървърна Инфраструктура	Несигурен обмен на файлове или медиа-носители		3	
Персонал	Прекомерно разполагане с информационни носители и документи на домашното работно място		3	
Персонал	Липса на или недостадъчно обучение на работещите с отдалечен достъп		4	
Персонал	Закъснения причинени от временно ограничена работоспособност на работещите чрез отдалечен достъп		3	
Персонал	Слаба интеграция на дистанционно работещите с общия информационен поток		2	
Договири	По-дълги времена за реакция в случай на пропадане на ИТ система		3	
Персонал	Загуба на конфиденциалност чрез скрити данни		3	
Персонал	Неконтролирана употреба на електронната поща		4	
Сървърна Инфраструктура	Некоректно описание на файловете		2	
Персонал	Неподходящо съхранение на информационни носители в спешни случаи		3	
Персонал	Работа с нерегистрирани компоненти		3	
Мрежово оборудване	Не е създадена стратегия за мрежовата и управленската системи или не е достатъчна		3	
Персонал	Неоторизирано събиране на лични данни		2	
Персонал	Неподходящо отработване на инциденти свързани с информационната сигурност		4	
Персонал	Липса на или неадекватен ИТ мениджмънт по информационната сигурност		3	
Персонал	Неподходящо администриране на правата за достъп		4	
Сървърна Инфраструктура	Липса на или неподходящо планиране на Активната директория		4	
Персонал	Некоректно преместване на архивните системи		3	
Сървърна Инфраструктура	Недостатъчен капацитет на информационните носители за съхраняване на архивите		3	
Персонал	Некоректно документиране на достъпите до архивите		3	

Актив	Заплаха	Вероятност	Влияние	Риск
Персонал	Лошо планиране на разположението на архивната система		3	
Договири	Погрешна аутсорсинг стратегия		4	
Договири	Незадоволителни споразумения с външни доставчици на услуги		4	
Договири	Неадекватни разпоредби за прекратяване на аутсорсинг проекти		3	
Договири	Зависимост от изнесен доставчик на услуги		3	
Мрежово оборудване	Несигурни протоколи в публичните мрежи		4	
Договири	Негативно влияние на проект за аутсорсинг върху организационния климат		2	
Договири	Неадекватна ИТ сигурност по време на внедрителска фаза на аутсорсинг		2	
Договири	Слабости в отношенията с външен доставчик на услуги		4	
Договири	Неадекватна концепция за планиране на непредвидимости при аутсорсинга		4	
Сървърна Инфраструктура	Неподходяща концепция за свързване на e-mail системи към Exchange/Outlook		3	
Сървърна Инфраструктура	Остаряла или некоректна информация в website-а		2	
Мрежово оборудване	Некоректно планиране и дизайн на приложението на рутерите и суичовете		3	
Сървърна Инфраструктура	Грешки при кандидатстването за и управлението на Internet domain имената		3	
Мрежово оборудване	Неадекватно планиране на непредвидимостите за secutiry gateway		2	
	Заплахи свързани с човешките грешки			
Персонал	Загуба на поверителността/целостта на данни в резултат от грешка на ИТ потребител		2	
Персонал	Увреждане на оборудване или данни по невнимание		2	
Персонал	Несъответствие с ИТ мерките за сигурност		3	
Персонал	Недопустимо/некоректно свързване на кабели		3	
Персонал	Повреда на кабели от небрежни действия		4	
Персонал	Повреди причинени от хигиенисти или външен персонал		4	
Персонал	Отпадане на офисната телефонна централа вследствие на оперативни грешки		2	

Актив	Заплаха	Вероятност	Влияние	Риск
Персонал	Неправилно ползване на ИТ система		4	
Персонал	Неправилно администриране на ИТ система		5	
Персонал	Пренос на неточни или нежелани записи от данни		4	
Персонал	Неправилно разбиране на правната стойност на факс		2	
Персонал	Неправилна администрация на права за достъп до сайт или данни		4	
Персонал	Некоректна промяна на потребителите на компютри		2	
Персонал	Споделяне на директории, принтери или clipboard		2	
Персонал	Неправилно администриране на системите за управление на бази данни		4	
Персонал	Небрежно манипулиране с данни		4	
Персонал	Изтриване на обекти по невнимание		4	
Персонал	Неадекватна конфигурация на активни мрежови компоненти		4	
Персонал	Липса на или неподходяща сегментация		4	
Персонал	Неоторизирано частно ползване на телекомуникационни работни станции		4	
Персонал	Незащитена организация на данните		4	
Персонал	Нарушаване на базови правни условия за ползване на криптографски процедури		3	
Персонал	Неправилна употреба на крипто-модули		2	
Персонал	Неподходяща конфигурация на системата за мениджмънт		4	
Персонал	Изключване на сървър докато е в работно състояние		4	
Персонал	Погрешно разбиране на събития		3	
Персонал	Грешки в конфигурацията и експлоатацията		5	
Персонал	Неправилна употреба на автентикационни услуги с отдалечен достъп		2	
Персонал	Неправилна употреба на услугите по отдалечено достъпване		2	
Персонал	Незащитена конфигурация на RAS клиенти		1	
Персонал	Неподходящо управление на паролите		2	
Персонал	Небрежност при боравенето с информация		3	
Персонал	Неадекватна проверка на идентичността на комуникационните партньори		2	

Актив	Заплаха	Вероятност	Влияние	Риск
Персонал	Неправилна конфигурация на Windows сървъри		4	
Персонал	Неправилна конфигурация на Активната директория		3	
Персонал	Ползване на неподходящи информационни носители за архивиране		2	
Персонал	Неспазване на правните изисквания по отношение на употребата на архивиращи системи		2	
Персонал	Неправилна интеграция на IIS в системната среда		2	
Персонал	Неправилна конфигурация на операционната система за IIS		2	
Персонал	Неправилна конфигурация на IIS		2	
Персонал	Недостатъчно познание в областта на сигурността и тестовите инструменти за IIS		2	
Персонал	Неправилна конфигурация на Exchange сървъри		4	
Персонал	Неправилна конфигурация на рутери и суичове		4	
Персонал	Неправилно администриране на рутери и суичове		4	
	Заплахи свързани с технически повреди			
Сървърни Помещения	Прекъсване на токозахранването		4	
Сървърни Помещения	Отпадане на вътрешните захранващи мрежи		3	
Сървърни Помещения	Отпадане на съществуващите предпазни устройства		4	
Сървърни Помещения	Повреда в линиите, поради неблагоприятни външни условия		4	
Сървърни Помещения	Промени в подаваното напрежение/пренапрежение/недостиг на напрежение		4	
Сървърни Помещения	Дефектни информационни носители		4	
Сървърна Инфраструктура	Откриване на софтуерни уязвимости		3	
Сървърни Помещения	Прекъсване на локалното токозахранване		4	
Мрежово оборудване	Усложнен достъп до ИТ системите в мрежа		3	
Сървърна Инфраструктура	Загуба на съхранявани данни		3	
Мрежово оборудване	Разреждане или изтощаване на резервните захранвания на комуникационни машини		2	
Сървърна Инфраструктура	Загуба на информация, дължаща се на износена сторидж-среда		4	

Актив	Заплаха	Вероятност	Влияние	Риск
Сървърна Инфраструктура	Загуба на данни, дължаща се на износени информационни носители (дискове, ленти)		4	
Сървърна Инфраструктура	Софтуерни уязвимости или грешки		4	
Сървърна Инфраструктура	Отпадане на база данни		4	
Сървърна Инфраструктура	"Заобикаляне" на системата за контрол на достъпа чрез директен достъп до данните		4	
Сървърна Инфраструктура	Загуба на данни поради отпадане на системата за поддръжка на база данни		5	
Сървърна Инфраструктура	Загуба на данни в БД поради липса на място в базата и на дисковите масиви		4	
Сървърна Инфраструктура	Загуба на интегритета/съдържателността на БД		4	
Мрежово оборудване	Отпадане или некоректна работа на мрежови компонент		2	
Сървърна Инфраструктура	Неуспех при разпращане на съобщение		2	
Сървърна Инфраструктура	Липсваща процедура по автентикация или процедура с недостатъчно качество		2	
Мрежово оборудване	Отпадане на крипто-модул		2	
Мрежово оборудване	Несигурни криптографски алгоритми		3	
Мрежово оборудване	Грешки в криптираните данни		2	
Сървърна Инфраструктура	Липса на времева автентикация в е-мейл		2	
Мрежово оборудване	Опадане на компоненти от системата за управление на мрежата или системата за управление на системите		3	
Сървърна Инфраструктура	Концептуални грешки на софтуера		3	
Сървърна Инфраструктура	Недокументирани функции		3	
Мрежово оборудване	Излизане от употреба на крипто-методи		2	
Договири	Отпадане на системите на доставчик на аутсорсинг услуги		2	
Мрежово оборудване	Несигурни фабрични настройки на рутери и суичове		2	
	Заплахи свързани с преднамерени действия			
Персонал	Манипулации или разрушаване на ИТ оборудване или аксесоари		4	
Персонал	Манипулации с данни или софтуер		4	

Актив	Заплаха	Вероятност	Влияние	Риск
Персонал	Неоторизирано влизане в сграда		4	
Персонал	Кражба		2	
Персонал	Вандалски прояви		4	
Персонал	Нападение		4	
Персонал	Неоторизирано ползване на ИТ системи		3	
Персонал	Злоупотреба с портове за дистанционна поддръжка/отдалечено администриране		3	
Персонал	„Любопитни“ служители		3	
Персонал	Заплаха, предизвикана от вътрешен персонал по време на административна работа или поддръжки		4	
Договири	Заплаха, предизвикана от външни служители по време на профилактични работи по поддръжка		4	
Персонал	Заплаха предизвикана от вътрешен персонал по време на административна работа или поддръжки		4	
Персонал	Злоупотреба с потребителски права		3	
Персонал	Злоупотреба с администраторски права		4	
Сървърна Инфраструктура	Троянски коне		3	
Персонал	Кражба на мобилна ИТ система		2	
Сървърна Инфраструктура	Компютърни вируси		2	
Персонал	Отказване от изпратено съобщение		2	
Сървърна Инфраструктура	Срив на услуга		5	
Персонал	Неоторизирано копиране на информационни носители		3	
Персонал	Следене на помещения посредством компютри, оборудвани с микрофони		3	
Персонал	Злоупотреба с ICMP протокол		3	
Персонал	Злоупотреба с протоколите за рутиране		4	
Персонал	Злоупотреба с администраторски права в Windows NT системи		3	
Персонал	Заобикаляне на процедурата по login		3	
Персонал	Временно свободно-достъпни акаунти		3	
Персонал	Инструменти за анализ на мрежата		3	
Персонал	Злоупотреба с дистанционния достъп до мениджмънт функциите върху рутери		4	
Персонал	Злоупотреба с ресурси чрез отдалечени ИТ системи		4	
Персонал	Неоторизирано свързване на ИТ система към мрежа		3	

Актив	Заплаха	Вероятност	Влияние	Риск
Персонал	Неоторизирано изпълнение на управление на мрежата		3	
Персонал	Неоторизиран достъп до активни мрежови компоненти		3	
Персонал	По-висок риск за кражба от домашно работно място		2	
Персонал	Вмешателство на членове на семейството или външни посетители		3	
Персонал	Загуба на конфиденциалност на класифицирана информация		3	
Персонал	Злоупотреба с е-мейл услугите		4	
Персонал	Заблуда относно изпращача		2	
Персонал	Неразрешено получаване на администраторски права под Windows NT		3	
Персонал	Измами/погаждане на номера		3	
Персонал	Неразрешено ползване на крипто-модул		2	
Персонал	Загуба на интегритет на информация, която би трябвало да е защитена		3	
Персонал	Манипулации с параметри за управление		3	
Персонал	Web измами		2	
Персонал	Злоупотреба с активни съдържания		2	
Персонал	Измами с мрежови връзки		2	
Персонал	Манипулации с адресни книги и списъци		3	
Персонал	Злоупотреба с карти за достъп		4	
Персонал	Неразрешен пренос на данни през мобилни телефони		2	
Персонал	Шпионаж		4	
Персонал	Подривна дейност с услугите на архивна система		4	
Персонал	Неразрешено презаписване или изтриване на архивен носител		4	
Персонал	Разпространяване на данни на трети страни от доставкик на външни услуги		4	
Персонал	Манипулации с ARP таблици		3	
Персонал	Измами с MAC адреси		3	
Персонал	Злоупотреба със spanning tree протокол		3	
Персонал	Припокриване на границите между VLAN-и		3	

ФОНД „ВЪТРЕШНА СИГУРНОСТ“

На база на опита си в реализацията на комплексни ИТ проекти, представяме следните предварително идентифицирани рискове по проекта, заедно с мерките за предотвратяването им

№	Категория	Описание на риска	Въздействие / Приоритет / Сфера на влияние / Вероятност	Индикатор	Мерки за недопускане на риска	Мерки за предотвратяване на негативното влияние
1.	Управленски рискове	Недобра комуникация между екипите на възложителя и изпълнителя по време на аналитичните дейности на проекта, в резултат на което може да се получи неразбиране на действителните нужди на възложителя и непостигане на целите на поръчката	Високо 5 Голяма Средна	Нарушаване на нормалния ритъм на работа, затруднения в изпълнението на ежедневните задачи	Провеждане на необходимия брой работни срещи за пълно детайлизиране на изискванията и нуждите, както и провеждане на редовни срещи по управлението на проекта	Допълнителни срещи относно прогреса на засегнатите дейности и идентифициране на конфликтните точки или липсващата информация в възможно най-ранна фаза. Допълнителни активности по координация и/или техническа консултация от страна на изпълнителя.
2.	Управленски рискове	Недостатъчна ангажираност на персонала по време на формулиране на детайлните изисквания към проекта в резултат на което могат да се получат непълноти и/или забавяне	Високо 2 Голяма Ниска	Липса на капацитет и ангажираност по време на детайлното описание	Активна комуникация във фазите по планиране	Потвърждаване на ангажиментите от страна на възложителя. Добро планиране.
3.	Управленски рискове	Възникване на проблеми при изпълнение на поръчката заради трета страна в процеса на доставките	Забавяне на целия проект 6 Високо Ниска (21 - 40%)	Разминаване между поети ангажименти и реални срокове на доставка	Навременно подаване на поръчки за доставка	Осигуряване на детайлни спецификации

[redacted]

№	Категория	Описание на риска	Въздействие / Приоритет / Сфера на влияние / Вероятност	Индикатор	Мерки за недопускане на риска	Мерки за предотвратяване на негативното влияние
4.	Управленски рискове	Недостиг на компетентност и умения в рамките на проектния екип	Забавяне на целия проект 4 Значителна Минимална (1 - 20%)	Неизпълнени срокове и липсващи одобрения на ключови дейности	Добро планиране и осигуряване на екип с необходимия капацитет	Добро планиране
5.	Управленски рискове	Смяна на ключов за проекта персонал на възложителя	Забавяне на целия проект 4 Малка Ниска (21 - 40%)	Смяна на ключов за проекта персонал на възложителя	Няма	Няма стратегия
6.	Управленски рискове	Недооценени големина и сложност на проекта	Забавяне на целия проект 6 Умерена Ниска (21 - 40%)	Неизпълнени срокове и липсващи одобрения на ключови дейности	Извършване на цялостен анализ по проекта	Добро планиране
7.	Управленски рискове	Необходимата информация за анализ не се предоставя навреме от Възложителя на Изпълнителя	Забавяне на дейности в проекта 2 Малка Минимална (1 - 20%)	Неизпълнени срокове и липсващи одобрения на съответстващи дейности	Активна комуникация във аналитичните дейности	Потвърждаване на ангажиментите от страна на възложителя. Добро планиране.
8.	Управленски рискове	Екипът на възложителя по координация и управление на проекта да няма достатъчно ресурсен капацитет	Забавяне на целия проект 8 Високо Висока (61 - 80%)	Закъснения в проектния график, пропуснати срокове за	Ясно и точно комуникирани отговорности на екипа на възложителя в първоначалната фаза	Допълнителни седмични срещи относно прогреса на засегнатите дейности и идентифициране на конфликтните точки или

№	Категория	Описание на риска	Въздействие / Приоритет / Сфера на влияние / Вероятност	Индикатор	Мерки за недопускане на риска	Мерки за предотвратяване на негативното влияние
				дейности зависещи от екипа на възложителя и закъснения в приемателните процедури	на проекта.	липсващата информация в ранна фаза. Допълнителни активности по координация и/или техническа консултация от страна на изпълнителя.
9.	Управленски рискове	Проблем с ресурсите за проверка на предавани материали / бавно взимане на решения по изискванията	Забавяне на целия проект 3 Съществена Висока (61 - 80%)	Забавяне приемането на резултатите по проекта	Съобразяване при задаване на оперативните задачи със задачите по проекта за всички ресурси въвлечени в него.	Осигуряване на допълнителен ресурс.
10.	Технически	Повреда в поддържаното оборудване	Прекъсване на работата на засегнатото устройство и спиране на зависими услуги 4 Средна (21-50%)	Загуба на свързаност или достъп до системи	Смекчаване	Осигуряване на възможност за временна замяна на повреденото сървърно или комуникационно оборудване. Създаване на процедури за действие при бедствия и аварии, както и за архивиране и възстановяване на системи и данни
11.	Организационни/	Прекратяване на	Повишаване риска	Достигната	Смекчаване	Осигуряване на оборотно

№	Категория	Описание на риска	Въздействие / Приоритет / Сфера на влияние / Вероятност	Индикатор	Мерки за недопускане на риска	Мерки за предотвратяване на негативното влияние
	Технически	поддръжката устройствата от производителите в рамките на договора	от прекъсване работата на системи в случай на повреди в оборудването 6 Висока (51-80%)	крайна дата на поддръжка на оборудването от производителя		сервизно оборудване на склад. Използване на споделени депа за резервни части.
12.	Технически/ Сигурност	Неоторизирана или неумишлена зловредна намеса в настройки и конфигурации оборудването	Загуба или кражба на данни, отпадане на системи и услуги 5 Средна (21-50%)	Загуба на свързаност или достъп до системи	Смекчаване	Предоставяне на права за достъп до поддържаните системи само за оторизирани лица. Непрекъснато проследяване и контрол на дейностите по поддръжката. Предлагане на контролни мерки за повишаване сигурността и защитата на системите
13.	Форс-мажорни	Наводняване или пожар в сървърни помещения и поражения върху инсталираното оборудване.	Прекъсване на работата на засегнатото устройство и спиране на зависими услуги 3 Минимална (1 -	Вдигнати аларми за пожар/ наводнение	Прехвърляне/ Избягване	Застраховане на оборудването. Създаване на планове за действие при бедствени ситуации.

[redacted]

Заличени съгласно чл. 2 от ЗЗЛД

№	Категория	Описание на риска	Въздействие / Приоритет / Сфера на влияние / Вероятност	Индикатор	Мерки за недопускане на риска	Мерки за предотвратяване на негативното влияние
			20%)			
14.	Организационни	Липса на необходимите права за изпълнение на дейностите по поддръжка	Невъзможност за изпълнение на дейностите по проекта 4 Минимална (1 - 20%)	Невъзможност за достъп до поддържаното оборудване	Смекчаване	Вземане на управленско решение от страна на Възложителя за създаване на необходимата организация и даване на необходимите права за достъп
15.	Технически/ Инфраструктурни	Липсата на оригинални резервни части и компоненти за поддържаното оборудване, както и забавянето на доставката на същите	Неработоспособ-ност на системи и услуги, зависещи от съответното дефектирало устройство 5 Средна (21-50%)	Загуба на свързаност или достъп до системи	Смекчаване	Осигуряване на оборотно сервизно оборудване на склад. Използване на споделени депа за резервни части.

Дата: 25.05.2016
Представляващ ДЗЗД Ай Би Ес Индекс, съгласно Договор за консорциум от 19.05.2016,
Горан Ангелов, Управител на Водещ съдружник Ай Би Ес – България ЕООД:

(печат на Водещ съдружник, съгласно т. 3.5. от Договор за консорциум от 19.05.2016)

Приложение №6

Подход, методика и начин на изпълнение на дейностите по обслужване на инцидентите и механизма за управление на възникналите проблеми в периода на поддръжката на системите

към

ТЕХНИЧЕСКА ОФЕРТА

за участие в открита процедура за възлагане на обществена поръчка с предмет: "Поддръжка и обновяване на програмното и техническо осигуряване на Националната визова информационна система и на визовата дейност в консулските служби на Р България",

Обособена позиция 1: „Поддръжка и осъвременяване на техническото осигуряване и инфраструктурата на НВИС“

От КОНСОРЦИУМ ДЗЗД „Ай Би Ес Индекс”

СЪДЪРЖАНИЕ

ИЗПОЛЗВАНИ ТЕРМИНИ И СЪКРАЩЕНИЯ

Съкращение / Термин	Значение
PMI	Project Management Institute
Възложител	Министерство на външните работи
Изпълнител	ДЗЗД „Ай Би Ес Индекс”
ИТ	Информационни технологии
ТС	Технически спецификации по обществената поръчка

1. ВЪВЕДЕНИЕ

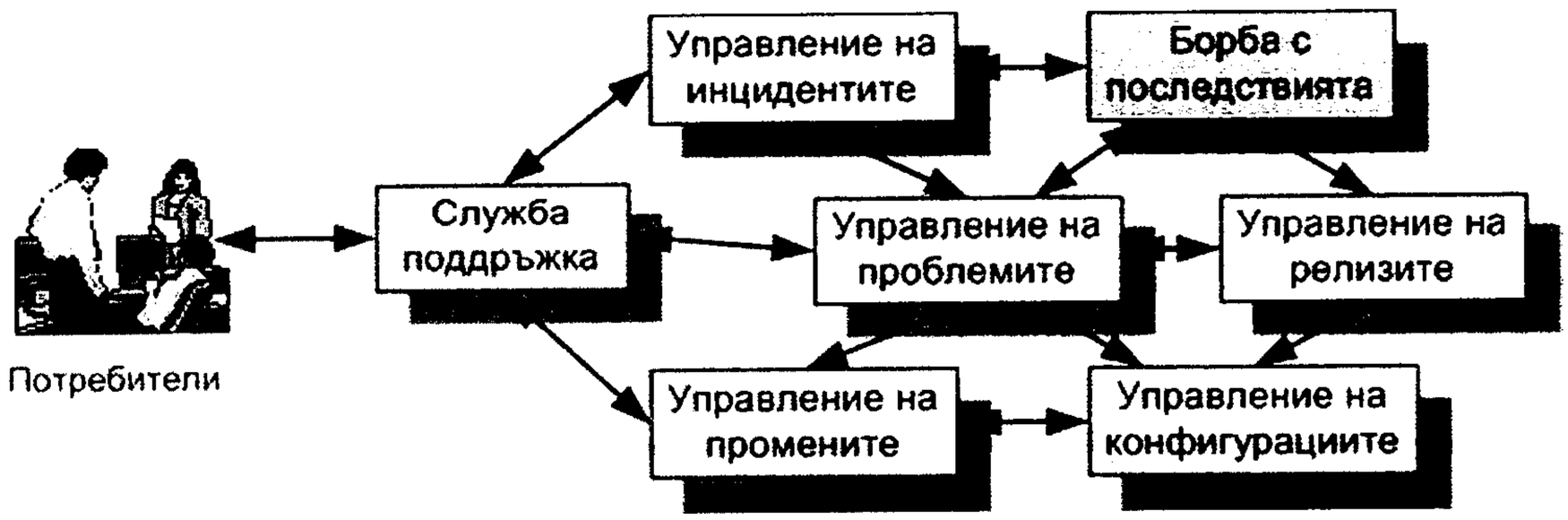
Настоящият документ е разработен възоснова на поставените изисквания в документацията за участие в открита процедура с предмет "Поддръжка и обновяване на програмното и техническо осигуряване на Националната визова информационна система и на визовата дейност в консулските служби на Р България", Обособена позиция 1: „Поддръжка и осъвременяване на техническото осигуряване и инфраструктурата на НВИС".

Целта на този документ е да се опишат подхода, методиката и начина на изпълнение на дейностите по обслужване на инцидентите и механизма за управление на възникналите проблеми в периода на поддръжката на системите.

Системата за Управление на Качеството и Информационната Сигурност се базира на стандартите по ISO 9001:2008, ISO 20000-1:2005, ISO 27001:2005, ISO 14001:2004, OHSAS 18001:2007, което свидетелства, че дейностите по предоставяне на услуги, включително и извършване на поддръжка се изпълняват съгласно най-високите изисквания на международните стандарти за качество и информационна сигурност и управление на услуги.

Всички процеси по гаранционното обслужване ще са съгласно най-добрите практики при обслужването на ИТ системи в съответствие с ITIL книга Поддръжка на услуги (Service Support) част от методологията ITSM версия 2, състояща се от следните части:

- Служба Поддръжка (Service Desk)
- Процес за управление на инцидентите (Incident Management)
- Процес за управление на проблемите (Problem Management)
- Процес за управление на конфигурациите (Configuration Management)
- Процес за управление на промените (Change Management)
- Процес за управление на релизите (Release Management)



2. ОПИСАНИЕ НА ПРОЦЕСИТЕ ОТ ОБЛАСТ SERVICE SUPPORT (ПОДДРЪЖКА НА УСЛУГИ)

2.1. Функция Хелп Деск (Help Desk)

2.1.1. Цели и задачи на функцията

Основната цел на функцията Хелп Деск е да осигурни възстановяване на ИТ услугите с минимално влияние върху бизнес операциите и за да изпълни тази цел функцията изпълнява процеса за управление на инцидентите. Хелп дескът отговаря за жизнения цикъл на инцидентите, както и изпълнява заявки за услуги, промени, информация и т.н.

Основните дейности на функцията Хелп Деск са:

- Приемане на обаждания, първа точка на контакт за потребителите
- Записване и проследяване на инцидентите
- Първоначална поддръжка и класификация
- Мониториране и процедури за ескалиране в зависимост от договорите за доставка
- Пренасочване на инциденти към екипи по поддръжка
- Разрешаване на инциденти от първо ниво на поддръжка
- Информиране на потребителите за статуса на инцидентите
- Затваряне на инциденти след потвърждение от потребителите
- Комуникиране на планирани промени с потребителите
- Предоставяне на статистика и информация за ръководството

2.1.2. Планове и процедури

Функцията основно поддържа процеса за управление на инцидентите (Incident management) и дейностите й са описани в процедурата за изпълнение на този процес.

2.1.3. Роли и отговорности

Виж роли и отговорности в процеса за управление на инцидентите.

2.2. Процес за управление на инцидентите, свързани с ИТ услугите (Incident Management)

2.2.1. Цели и задачи на процеса

Основните цели на процеса са следните:

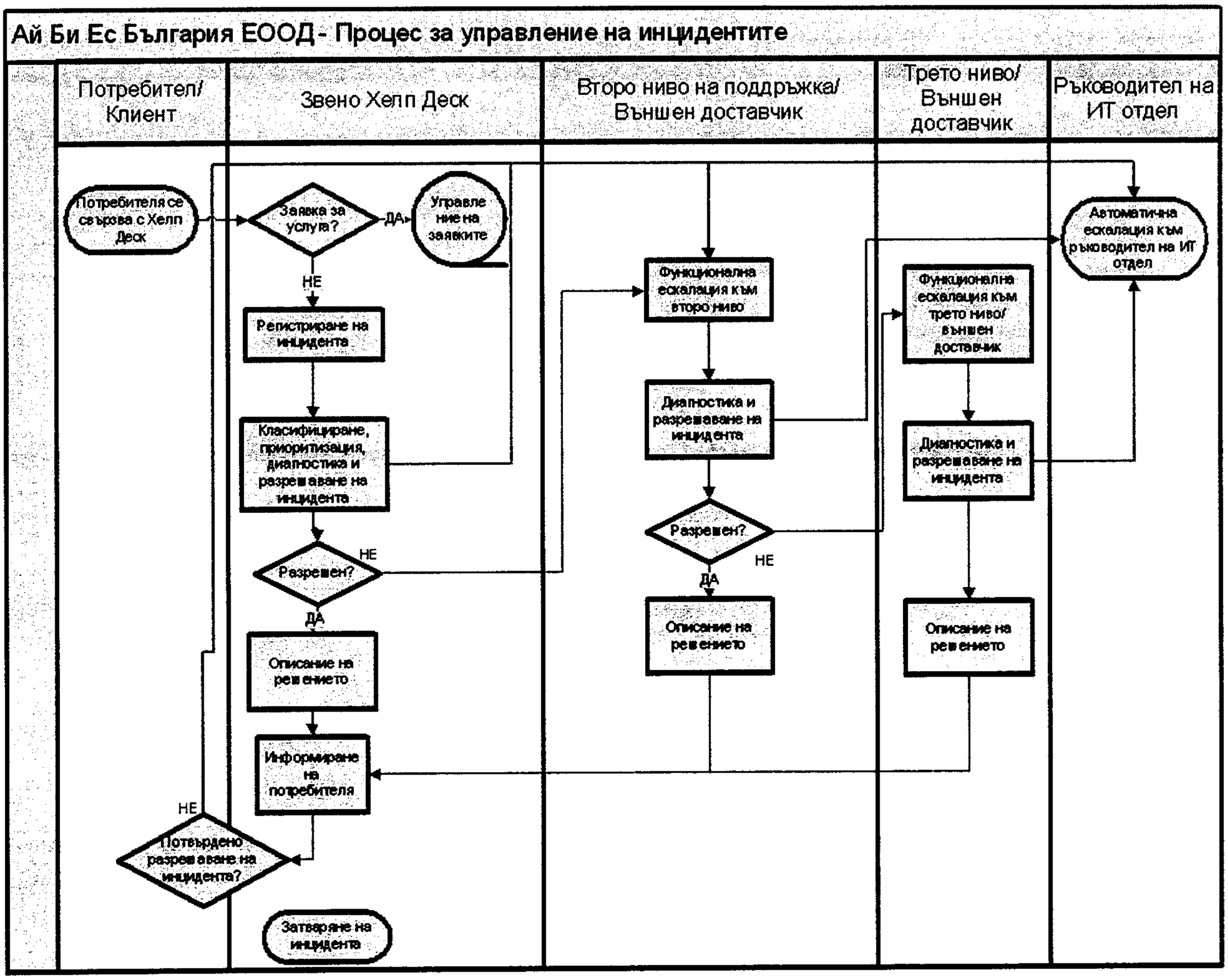
- Детайлно и точно регистриране на всички инциденти
- Максимално бързо разрешаване на инцидентите
- Максимално бързо възстановяване на услугата в зависимост от договорените пареметри на доставка
- Подробно описание на дейностите по разрешаването на инцидента
- Предоставяне на информация на процеса за управление на проблемите (Problem Management) относно взимане на мерки за предотвратяване повторяемостта на инцидентите

Основните дейности по управление на инцидентите са следните:

- Идентификация на инцидентите (Incident identification)
- Регистриране на инцидентите (Incident logging)
- Категоризиране на инцидентите (Incident categorisation)
- Приоритизация на инцидентите (Incident prioritisation)
- Първоначална диагностика (Initial diagnosis)
- Ескалация на инцидентите (Incident escalation) – функционална и йерархична (мениджмънт ескалация)
- Изследване и диагностика (Investigation and diagnosis)
- Разрешаване и възстановяване на услугата (Resolution and recovery)
- Затваряне на инцидента (Incident closure)

2.2.2. Планове и процедури

2.2.2.1. Диаграма на процеса



2.2.2.2. Процедура за изпълнение на процеса

a) Потребителят се свързва с Хелп Деск

Потребителя установява контакт с хелп деск по някой от следните 3 начина:

- По телефон
- Чрез email
- През уеб интерфейс на системата за поддръжка
- На място в офиса на IBS

b) Това заявка за услуга ли е?

Ако потребителя се е свързал със заявка за услуга или оборудване – следва пренасочване по процедурата за обслужване на заявки (Request Management)

Ако заявката е за инцидент, то премини към следващата стъпка – регистриране на инцидента

c) Регистриране на инцидента и събиране на информация

Информацията за инцидента се попълва в системата за поддръжка (SupportLine). Като минимум трябва да имаме попълнени следните полета:

Поле от форма за регистриране на инцидент	**Стойност**
Уникален идентификатор (Ticket number)	Генерира се автоматично от системата, или ръчно при липса на такава.
Дата и час на регистриране	
Статус	Регистриран, активен, изчакване, разрешен, затворен, и т.н.
Категория	Тип на инцидента (и екип за поддръжка)
Потребител	Контактна информация (Име, отдел, телефон, локация, email адрес)
Отговорник/ Оператор	Служител от Хелп Деск, регистрирал инцидента
Приоритет	Колко бързо трябва да бъде намерено решение на инцидента (производен от мащаба и спешността)
Описание	Подробна информация за инцидента
Детайли	Връзка с регистрирани инциденти, прикачени файлове и др.
Дата и час на разрешаване	
Дата и час на затваряне	

d) Класифициране, приоритизация, диагностика и опит за разрешаване на инцидента

В тази стъпка се определя категорията на инцидента, неговия мащаб, спешност и приоритет, както и да се прецени дали Хелп деск звеното може да го разреши.

e) Разрешен ли е инцидента?

Ако инцидента е разрешен то премини към **описание на решението.** Ако не – премини към **функционална ескалация на второ ниво** и уведоми съответния ръководител (мениджмънт ескалация)

f) Функционална ескалация към второ ниво

Препращане на инцидента към най-подходящата група в зависимост от категорията на инцидента.

g) Диагностика и разрешаване на инцидента

В тази стъпка се работи по разрешаването на инцидента от специалисти на второ ниво на поддръжка.

h) Разрешен ли е инцидента?

Ако инцидента е разрешен в рамките на договореностите (Service Level Agreement) то се преминава към **описание на решението.** Ако не (напр. инцидента не е разрешен в рамките на договореното време), се преминава към **функционална ескалация на трето ниво или външен доставчик** и се уведомява съответния ръководител (**мениджмънт ескалация**).

i) Диагностика и разрешаване на инцидента

В тази стъпка се работи по разрешаването на инцидента от специалисти на трето ниво на поддръжка или външни доставчици

j) Разрешен ли е инцидента?

Ако инцидента е разрешен то премини към **описание на решението.** Ако не –уведоми съответния ръководител (**мениджмънт ескалация**)

k) Описание на решението

В определните за целта полета се описва в детайли как е разрешен инцидента.

l) Информиране на потребителя за решението
m) Потребителя потвърждава ли разрешаването на инцидента?

Ако потребителя потвърди, че инцидента е разрешен успешно, се преминава към **затваряне на инцидента.** Ако не, се преминава към **функционална ескалация на второ ниво** и се уведомява съответния ръководител (**мениджмънт ескалация**).

n) Затваряне на инцидента

2.2.3. Роли и отговорности

2.2.3.1. Ръководител на Хелп Деск и управлението на инцидентите

Служителят в тази роля отговаря за

- Управление на всички дейности на екипа Хелп Деск
- Играе роля на контакт за ескалация за Хелп Деск операторите
- Носи като цяло отговорността за обслужването на инцидентите и заявките към екипа Хелп Деск
- Осигурява равномерно разпределение на компетентностите на хората в екипа Хелп Деск ако се работи на смени
- Създава и предоставя статистика и отчети на ръководството

- Грижи се за ефективността и ефикасността на процеса за управление на инцидентите, както и за подобрението му
- Директно контролира работата на екип Хелп Деск
- Координира работата на всички нива на поддръжка

2.2.3.2. Оператор в Хелп Деск

- Отговаря за регистриране на инцидентите
- Препраща заявки за услуги към съответните групи
- Извършва първоначална поддръжка и класифицира инцидентите
- Поема собствеността на инциденти, извършва мониторирането им и проследяване
- Разрешава инциденти на първо ниво на поддръжка
- Прави йерархични (мениджмънт) ескалации

2.2.3.3. Специалист от второ и трето ниво на поддръжка

- Обслужва заявки за услуги
- Мониторира детайлите на инцидента, включително засегнатите ИТ компоненти
- Извършва диагностика и разрешаване на инцидентите
- Проактивно изследва инциденти с цел окриване на проблеми – коренната причина за възникването на инцидентите
- Разрешава инциденти и възстановява ИТ услугите

2.2.3.4. Матрица на ролите и отговорностите (RACI matrix) на процеса за управление на инцидентите (Incident Management)

Дейност		Оператор Хелп Деск	Ръководител Хелп Деск	Специалист по поддръжка	Потребител/Клиент
Управление на инциденти					
Потребителят се свързва с Хелп Деск		I	A		R
Това заявка за услуга ли е?		R	A		C
Регистриране на инцидента и събиране на информация		R	A		
Класифициране, приоритизация, диагностика		R	A		
Инцидентът в компетентност на Хелп Деск ли е?		R	AC		
Разрешаване на инцидента от Хелп Деск		R	A	R	
Функционална ескалация към второ/ трето ниво или външен доставчик		R	A	I	
Разрешаване на проблема от второ/трето ниво		I	A	R	
Потребителят удовлетворен ли е от решението?		R	A		C
Затваряне на инцидента		R	AC		

2.3. Процес за управление на проблемите (Problem Management)

2.3.1. Цели и задачи на процеса

Основната цел на процеса за управление на проблемите (Problem Management) е да минимизира вредното влияние на инцидентите, причинени от грешки в ИТ инфраструктурата, върху бизнес операциите, както и да предотврати повторяемостта на инциденти, свързани с тези грешки. За да постигне тази цел процесът за управление на проблеми се опитва да идентифицира коренната причина за възникване на инцидентите и да инициира активности за подобрение или коригиране на ситуацията.

Основните дейности по управление на проблемиете са следните:

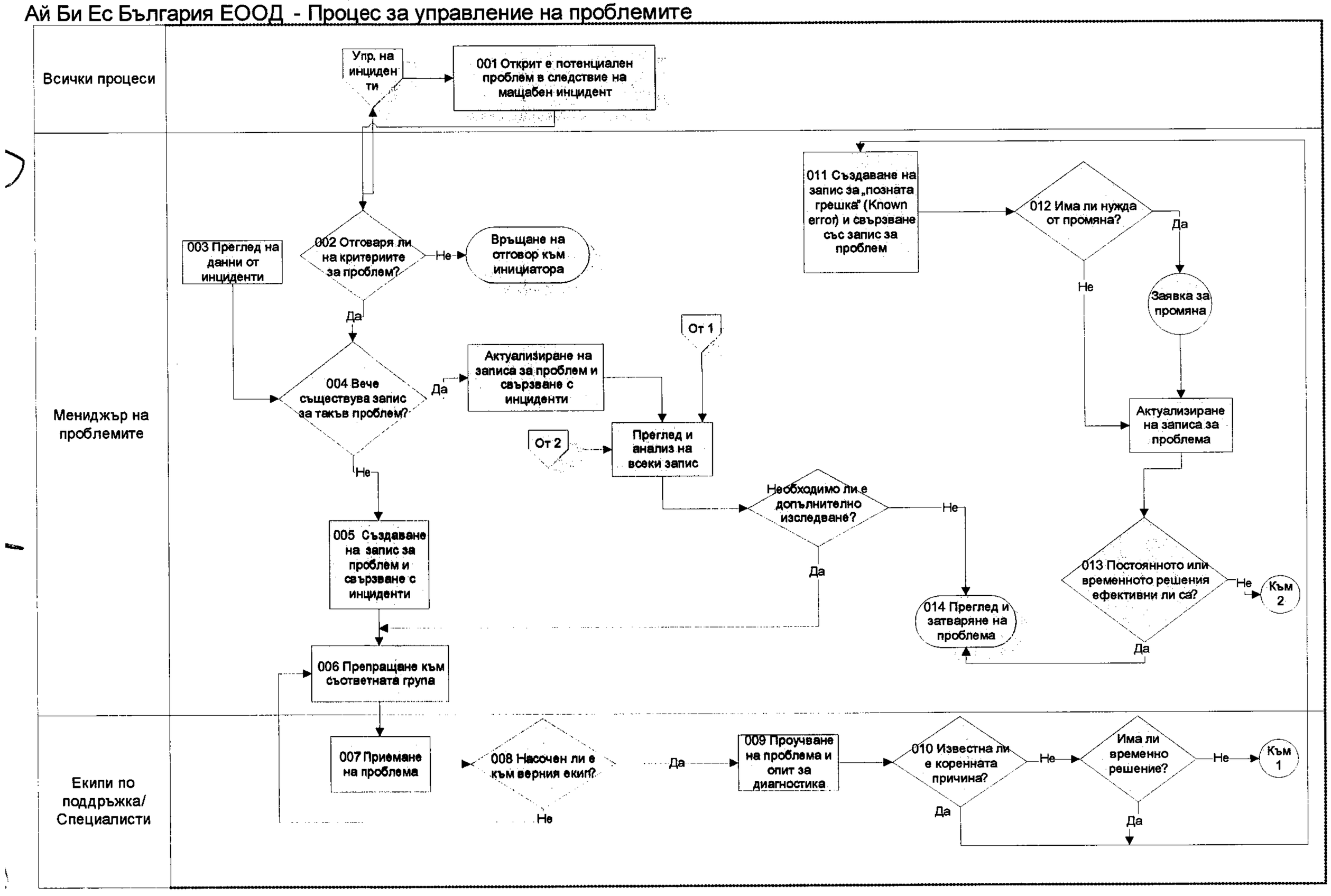
- Откриване на проблеми (Problem Detection)
- Регистриране на проблеми (Problem Logging)
- Категоризиране на проблеми (Problem Categorisation)
- Приоритизане на проблеми (Problem Prioritisation)
- Изследване и диагностика на проблеми (Problem Investigation & Diagnosis)
- Намиране на временни решения (Workarounds)
- Регистриране на грешки, за които има временно решение (Raising a Known Error record)
- Разрешаване на проблеми (Problem Resolution)
- Затваряне на проблеми (Problem Closure)
- Основен преглед на мащабни инциденти и проблеми (Major Problem Review)

2.3.2. Планове и процедури

[redacted]

2.3.2.1. Диаграма на процеса

Ай Би Ес България ЕООД - Процес за управление на проблемите



Открит е потенциален проблем в следствие на мащабен инцидент

Предложение за проблем може да възникне в следствие на мащабен инцидент. След регистриране на проблема мениджъра на проблемите (Problem Manager) преценява дали предложението е подходящо за генериране на запис за проблем (Problem Record)

Съответствие с критериите за проблем

Ако предложението не отговаря на критериите за регистриране на запис за проблем, тогава се връща отговор към инициатора на предложението.

Преглед на данни от инциденти

Мениджърът на проблемите генерира редовно отчет за предоставяне на информация относно тенденции, кандидати за проблеми или „познати грешки” (Known Errors). За целта трябва да се изследват:

- Всички разрешени инциденти, разпределени по услуги
- Всички разрешени инциденти, разпределени по компоненти
- Всички разрешени инциденти с еднакъв код на разрешаване
- Всички разрешени инциденти на база класификация

Мениджърът на проблемите решава на база на предходната информация дали има потенциален кандидат за регистриране на проблем. За да направи верен извод, той трябва да намери отговор на следните въпроси:

- Повторяем ли е инцидента?
- Често ли се случва?
- Много пъти ли се е случвал?
- Конкретна услуга или компонент е засегнат?
- Имало ли е мащабен инцидент?
- Разрешен ли е инцидента?

Наличие на запис за такъв проблем

Проверка дали вече няма регистриран такъв проблем.

Приоритизиране на проблеми - пример

Приоритет	Време за разрешаване
Висок	2 дни
Среден	5 дни
Нисък	20 дни

Препращане към съответната група

Мениджърът на проблемите асоциира проблема с най-подходящия екип по поддръжка.

Приемане на проблема

Член на съответния екип приема проблема и започва работа по него. Ако до никой не приеме проблема се извършва ескалация към ръководителя на екипа.

Проверка дали проблема е насочен към верния екип

Ако се окаже, че проблемът не е насочен към вярната група, той се връща към мениджъра на проблемите. Ако е във верния екип се преминава към проучването и диагностиката му.

Проучване на проблема и опит за диагностика

Проблемът се проучва и се прави опит да се открие коренната причина, използвайки различни методи.

При условие, че е открита коренната причина, следва Създаване на запис за „позната грешка” (Known error) и свързване със запис за проблем.

При условие, че коренната причина е известна, но има само временно решение в момента, следва Създаване на запис за „позната грешка” (Known error) и свързване със запис за проблем. В противен случай проблема се връща към мениджъра на проблеми за допълнително проучване.

Създаване на запис за „позната грешка” (Known error) и свързване със запис за проблем

Извършва се диагностика на познатата грешка и се взима решение дали има възможност за постоянно решение или не.

Необходимост от промяна

Ако се окаже, че има нужда от промяна в услуга или компонент, то се създава заявка за промяна, която се свързва със записа на проблема.

Ефективност на решенията (временни и/или постоянни)

Ако решението е ефективно се преминава към преглед и затваряне на проблема. Ако не, то проблема се връща към мениджъра на проблеми за допълнително проучване.

Преглед и затваряне на проблема

Затваря се записът за позната грешка, след което се затваря записа на проблема.

Роли и отговорности

Мениджър на проблемите

Основните отговорности на мениджъра на проблемите включват:

- Развитие и подобряване на процеса за управление на проблемите;
- Създаване на статистика и отчети за ръководството;
- Управление на персонала за разрешаване на проблеми;
- Разработка на проактивни дейности за управление на проблеми;
- Координиране на персонала при мащабни инциденти и проблеми;

Екипи по поддръжка (Specialist Support)

- Мониторира детайлите на проблема, включително засегнатите ИТ компоненти;
- Извършва диагностика и разрешаване на проблемите;
- Проактивно изследва инциденти с цел окриване на проблеми – коренната причина за възникването на инцидентите;
- Намира временни решения на проблеми;
- Разрешава проблеми и възстановява ИТ услугите;

3. КОНКРЕТНИ ДЕЙНОСТИ

3.1. Осигуряване 24/7 техническа поддръжка

Изпълнителят ще осигури 24/7 техническа поддръжка на системите, обект на настоящата методика, която включва текущи ремонти, замяна на повредено оборудване, ъпгрейд или подобряване на наличните технически средства и техническа поддръжка 8/5 (8 часа в работни дни) на конкретното техническо оборудване и програмно осигуряване.

Изпълнителят ще осигури поддръжка на цялостното техническо оборудване за целия срок на договора, включително в случаите, когато официалната поддръжка на оборудването е спряна от производителя. При подмяна на оборудване с ново от Възложителя техническата поддръжка ще бъде съобразена с гаранционния срок на новодоставеното за срок не по-малък от 3 години или 31.12.2019 (което настъпи по-късно).

В случай на подмяна на инфраструктурни компоненти, Изпълнителят ще осигури миграцията и ще продължи да осигурява софтуерна поддръжка на мигрираните върху новото оборудване съществуващи услуги.

Поддръжката ще включва следните етапи:

3.1.1. Анализ на текущото състояние на компонентите на системата.

Специалистите на Изпълнителя ще анализират внимателно състоянието на всички компоненти, обект на настоящата методика и до 30 календарни дни след сключване на договора и впоследствие веднъж годишно до края на договора ще предоставят доклад с анализ на състоянието на инфраструктурата, съдържащ, но не задължително ограничен до следните компоненти:

- Съответствие на действителното състояние на компонентите с описанието им в наличната документация – характеристики, серийни номера, количества и др.;
- Оценка на техническото им състояние – съществуващи и потенциални проблеми и др;
- Обща оценка за цялостното състояние на системата.

Анализът на мрежовата инфраструктура и комуникациите ще включва, но няма да бъде ограничен до следните дейности:

- Проверка на функционирането на мрежата като цяло:
  - вътрешни комуникации между НВЦ и РВЦ;
  - маршрутни протоколи;
  - криптиране на трафика;
  - комуникация с външни мрежи (МВР, ДАНС, Европейска визова система, МВнР);
  - свързаност на сървърите с мрежовите устройства;
  - резервираност на комуникациите;-
- Преглед на сигурността на мрежата.
  - Достъпа до устройствата да става по сигурни протоколи. Смяна на паролите.

3.1.2. Планиране на дейностите по поддръжка и обновяване на системите

До 7 календарни дни след извършване на анализа от т. 3.1.1 след подписване на договора и след това веднъж годишно до края на договора ще бъде извършвано планиране на дейностите по поддръжка и обновяване на системите за текущата година. То ще бъде приемано с доклад за изпълнение на дейността.

3.1.3. Ремонт на дефектирали хардуерни устройства

Дейността се изпълнява в рамките на 15 работни дни от приемането на доклада за извършен анализ на текущото състояние от точка 4.1.1, а след това спрямо нивото на критичност на устройството/ компонента за срока на договора.

Ремонтът на дефектирали устройства и/ или компоненти ще се извършва спрямо тяхната критичност за функционирането на всички системи. Нивата на критичност се дефинират както следва:

Ниво на критичност	**Време за възстановяване**
Високо (Заплаха за спиране на НВИС или основни инфраструктурни системи)	4 часа
Средно (Заплаха за липса на резервираност)	8 часа
Ниско (Потенциална заплаха за инцидент)	24 часа

Сроковете в таблицата започват да текат от официалното заявяване от Възложителя към Изпълнителя за дефектирало устройство или компонент.

Определянето на нивото на критичност се съгласува писмено между Възложителя и Изпълнителя.

3.1.4. Профилактика на оборудването

В рамките на 30 дни след сключване на договора за възлагане на поръчката към Изпълнителя, а след това веднъж годишно до края на договора ще бъде извършвана профилактика на оборудването.

Профилактиката ще включва:

- Отстраняване на установени неизправности, дефекти и функционални откази, както при оборудването, така и при софтуера, явяващ се неразделна част от оборудването (firmware, операционна система, разширения и др.);
- Отстраняване на прах и други замърсители от повърхността и вътрешността на оборудването;
- Контролирано рестартиране на всеки от мрежовите и сървърни компоненти с цел проверка работоспособността на резервираността на системите, както и установяване на възможностите за автоматично възстановяване след сривове.

Тестване на функционалности на системи

- Тестването на функционалности на системи се заключава в извършването на проверка на коректното функциониране на системите като цяло или на отделни техни компоненти.
- Сравняват се предварително известни и очаквани стойности на различни параметри с реално измерени / проверени стойности.
- В зависимост от характера на тестваната система се допуска проверка на функционалността ѝ чрез подаване на входни данни /или въздействие на вход/, като изходните данни /или резултат на изход/ се сравняват с очакваните данни или резултати при нормално функциониране на системите.
- Получените данни се анализират, като се проверява дали съвпадат с очакваните резултати.
- Ако получените стойности / резултати съвпадат с предварително очакваните или са в рамките на допустимо отклонение, съгласно експертна оценка, съответният тест се приема за успешен.
- Провеждането на тестове за функционалност на системи се документира, като се описват:
    - Тествана система
    - Обхват на теста
    - Параметри
    - Процедури, които ще се изпълнят по време на теста
    - Получени резултати, стойности и т.н.
    - Критерии за приемане
    - Общ резултат от теста
    - Имена и длъжност на провеждащите теста лица
    - Имена и длъжност на проверяващо лице

Преглед на хардуерна част за видими дефекти

- Дейностите по преглед на хардуерна част на система се извършват съгласно плана за профилактика на оборудването.
- Наблюдават се светлинни индикатори на устройствата за индикации за грешки, съгласно спецификациите в документацията на производителя.
- Наблюдават се дисплеи на устройствата (напр. front panel) за изведени съобщения за грешки .
- Проверява се хардуера за нехарактерен шум при работа.
- В случай на открити грешки в работата на хардуера, същите се регистрират в протокола от извършения преглед и се отваря ЗСУ за отстраняване на регистрирания проблем.

Отстраняване на прах и други замърсители

- Преглеждат се повърхността и вътрешността на оборудването за прах и замърсители и същите се отстраняват.
- Специално внимание се обръща на местата около въртящи се части, вентилатори, охладители и други, в околност на които традиционно се отлагат прах и замърсители.
- При отстраняване на прах и други замърсители от вътрешността на оборудването, когато ситуацията го налага, се извършва:
  - Изваждане на охлаждания / вентилатори
  - Почистване на прашните радиатори и вентилатори
  - Почистване на останалия прах в оборудването
  - Монтиране на охладителните модули и вентилатори
- Контролирано рестартиране на всеки от мрежовите компоненти с цел проверка работоспособността на резервираността на системите, както и възможностите за автоматично възстановяване след сривове.

3.1.5. Докладване на инциденти

Всички заявки и съобщения се считат за направени, след като Възложителят ги е изпратил на Изпълнителя на посочени телефон/факс или e-mail адрес. За целта ще бъде осигурена гореща телефонна линия, достъпна 24 часа в денонощието, без почивен ден.

3.1.6. Време за реакция

Времената за реакция са както следва:

No	**Тип на дейността**	**Време за реакция**
1	Дистанционни дейности	До 15 минути след докладване на инцидент
2	При необходимост от "ремонт на място"	До 18:00 часа на следващия работен ден, считано от времето на докладване на инцидент

3.1.7. Време за разрешаване на инцидент

No	Ниво на критичност	Намиране на временно решение (Заобикаляне на проблем)	Пълно разрешаване на инцидента
1	За дублираните компоненти	4 часа	До 18:00 часа на следващия работен ден (ако не е станало автоматично)
2	За критичните компоненти, които блокират цялостната работа на системата или съществена част от нея	8 часа	В рамките на два работни дни

Ако възникнал проблем блокира цялостната работа на системата, но позволява активирането на Резервния център и ако времето за заобикаляне/отстраняване на проблема надвишава 1 час, то се пристъпва към активиране на Резервния център, съгласно подробно разписан при Възложителя план за работа при критични ситуации.

3.2. Структуриране на поддръжката

Предвижда се поддръжката да се осъществява на следните две нива:

3.2.1. Първо (Базово) ниво

Това е нивото на поддръжка от страна на Възложителя. Извършва се първоначално диагностициране на възникналите проблеми от служителите на Възложителя, преди да бъде отправено официално искане за извършване на сервизно обслужване. Това включва: събиране на нужната информация, базово диагностициране на проблема, както и дейности за неговото отстраняване при възможност.

3.2.2. Второ (Разширено) ниво

Позволява решаване на проблема, в зависимост от неговата специфика и сложност, като се извършва от Изпълнителя, съгласно неговата вътрешна организация и вътрешни процедури на работа и се съгласува с Възложителя.

3.3. Ред за извършване на следгаранционното обслужване

Заявката за отстраняване на възникнал проблем с оборудването се подава от упълномощен представител на Възложителя на посочен от Изпълнителя телефон, електронен адрес или факс. Отбелязва се датата и часа на подаване на заявката. Заявката трябва да съдържа информация за: проблема; часа и датата, когато е констатиран проблема; вероятния характер на повредата.

Изпълнителят изготвя тримесечни доклади за изпълнение с пълен запис на всички заявки и извършени дейности.

Тримесечните доклади ще се изготвят до 5-то число на следващия месец след изтичане на предходното тримесечие. Доклади подлежат на съгласуване и одобрение от Възложителя.

3.4. Специални условия

Достъпът на Изпълнителя до помещенията, в които се намира оборудването, обект на договора, ще се извършва по начина и във времето, допустими съгласно правилата и инструкциите за организация на охраната и пропускателния режим в двата визови центъра на Възложителя (НВЦ и РВЦ).

Дата: 25.05.2016

Представляващ ДЗЗД Ай Би Ес Индекс, съгласно Договор за консорциум от 19.05.2016,

Горан Ангелов, Управител на Водещ съдружник Ай Би Ес – България ЕООД:

(печат на Водещ съдружник, съгласно т. 3.5. от Договор за консорциум от 19.05.2016)

Даниел Комерс
Е.Т. "Даниел-Комерс-Поля Петрова"
1113-София,ул. "Ж.Кюри"46,тел:02/865 74 27,тел/факс:02/866 12 45
E-mail:danielcommerce@mail.orbitel.bg

Превод от английски език

На бланка на Bureau Veritas Certification

Lenovo Group Ltd.

Адрес: 1009 ThinkPlace Morrisville, NC 27560 USA

Моля, вижте приложението за допълнителни сертифицирани местоположения.

Bureau Veritas Certification удостоверява, че системата за управление на горепосочената организация е одитирана и се установи, че съответства на изискванията на стандартите за системи за управление по-долу:

Стандарти

ISO 9001:2008

Обхват на сертификация

Дизайн, разработка, производство, маркетинг, продажби и услуги на Lenovo компютърни продукти и устройства

Начална дата на сертификационния цикъл: 17 юни 2013

Обект на продължителното задоволително действие на системата за управление на организацията, този сертификат изтича на: 16 юни 2016

Сертификат No. US005995-1

(не се чете)

сертифициращ орган

Долуподписаният Д.Николчев с настоящото удостоверявам верността на извършения от мен превод от английски език на български език на приложения тук документ-сертификат. Преводът съдържа 1 страница.

Преводач: ....

ДАНИЕЛ КОМЕРС * СОФИЯ * DANIEL COMMERCE * SOFIA

ВЯРНО С ОРИГИНАЛА

BUREAU VERITAS
Certification

LENOVO GROUP LTD.

Executive HQ: 1009 Think Place Morrisville, NC 27560 USA

PLEASE SEE APPENDIX FOR ADDITIONAL CERTIFIED LOCATIONS

Bureau Veritas Certification certifies that the Management System of the above organization has been audited and found to be in accordance with the requirements of the management system standards detailed below

Standards

ISO 9001:2008

Scope of certification

Design, development, manufacturing fulfillment, marketing, sales and services of Lenovo computer products and devices

Certification cycle start date: **17 June 2013**

Subject to the continued satisfactory operation of the organization's Management System, this certificate expires on: **16 June 2016**

Certificate No. US005995-1

Certification Authority

Certification body address: Brandon House, 180 Borough High Street, London SE1 1LB,United Kingdom

Local office: Bureau Veritas Certification North America, Inc.
390 Benmar Drive, Houston, Texas, USA
www.us.bureauveritas.com/bvc

UKAS MANAGEMENT SYSTEMS
008

Further clarifications regarding the scope of this certificate and the applicability of the management system requirements may be obtained by consulting the organization.
To check this certificate validity please call **+(800) 937-9311**.

ВЯРНО С ОРИГИНАЛА

Заличени съгласно
чл. 2 от ЗЗЛД