Velox | Сигурна ИТ инфраструктура

ПОРЕДИЦА NIS2 · КНИЖКА 2 ОТ 4

Готови ли сте за NIS2?

Въпросник за самооценка:
117 въпроса в 15 области

Оценете | Пресметнете | Определете приоритетите

Велокс ООД · София

www.velox-systems.com

Как да използвате въпросника

1. **Съберете екипа.** Попълвайте заедно: човек от ръководството и отговорният за ИТ. Отделете 60–90 минути.
2. **Отговаряйте честно.** Отбелязвайте реалното състояние днес, не плановете. „Напълно внедрено“ значи, че работи, документирано е и се проверява.
3. **Използвайте „Н/П“ пестеливо.** Само когато въпросът наистина не се отнася за вас. Тези въпроси не се броят в резултата.
4. **Пресметнете всяка област.** Сумирайте точките и преброете отговорените въпроси (без Н/П). Резултат = сума ÷ (4 × отговорени) × 100.
5. **Нанесете резултатите.** Пренесете процентите в обобщението и в паяжината в края на книжката.

0	Не — нищо не е направено
1	Начален етап — има намерение или първи стъпки
2	Частично — около половината е направено
3	Почти готово — остават дребни неща
4	Напълно внедрено — работи, документирано е и се проверява
Н/П	Не е приложимо — не се брои в резултата

Организация _____

Попълнили _____

Дата _____

Областите

Всяка област посочва мерките от NIS2 (чл. 21, ал. 2 и други членове), които проверява, и съответните изисквания и контроли от ISO/IEC 27001:2022. Така въпросникът е полезен и за организации, които вече работят по ISO 27001.

01	Обхват и регистрация	5 въпр.	4
02	Ръководство и отговорност	8 въпр.	5
03	Управление на риска и политики	8 въпр.	6
04	Активи и инвентаризация	7 въпр.	7
05	Контрол на достъпа и MFA	10 въпр.	8
06	Мрежова сигурност	10 въпр.	9
07	Крайни устройства и имейл	8 въпр.	10
08	Наблюдение, логове и SIEM	10 въпр.	11
09	Инциденти и докладване	10 въпр.	12
10	Непрекъснатост и резервни копия	9 въпр.	13
11	Уязвимости и актуализации	8 въпр.	14
12	Криптография	5 въпр.	15
13	Доставчици	7 въпр.	16
14	Персонал, обучение и киберхигиена	7 въпр.	17
15	Проверка на ефективността	5 въпр.	18
—	Обобщение на резултата		19
—	Паяжина на готовността		20
—	Как да тълкувате резултата		21

0 Не · **1** Начален етап · **2** Частично · **3** Почти готово · **4** Напълно внедрено · **Н/П** Не е приложимо

01 Обхват и регистрация

NIS2: чл. 2, 3, 27 · ISO 27001:2022: Кл. 4.3 · A.5.31

№	Въпрос	0	1	2	3	4	Н/П
1.1	Проверили ли сте дали дейността ви попада в секторите от Приложения I или II?	☐	☐	☐	☐	☐	☐
1.2	Определили ли сте дали сте средно или голямо предприятие, като сте отчели и свързаните и партньорските предприятия?	☐	☐	☐	☐	☐	☐
1.3	Знаете ли дали сте съществен или важен субект?	☐	☐	☐	☐	☐	☐
1.4	Подадени ли са данните ви към компетентния орган и актуални ли са?	☐	☐	☐	☐	☐	☐
1.5	Има ли процедура, с която съобщавате промени в данните си в двуседмичния срок?	☐	☐	☐	☐	☐	☐

Резултат, област 01 **Сума** _____ **Отговорени** _____ **%** _____

0 Не · **1** Начален етап · **2** Частично · **3** Почти готово · **4** Напълно внедрено · **Н/П** Не е приложимо

02 Ръководство и отговорност

NIS2: чл. 20 · ISO 27001:2022: Кл. 5 · A.5.1, A.5.2, A.5.4

№	Въпрос	0	1	2	3	4	Н/П
2.1	Ръководството официално ли е одобрило мерките за управление на киберрисковете?	☐	☐	☐	☐	☐	☐
2.2	Има ли определен отговорник за киберсигурността с ясни правомощия?	☐	☐	☐	☐	☐	☐
2.3	Описани ли са писмено ролите и отговорностите по сигурността?	☐	☐	☐	☐	☐	☐
2.4	Получава ли ръководството редовни отчети за състоянието на киберсигурността?	☐	☐	☐	☐	☐	☐
2.5	Има ли отделен бюджет за киберсигурност?	☐	☐	☐	☐	☐	☐
2.6	Преминали ли са членовете на ръководството обучение по киберсигурност през последните две години?	☐	☐	☐	☐	☐	☐
2.7	Обсъжда ли ръководството киберсигурността поне веднъж на тримесечие?	☐	☐	☐	☐	☐	☐
2.8	Документирани ли са решенията на ръководството по киберсигурност?	☐	☐	☐	☐	☐	☐

Резултат, област 02 **Сума** _____ **Отговорени** _____ **%** _____

0 Не · **1** Начален етап · **2** Частично · **3** Почти готово · **4** Напълно внедрено · **Н/П** Не е приложимо

03 Управление на риска и политики

NIS2: (a) · ISO 27001:2022: Кл. 6.1, 8.2 · A.5.1, A.5.37

№	Въпрос	0	1	2	3	4	Н/П
3.1	Има ли одобрена политика за информационна сигурност?	☐	☐	☐	☐	☐	☐
3.2	Направена ли е оценка на киберрисковете през последните 12 месеца?	☐	☐	☐	☐	☐	☐
3.3	Има ли регистър на рисковете с отговорник и срок за всеки риск?	☐	☐	☐	☐	☐	☐
3.4	Има ли план за намаляване на основните рискове?	☐	☐	☐	☐	☐	☐
3.5	Преглеждат ли се политиките поне веднъж годишно?	☐	☐	☐	☐	☐	☐
3.6	Запознати ли са служителите с политиките срещу подпис?	☐	☐	☐	☐	☐	☐
3.7	Документирани ли са ключовите процедури по сигурността?	☐	☐	☐	☐	☐	☐
3.8	Оценяват ли се рисковете при всяка съществена промяна в системите?	☐	☐	☐	☐	☐	☐

Резултат, област 03 **Сума** _____ **Отговорени** _____ **%** _____

0 Не · **1** Начален етап · **2** Частично · **3** Почти готово · **4** Напълно внедрено · **Н/П** Не е приложимо

04 Активи и инвентаризация

NIS2: (i) · ISO 27001:2022: A.5.9, A.5.10, A.5.12, A.8.9

№	Въпрос	0	1	2	3	4	Н/П
4.1	Има ли пълен и актуален списък на компютрите, сървърите и мрежовите устройства?	☐	☐	☐	☐	☐	☐
4.2	Има ли списък на използвания софтуер и облачните услуги?	☐	☐	☐	☐	☐	☐
4.3	Има ли всеки актив определен отговорник?	☐	☐	☐	☐	☐	☐
4.4	Класифицирани ли са данните според важността им?	☐	☐	☐	☐	☐	☐
4.5	Знаете ли къде се съхраняват критичните ви данни?	☐	☐	☐	☐	☐	☐
4.6	Има ли правила за приемливо използване на служебните устройства?	☐	☐	☐	☐	☐	☐
4.7	Документирани ли са стандартните сигурни настройки на устройствата?	☐	☐	☐	☐	☐	☐

Резултат, област 04 **Сума** _____ **Отговорени** _____ **%** _____

0 Не · **1** Начален етап · **2** Частично · **3** Почти готово · **4** Напълно внедрено · **Н/П** Не е приложимо

05 Контрол на достъпа и MFA

NIS2: (i) (ĭ) · ISO 27001:2022: A.5.15–5.18, A.8.2, A.8.5

№	Въпрос	0	1	2	3	4	Н/П
5.1	Има ли всеки потребител собствен акаунт, без общи акаунти?	☐	☐	☐	☐	☐	⬚
5.2	Дават ли се правата по принципа на минималния необходим достъп?	☐	☐	☐	☐	☐	⬚
5.3	Има ли процедура за откриване, промяна и закриване на достъп?	☐	☐	☐	☐	☐	⬚
5.4	Спира ли се достъпът на напускащите служители в последния им работен ден?	☐	☐	☐	☐	☐	⬚
5.5	Преглеждат ли се правата за достъп поне веднъж на шест месеца?	☐	☐	☐	☐	☐	⬚
5.6	Включено ли е MFA за имейла и облачните услуги?	☐	☐	☐	☐	☐	⬚
5.7	Включено ли е MFA за VPN и отдалечения достъп?	☐	☐	☐	☐	☐	⬚
5.8	Работят ли администраторите с отделни привилегировани акаунти?	☐	☐	☐	☐	☐	⬚
5.9	Има ли политика за сложни пароли или мениджър на пароли?	☐	☐	☐	☐	☐	⬚
5.10	Използват ли се методи за MFA, устойчиви на фишинг?	☐	☐	☐	☐	☐	⬚

Резултат, област 05 **Сума** _____ **Отговорени** _____ **%** _____

0 Не · **1** Начален етап · **2** Частично · **3** Почти готово · **4** Напълно внедрено · **Н/П** Не е приложимо

06 Мрежова сигурност

NIS2: (g) (u) · ISO 27001:2022: A.8.20–8.23

№	Въпрос	0	1	2	3	4	Н/П
6.1	Защитена ли е мрежата със защитна стена от ново поколение (NGFW)?	☐	☐	☐	☐	☐	☐
6.2	Активни ли са абонаментите за защита на NGFW (IPS, антивирус, уеб филтър)?	☐	☐	☐	☐	☐	☐
6.3	Разделена ли е мрежата на сегменти (офис, сървъри, гости, IoT)?	☐	☐	☐	☐	☐	☐
6.4	Отделена ли е мрежата за гости от служебната?	☐	☐	☐	☐	☐	☐
6.5	Възможен ли е отдалеченият достъп само през VPN?	☐	☐	☐	☐	☐	☐
6.6	Затворени ли са към интернет панелите за управление и RDP?	☐	☐	☐	☐	☐	☐
6.7	Използва ли се WPA2/WPA3-Enterprise за служебната безжична мрежа?	☐	☐	☐	☐	☐	☐
6.8	Преглеждат ли се правилата на защитната стена поне веднъж годишно?	☐	☐	☐	☐	☐	☐
6.9	Филтрират ли се опасните сайтове и DNS заявки?	☐	☐	☐	☐	☐	☐
6.10	Сменени ли са фабричните пароли на всички мрежови устройства?	☐	☐	☐	☐	☐	☐

Резултат, област 06 **Сума** _____ **Отговорени** _____ **%** _____

0 Не · **1** Начален етап · **2** Частично · **3** Почти готово · **4** Напълно внедрено · **Н/П** Не е приложимо

07 Крайни устройства и имейл

NIS2: (б) (g) (з) · ISO 27001:2022: A.6.7, A.8.1, A.8.7, A.8.19

№	Въпрос	0	1	2	3	4	Н/П
7.1	Инсталирана ли е EDR защита на всички компютри?	☐	☐	☐	☐	☐	☐
7.2	Инсталирана ли е EDR защита на всички сървъри?	☐	☐	☐	☐	☐	☐
7.3	Управляват ли се централно мобилните устройства (MDM)?	☐	☐	☐	☐	☐	☐
7.4	Криптирани ли са дисковете на лаптопите?	☐	☐	☐	☐	☐	☐
7.5	Ограничено ли е инсталирането на софтуер от потребителите?	☐	☐	☐	☐	☐	☐
7.6	Има ли филтър срещу фишинг и зловредни прикачени файлове?	☐	☐	☐	☐	☐	☐
7.7	Настроени ли са SPF, DKIM и DMARC за вашия домейн?	☐	☐	☐	☐	☐	☐
7.8	Има ли правила за работа от разстояние и от лични устройства?	☐	☐	☐	☐	☐	☐

Резултат, област 07 **Сума** _____ **Отговорени** _____ **%** _____

0 Не · **1** Начален етап · **2** Частично · **3** Почти готово · **4** Напълно внедрено · **Н/П** Не е приложимо

08 Наблюдение, логове и SIEM

NIS2: (б) (е) · ISO 27001:2022: A.8.15–8.17

№	Въпрос	0	1	2	3	4	Н/П
8.1	Наблюдават ли се наличността и състоянието на сървърите и мрежата?	☐	☐	☐	☐	☐	☐
8.2	Има ли автоматични сигнали при отказ?	☐	☐	☐	☐	☐	☐
8.3	Събират ли се логовете от защитната стена, сървърите и облачните услуги на едно място?	☐	☐	☐	☐	☐	☐
8.4	Защитени ли са логовете от промяна и изтриване?	☐	☐	☐	☐	☐	☐
8.5	Определен ли е срок за съхранение на логовете?	☐	☐	☐	☐	☐	☐
8.6	Използва ли се SIEM за анализ и свързване на събитията?	☐	☐	☐	☐	☐	☐
8.7	Синхронизирано ли е времето на всички системи (NTP)?	☐	☐	☐	☐	☐	☐
8.8	Има ли определен човек или услуга, които реагират на сигналите?	☐	☐	☐	☐	☐	☐
8.9	Работи ли наблюдението и извън работно време?	☐	☐	☐	☐	☐	☐
8.10	Преглеждат ли се редовно неуспешните опити за вход и подозрителната активност?	☐	☐	☐	☐	☐	☐

Резултат, област 08 **Сума** _____ **Отговорени** _____ **%** _____

0 Не · **1** Начален етап · **2** Частично · **3** Почти готово · **4** Напълно внедрено · **Н/П** Не е приложимо

09 Инциденти и докладване

NIS2: (б) · чл. 23 · ISO 27001:2022: A.5.24–5.28, A.6.8

№	Въпрос	0	1	2	3	4	Н/П
9.1	Има ли писмен план за реакция при инциденти?	☐	☐	☐	☐	☐	☐
9.2	Определени ли са ролите и заместниците при инцидент?	☐	☐	☐	☐	☐	☐
9.3	Има ли критерии кога един инцидент е значителен?	☐	☐	☐	☐	☐	☐
9.4	Знаете ли към кой екип за реагиране (СЕРИКС) докладвате?	☐	☐	☐	☐	☐	☐
9.5	Има ли готови шаблони за уведомленията до 24 и до 72 часа?	☐	☐	☐	☐	☐	☐
9.6	Знаят ли служителите как и на кого да съобщят за подозрително събитие?	☐	☐	☐	☐	☐	☐
9.7	Има ли процедура за запазване на доказателства?	☐	☐	☐	☐	☐	☐
9.8	Има ли ред за уведомяване на КЗЛД при засегнати лични данни?	☐	☐	☐	☐	☐	☐
9.9	Тестван ли е планът за инциденти през последните 12 месеца?	☐	☐	☐	☐	☐	☐
9.10	Анализират ли се инцидентите след приключването им?	☐	☐	☐	☐	☐	☐

Резултат, област 09 **Сума** _____ **Отговорени** _____ **%** _____

0 Не · **1** Начален етап · **2** Частично · **3** Почти готово · **4** Напълно внедрено · **Н/П** Не е приложимо

10 Непрекъснатост и резервни копия

NIS2: (в) · ISO 27001:2022: A.5.29, A.5.30, A.8.13, A.8.14

№	Въпрос	0	1	2	3	4	Н/П
10.1	Правят ли се автоматично резервни копия на всички критични данни и системи?	☐	☐	☐	☐	☐	☐
10.2	Има ли копие извън офиса или извън основния облак?	☐	☐	☐	☐	☐	☐
10.3	Има ли неизменимо или офлайн копие?	☐	☐	☐	☐	☐	☐
10.4	Защитен ли е с MFA достъпът до системата за резервни копия?	☐	☐	☐	☐	☐	☐
10.5	Тества ли се възстановяването поне веднъж на тримесечие?	☐	☐	☐	☐	☐	☐
10.6	Определени ли са RTO и RPO за критичните системи?	☐	☐	☐	☐	☐	☐
10.7	Има ли план за непрекъснатост на дейността?	☐	☐	☐	☐	☐	☐
10.8	Има ли план за кризисно управление и комуникация?	☐	☐	☐	☐	☐	☐
10.9	Резервирани ли са критичните компоненти (интернет, захранване, ключови сървъри)?	☐	☐	☐	☐	☐	☐

Резултат, област 10 **Сума** _____ **Отговорени** _____ **%** _____

0 Не · **1** Начален етап · **2** Частично · **3** Почти готово · **4** Напълно внедрено · **Н/П** Не е приложимо

11 Уязвимости и актуализации

NIS2: (g) · ISO 27001:2022: A.8.8, A.8.25, A.8.32

№	Въпрос	0	1	2	3	4	Н/П
11.1	Инсталират ли се критичните актуализации на операционните системи до дни?	☐	☐	☐	☐	☐	☐
11.2	Актуализират ли се приложенията (браузъри, офис пакети, PDF четци)?	☐	☐	☐	☐	☐	☐
11.3	Актуализира ли се фърмуерът на защитната стена, VPN и мрежовите устройства?	☐	☐	☐	☐	☐	☐
11.4	Сканира ли се редовно за уязвимости?	☐	☐	☐	☐	☐	☐
11.5	Следите ли бюлетините за уязвимости на използваните продукти?	☐	☐	☐	☐	☐	☐
11.6	Има ли процедура за управление на промените?	☐	☐	☐	☐	☐	☐
11.7	Подменени ли са системите, които вече нямат поддръжка от производителя?	☐	☐	☐	☐	☐	☐
11.8	Проверява ли се сигурността при покупка или разработка на нов софтуер?	☐	☐	☐	☐	☐	☐

Резултат, област 11 **Сума** _____ **Отговорени** _____ **%** _____

0 Не · **1** Начален етап · **2** Частично · **3** Почти готово · **4** Напълно внедрено · **Н/П** Не е приложимо

12 Криптография

NIS2: (3) · ISO 27001:2022: A.8.24

№	Въпрос	0	1	2	3	4	Н/П
12.1	Има ли политика за използване на криптиране?	☐	☐	☐	☐	☐	☐
12.2	Криптирани ли са данните при пренос (TLS, VPN)?	☐	☐	☐	☐	☐	☐
12.3	Криптирани ли са чувствителните данни при съхранение?	☐	☐	☐	☐	☐	☐
12.4	Управляват ли се и защитени ли са ключовете и сертификатите?	☐	☐	☐	☐	☐	☐
12.5	Следи ли се изтичането на SSL/TLS сертификатите?	☐	☐	☐	☐	☐	☐

Резултат, област 12 **Сума** _____ **Отговорени** _____ **%** _____

0 Не · **1** Начален етап · **2** Частично · **3** Почти готово · **4** Напълно внедрено · **Н/П** Не е приложимо

13 Доставчици

NIS2: (г) · ISO 27001:2022: A.5.19–5.23

№	Въпрос	0	1	2	3	4	Н/П
13.1	Има ли списък на доставчиците с достъп до системите или данните ви?	☐	☐	☐	☐	☐	☐
13.2	Оценен ли е рискът от ключовите доставчици?	☐	☐	☐	☐	☐	☐
13.3	Съдържат ли договорите изисквания за сигурност?	☐	☐	☐	☐	☐	☐
13.4	Задължават ли договорите доставчиците да ви уведомяват за инциденти?	☐	☐	☐	☐	☐	☐
13.5	Ограничен и наблюдаван ли е отдаленият достъп на доставчиците?	☐	☐	☐	☐	☐	☐
13.6	Проверява ли се периодично дали доставчиците изпълняват изискванията?	☐	☐	☐	☐	☐	☐
13.7	Оценена ли е сигурността на използваните облачни услуги?	☐	☐	☐	☐	☐	☐

Резултат, област 13 **Сума** _____ **Отговорени** _____ **%** _____

0 Не · **1** Начален етап · **2** Частично · **3** Почти готово · **4** Напълно внедрено · **Н/П** Не е приложимо

14 Персонал, обучение и киберхигиена

NIS2: (ж) (и) · ISO 27001:2022: A.6.1–6.6

№	Въпрос	0	1	2	3	4	Н/П
14.1	Преминават ли всички служители обучение по киберсигурност при постъпване?	☐	☐	☐	☐	☐	☐
14.2	Има ли опреснително обучение поне веднъж годишно?	☐	☐	☐	☐	☐	☐
14.3	Правят ли се тестови фишинг кампании?	☐	☐	☐	☐	☐	☐
14.4	Съдържат ли трудовите договори задължения за поверителност?	☐	☐	☐	☐	☐	☐
14.5	Проверяват ли се кандидатите за ключови позиции?	☐	☐	☐	☐	☐	☐
14.6	Има ли процедура при напускане (връщане на техниката, спиране на достъпа)?	☐	☐	☐	☐	☐	☐
14.7	Спазват ли служителите основните правила: заключен екран, сигурни пароли, внимание към подозрителни имейли?	☐	☐	☐	☐	☐	☐

Резултат, област 14 **Сума** _____ **Отговорени** _____ **%** _____

0 Не · **1** Начален етап · **2** Частично · **3** Почти готово · **4** Напълно внедрено · **Н/П** Не е приложимо

15 Проверка на ефективността

NIS2: (e) · ISO 27001:2022: Кл. 9.1–9.3 · A.5.35

№	Въпрос	0	1	2	3	4	Н/П
15.1	Измервате ли показатели за сигурността (брой инциденти, време за актуализация и др.)?	☐	☐	☐	☐	☐	☐
15.2	Правят ли се вътрешни одити по сигурността?	☐	☐	☐	☐	☐	☐
15.3	Правени ли са външен одит или тест за проникване през последните две години?	☐	☐	☐	☐	☐	☐
15.4	Проследяват ли се откритите пропуски до отстраняването им?	☐	☐	☐	☐	☐	☐
15.5	Преглежда ли ръководството резултатите поне веднъж годишно?	☐	☐	☐	☐	☐	☐

Резултат, област 15 **Сума** _____ **Отговорени** _____ **%** _____

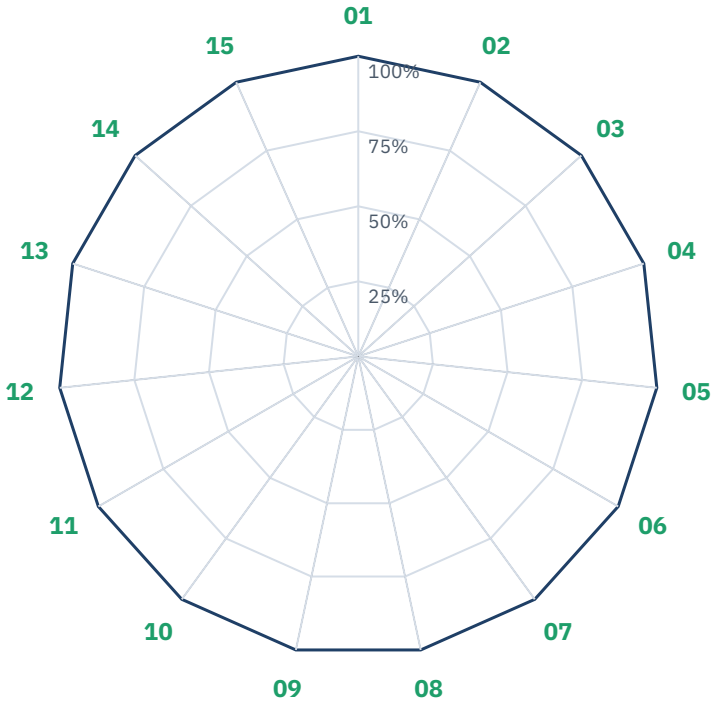
Обобщение на резултата

№	Област	Сума	Макс.	%
01	Обхват и регистрация			
02	Ръководство и отговорност			
03	Управление на риска и политики			
04	Активи и инвентаризация			
05	Контрол на достъпа и MFA			
06	Мрежова сигурност			
07	Крайни устройства и имейл			
08	Наблюдение, логове и SIEM			
09	Инциденти и докладване			
10	Непрекъснатост и резервни копия			
11	Уязвимости и актуализации			
12	Криптография			
13	Доставчици			
14	Персонал, обучение и киберхигиена			
15	Проверка на ефективността			
	Общо			

Как се смята: Макс. = 4 × броя отговорени въпроси (без Н/П). % = Сума ÷ Макс. × 100. Общият резултат се смята от общите суми, не като средно от процентите.

Паяжина на готовността

Отбележете процента на всяка област по нейната ос и свържете точките. Вдлъбнатините показват слабите места.



01 Обхват и регистрация
02 Ръководство и отговорност
03 Управление на риска и политики
04 Активи и инвентаризация
05 Контрол на достъпа и MFA
06 Мрежова сигурност
07 Крайни устройства и имейл
08 Наблюдение, логове и SIEM
09 Инциденти и докладване
10 Непрекъснатост и резервни копия
11 Уязвимости и актуализации
12 Криптография
13 Доставчици
14 Персонал, обучение и киберхигиена
15 Проверка на ефективността

Как да тълкувате резултата

Под 40% · Сериозни пропуски

Основите липсват. Нужен е план с ясни приоритети и бюджет, започнете от областите с най-нисък резултат.

40–69% · В процес

Има добра основа, но и празни места. Затворете пропуските в най-слабите области и документирайте направеното.

70% и повече · Добра готовност

Повечето мерки работят. Фокусирайте се върху доказателствата, редовните проверки и непрекъснатото подобрение.

ПРИОРИТЕТ НЕЗАВИСИМО ОТ ОБЩИЯ РЕЗУЛТАТ

Ако някоя от областите 05 (Контрол на достъпа и MFA), 09 (Инциденти и докладване) или 10 (Резервни копия) е под 50%, започнете от нея. Там се решава дали една атака ще бъде неприятност или криза.

Самооценката е ориентир и не замества одит или правна консултация. Тя показва къде да насочите усилията си първо.

Бележки

Velox | Сигурна ИТ инфраструктура

Следващата стъпка

Самооценката показва къде сте. Ние ще ви помогнем да стигнете дотам, където трябва да бъдете. Велокс е сертифицирана по ISO 27001 и прилага същите изисквания и в собствената си работа.

Преглед на резултата
Обсъждаме попълнения въпросник и уточняваме приоритетите.

Оценка на готовността
Проверка на място и подробен списък с пропуски.

Технически мерки
NGFW, SIEM, наблюдение на системите, MFA, резервни копия.

Абонаментна поддръжка
Постоянна грижа за системите, актуализации и наблюдение.

СВЪРЖЕТЕ СЕ С НАС

www.velox-systems.com

office@velox-systems.com

ПОРЕДИЦА NIS2

Кратки практически книжки за ръководители, които искат да разберат NIS2 и да действат.

1 · NIS2 · Въведение

2 · Въпросник за самооценка

3 · Наръчник по внедряване

4 · Действие при инцидент

Velox | Сигурна ИТ инфраструктура

www.velox-systems.com
office@velox-systems.com

© 2026 Велокс ООД. Информационен материал, не е правна консултация.