Додаток 2
до Методичних рекомендацій щодо
проведення зовнішнього оцінювання
поточного стану кіберзахисту
(пункт 3 розділу ІІ)

Критерії оцінки стану впровадження заходів з кіберзахисту з каталогу заходів з кіберзахисту

1. Організаційний контекст (GV.OC)

1.1. GV.OC-01 Забезпечити розуміння місії суб'єкта та її врахування при управлінні ризиками кібербезпеки

GV.OC-01 [01] Чи описано місію (мету функціонування) суб'єкта (наприклад, через бачення продуктів та послуг, які надаватиме суб'єкт, маркетинг та стратегії надання послуг), структуру та організаційні схеми забезпечення кібербезпеки для визначення ризиків кібербезпеки, які можуть перешкодити функціонуванню суб'єкта відповідно до його мети?

1.2. GV.OC-02 Визначити внутрішні та зовнішні заінтересовані сторони, забезпечити розуміння та врахування їхніх потреб і очікувань щодо управління ризиками

GV.OC-02 [01] Чи визначено підрозділи/посадові особи та їхні потреби/очікування від управління ризиками кібербезпеки?

GV.OC-02 [02] Чи визначено зовнішні заінтересовані сторони та їхні очікування щодо результатів управління ризиками кібербезпеки?

1.3. GV.OC-03 Визначити та забезпечити виконання співробітниками чинних законодавчих, нормативних та договірних вимог, а також вимог суб'єкта щодо кібербезпеки, включаючи вимоги щодо нерозголошення конфіденційної інформації та захисту прав та свобод

GV.OC-03[01] Чи визначено процес відстеження та впровадження змін законодавства щодо кіберзахисту та захисту інформації?

GV.OC-03[02] Чи визначено процес щодо відстеження дотримання партнерами договірних вимог; визначено стратегію управління ризиками кібербезпеки, узгоджено з правовими, нормативними та договірними вимогами та їх змінами?

1.4. GV.OC-04 Визначити та довести до відома співробітників ключові цілі, критичні послуги та спроможності суб'єкта

GV.OC-04[01] Чи встановлено критерії для визначення критичних спроможностей для послуг, які надаються внутрішніми і зовнішніми заінтересованими сторонами?

GV.OC-04[02] Чи визначено активи та операційні процеси, які безпосередньо впливають на досягнення цілей місії суб'єкта, і потенційний вплив від втрати (або часткової втрати) таких операційних процедур?

1.5. GV.OC-05 Визначити наслідки, спроможності та послуги, від яких залежить діяльність суб’єкта, забезпечити їх усвідомлення співробітниками

GV.OC-05[01] Чи створено зв’язки та визначено залежності суб’єкта від зовнішніх ресурсів (наприклад, систем, операторів електронних комунікацій, мереж електроживлення тощо) та їхні зв’язки з організаційними активами та послугами (сервісами)?

GV.OC-05[02] Чи визначено та задокументовано зовнішні залежності, які є ключовими точками для втрати суб’єктом критичних спроможностей та послуг, та чи доведено їх до відома визначених посадових осіб?

2. Стратегія управління ризиками (GV.RM)

2.1. GV.RM-01 Визначити та узгодити із заінтересованими сторонами суб’єкта цілі управління ризиками кібербезпеки

GV.RM-01[01] Чи оновлено/переглядаються з визначеною частотою короткострокові та довгострокові цілі з управління ризиками кібербезпеки, як частини річного стратегічного планування та в разі значних змін;?

GV.RM-01[02] Чи встановлено вимірювальні показники в рамках досягнення цілей управління ризиками кібербезпеки?

GV.RM-01[03] Чи погоджено з керівництвом цілі кібербезпеки, які використовуються ним у повсякденній діяльності, щодо заходів з управління ризиками кібербезпеки?

2.2. GV.RM-02 Визначити допустимий рівень ризику кібербезпеки, який суб’єкт може прийняти, довести до відома всіх співробітників та заінтересованих сторін і підтримувати таку інформацію в актуальному стані

GV.RM-02[01] Чи визначено допустимий рівень ризику кібербезпеки суб’єкта, який відповідає очікуванням щодо належного рівня ризику?

GV.RM-02[02] Чи інформація про готовність суб’єкта приймати певний рівень ризику кібербезпеки перенесена до розділу про допустимий рівень ризику?

GV.RM-02[03] Чи інформація про готовність суб’єкта до прийняття ризиків кібербезпеки та визначений допустимий рівень ризику доведена до відома співробітників та суб’єкта, інших заінтересованих сторін у конкретний, вимірюваний і зрозумілий спосіб?

GV.RM-02[04] Чи встановлено періодичність уточнення інформації про допустимий рівень ризику кібербезпеки?

2.3. GV.RM-03 Додати до загальних процесів управління ризиками суб’єкта діяльність з управління ризиками кібербезпеки та досягнення її цілей

GV.RM-03[01] Чи об’єднано ризики кібербезпеки, які управляються разом з іншими ризиками ?

GV.RM-03[02] Чи залучено менеджерів з управління ризиками кібербезпеки до планування управління ризиками суб’єкта?

GV.RM-03[03] Чи встановлено критерії для передачі ризиків кібербезпеки на більш високий рівень управління в рамках управління ризиками суб’єкта?

2.4. GV.RM-04 Визначити та довести до відома співробітників стратегічні напрями, які описують відповідні варіанти реагування на ризики кібербезпеки

GV.RM-04[01] Чи визначено варіанти реагування на ризик кібербезпеки, наприклад: зменшення ризику шляхом впровадження нових заходів кіберзахисту або посилення наявних заходів; прийняття ризику з відповідним обґрунтуванням; обмін, перенесення ризику або відхилення ризику?

GV.RM-04[02] Чи визначено критерії прийняття та уникнення ризику кібербезпеки для даних різних класифікацій?

GV.RM-04[03] Чи описано умови, за яких прийнятні моделі спільної відповідальності?

GV.RM-04[04] Чи ознайомлено співробітників суб’єкта та заінтересовані сторони?

2.5. GV.RM-05 Визначити та довести до відома співробітників способи обміну інформацією всередині суб’єкта щодо ризиків кібербезпеки, включаючи ризики, які несуть постачальники товарів, робіт, послуг та інші треті сторони

GV.RM-05[01] Чи визначено та узгоджено проміжки часу інформування старших керівників, директорів і керівництво про стан кібербезпеки суб’єкта?

GV.RM-05[02] Чи визначено механізми спілкування та інформування в рамках управління ризиками кібербезпеки у суб’єкті, наприклад, керівництво, служба безпеки суб’єкта, юридичний відділ, відділ закупівель, відділ фізичної безпеки та кадровий відділ спілкуватимуться між собою щодо ризиків кібербезпеки?

2.6. GV.RM-06 Визначити та довести до відома співробітників стандартизовані методи розрахунку, документування, ідентифікації та визначення пріоритетності ризиків кібербезпеки

GV.RM-06[01] Чи встановлено критерії для використання кількісного підходу до аналізу ризиків кібербезпеки?

GV.RM-06[02] Чи створено шаблони (наприклад, реєстр ризиків) для документування інформації про ризики кібербезпеки (включаючи опис ризику, контактну особу, відповідальну за ризик, загрозу)?

GV.RM-06[03] Чи встановлено критерії для визначення пріоритетів ризиків кібербезпеки для суб’єкта?

GV.RM-06[04] Чи використовується перелік категорій ризиків кібербезпеки для їх збору, накопичення та порівняння?

2.7. GV.RM-07 Визначити, охарактеризувати та забезпечувати обговорення зі співробітниками суб’єкта стратегічних можливостей щодо управління ризиками кібербезпеки

GV.RM-07[01] Чи визначено методи для виявлення можливостей і включення їх в обговорення ризиків кібербезпеки (наприклад, аналіз сильних і слабких сторін, можливостей і загроз [SWOT])?

GV.RM-07[02] Чи визначено та затверджено додаткові цілі?

GV.RM-07[03] Чи розраховано та затверджено пріоритетність позитивних ризиків кібербезпеки разом із негативними?

3. Ролі, обов'язки та повноваження (GV.RR)

3.1. GV.RR-01 визначити із числа керівництва суб'єкта посадову особу, яка звітує про ризики кібербезпеки та підтримання культури поведінки щодо усвідомлення ризиків та етики, її постійне вдосконалення, а також відповідає за них

GV.RR-01[01] Чи керівництвом узгоджено власні ролі та обов'язки щодо розробки, впровадження та оцінювання виконання стратегії кібербезпеки?

GV.RR-01[02] Чи доведено до відома співробітників суб'єкта очікування керівників щодо безпечної та етичної культури, особливо коли поточні події надають можливість підкреслити позитивні або негативні приклади управління ризиками кібербезпеки?

GV.RR-01[03] Чи утворено підрозділ з кіберзахисту, призначено керівника з кіберзахисту або відповідальну особу, яка виконує функції та завдання керівника з кіберзахисту відповідно до статті 51 Закону України «Про основні засади забезпечення кібербезпеки України», до завдань якого належить проведення заходів з управління ризиками кібербезпеки?

GV.RR-01[04] Чи проведено перевірки для забезпечення розуміння співробітниками своїх повноважень і налагодження координації між особами, відповідальними за управління ризиками кібербезпеки?

3.2. GV.RR-02 Встановити, забезпечити комунікацію, розуміння та дотримання ролей та повноважень щодо управління ризиками

GV.RR-02[01] Чи визначено в політиці та затверджено ролі та обов'язки з управління ризиками кібербезпеки?

GV.RR-02[02] Чи визначено відповідальних посадових осіб за діяльність з управління ризиками кібербезпеки, механізми проведення консультацій та механізми їх інформування?

GV.RR-02[03] Чи до посадових обов'язків включено та до відома співробітників доведено обов'язковість виконання вимог з кібербезпеки?

GV.RR-02[04] Чи затверджено показники продуктивності для співробітників, які виконують обов'язки з управління ризиками кібербезпеки; чи проводиться періодичне вимірювання продуктивності, щоб визначити напрями для покращення?

GV.RR-02[05] Чи визначено обов'язки з кібербезпеки в межах операцій, функцій управління ризиками кібербезпеки та функцій внутрішнього аудиту?

3.3. GV.RR-03 Визначити необхідні ресурси відповідно до стратегії управління ризиками кібербезпеки, ролей, відповідальності та політик

GV.RR-03[01] Чи забезпечено періодичні перевірки керівництва, щоб переконатися, що ті, хто відповідає за управління ризиками кібербезпеки, мають необхідні повноваження?

GV.RR-03[02] Чи забезпечено відповідність розподілу ресурсів та інвестиції ризику заходам протидії ризику кібербезпеки?

GV.RR-03[03] Чи забезпечено достатню кількість людей, процесів і технічних ресурсів для підтримки виконання заходів стратегії кібербезпеки?

3.4. GV.RR-04 Включити питання кібербезпеки в практики управління персоналом

GV.RR-04 [01] Чи у кадрову політику внесено управління ризиками кібербезпеки (наприклад, перевірка співробітників перед прийняттям на роботу, адаптація, сповіщення про зміни, звільнення)?

GV.RR-04 [02] Чи при підборі кадрів знання та навички кандидатів з кібербезпеки визначено як позитивний фактор?

GV.RR-04 [03] Чи проводиться перевірка біографій перед прийомом на роботу нових співробітників на чутливі посади?

GV.RR-04 [04] Чи періодично повторюються перевірки біографії для співробітників на таких посадах?

GV.RR-04 [05] Чи забезпечено перевірку дотримання співробітниками зобов’язань щодо знання, дотримання та підтримки політики безпеки відповідно до їхніх ролей та посадових інструкцій?

4. Політика (GV.PO)

4.1. GV.PO-01 Розробити та довести до відома співробітників суб’єкта політику управління ризиками кібербезпеки, яка визначена з урахуванням структури суб’єкта, стратегії кібербезпеки та пріоритетів

GV.PO-01 [01] Чи створено, поширено та підтримується політика управління ризиками кібербезпеки, яка зрозуміла та враховує цілі, очікування та спрямування керівництва суб’єкта?

GV.PO-01 [02] Чи проводиться періодичний перегляд політики та допоміжних послуг (сервісів) кібербезпеки для їх узгодження із цілями та пріоритетами стратегії управління ризиками кібербезпеки, а також з керівництвом політики кібербезпеки на високому рівні?

GV.PO-01 [03] Чи затверджено політику керівництвом вищого рівня та доведено її до відома всіх співробітників?

GV.PO-01 [04] Чи співробітниками отримано та вивчено політики під час першого прийому на роботу, щорічно та у разі внесення оновлень до неї?

4.2. GV.PO-02 Забезпечити періодичний перегляд, оновлення та виконання політики управління ризиками кібербезпеки з урахуванням змін нормативних вимог, загроз, технологій та місії суб’єкта

GV.PO-02 [01] Чи оновлено політику управління ризиками кібербезпеки на основі періодичних перевірок результатів управління ризиками кібербезпеки, щоб гарантувати, що політика та допоміжні послуги (сервіси з кібербезпеки) адекватно підтримують ризик на прийнятному рівні, зміни в правових і нормативних вимогах, у технологіях (наприклад, впровадження штучного інтелекту)?

GV.PO-02 [02] Чи встановлено графік для перегляду змін у середовищі ризиків кібербезпеки суб'єкта (наприклад, зміни в ризиках або в цілях місії суб'єкта) та чи визначено рекомендації з оновлення політики?

GV.PO-02 [03] Чи оновлено політику, щоб відобразити зміни в юридичних та нормативних вимогах?

GV.PO-02 [04] Чи оновлено політику, щоб відобразити зміни в технологіях (наприклад, впровадження штучного інтелекту) та організаційній діяльності (наприклад, придбання нових активів, нові вимоги до контрактів)?

5. Контроль (GV.OV)

5.1. GV.OV-01 Забезпечити врахування результатів стратегії управління ризиками кібербезпеки для вдосконалення та коригування її напрямів

GV.OV-01 [01] Чи проаналізовано, наскільки стратегія управління ризиками кібербезпеки та результати перевірки чи аудиту системи управління ризиками допомогли керівникам приймати рішення та досягати цілей суб'єкта?

GV.OV-01 [02] Чи проаналізовано, чи чинна стратегія управління ризиками кібербезпеки потребує коригування з метою усунення чинників, які перешкоджають ефективному функціонуванню суб'єкта та впровадженню інновацій в ньому?

5.2. GV.OV-02 Забезпечити перегляд і коригування стратегії управління ризиками кібербезпеки для забезпечення охоплення нею вимог суб'єкта та ризиків

GV.OV-02 [01] Чи переглядаються результати аудиту, щоб підтвердити, чи забезпечила наявна стратегія кібербезпеки відповідність внутрішнім і зовнішнім вимогам?

GV.OV-02 [02] Чи переглядається ефективність виконання функцій, пов'язаних з кібербезпекою, щоб визначити, чи потрібні зміни в політиці управління ризиками кібербезпеки?

GV.OV-02 [03] Чи переглядається стратегія управління ризиками кібербезпеки з огляду на інциденти кібербезпеки?

5.3. GV.OV-03 Забезпечити оцінювання продуктивності управління ризиками кібербезпеки для перегляду, внесення необхідних коригувань відповідно до поточних потреб

GV.OV-03 [01] Чи переглядаються ключові індикатори виконання (KPI) для переконання, що розроблена політика та впроваджені процедури допомагають досягти постановленої мети?

GV.OV-03 [02] Чи переглядаються ключові індикатори ризику кібербезпеки (KRI), в тому числі ймовірність їх виникнення та потенційний вплив з метою визначення ризиків, які можуть виникнути?

GV.OV-03 [03] Чи збираються та доповідаються керівництву показники з управління ризиками кібербезпеки?

6. Управління ризиками ланцюга постачання (GV.SC)

6.1. GV.SC-01 Розробити програму, стратегію, цілі, політики та процеси управління ризиками кібербезпеки, пов'язаними з ланцюгами постачання, погодити їх із заінтересованими сторонами суб'єкта

GV.SC-01 [01] Чи створено стратегію, яка відображає цілі програми управління ризиками кібербезпеки ланцюга постачання?

GV.SC-01 [02] Чи розроблено програму управління ризиками кібербезпеки в ланцюжку постачання, включаючи план (з основними показниками), політики та процедури, які керують впровадженням і вдосконаленням цієї програми; чи доведені до відома заінтересованих сторін суб'єкта політики та процедури?

GV.SC-01 [03] Чи створено міжорганізаційний механізм, який забезпечує узгодженість між функціями, які сприяють управлінню ризиками кібербезпеки ланцюга постачання, наприклад: кібербезпека, безпека IT, функціонування, юридичний, кадровий та інженерний аспекти?

6.2. GV.SC-02 Розробити, довести, здійснювати внутрішню та зовнішню координацію ролей з кібербезпеки при їх виконанні постачальниками товарів, робіт, послуг, користувачами та партнерами суб'єкта

GV.SC-02 [01] Чи визначено одну (або кілька) роль/посадову особу, яка відповідає за планування, забезпечення ресурсами та виконання діяльності з управління ризиками кібербезпеки ланцюга постачання?

GV.SC-02 [02] Чи затверджено в політиці ролі управління ризиками кібербезпеки ланцюга постачання та відповідальність за них?

GV.SC-02 [03] Чи створено матрицю відповідальності для визначення посадової особи (групи посадових осіб), відповідальної за виконання заходів з управління ризиками кібербезпеки ланцюга постачання, а також чи встановлено механізми проведення консультацій та інформування такої посадової особи (груп посадових осіб)?

GV.SC-02 [04] Чи визначено у посадових обов'язках обов'язки та показники результативності щодо управління ризиками кібербезпеки ланцюга постачання та чи проводиться їх періодичне вимірювання, щоб визначити та покращити продуктивність?

GV.SC-02 [05] Чи розроблено завдання та встановлено відповідальність до постачальників, користувачів та партнерів щодо допустимих ризиків кібербезпеки ланцюга постачання, які впроваджені в політику суб'єкта та застосовуються у відповідних договорах з постачальниками?

GV.SC-02 [06] Чи повідомлено про ролі та обов'язки з управління ризиками кібербезпеки в ланцюгу постачання для третіх сторін?

GV.SC-02 [07] Чи встановлено правила та протоколи обміну інформацією та звітування між суб’єктом та постачальником?

6.3. GV.SC-03 Забезпечити інтеграцію управління ризиками ланцюга постачання у сфері кібербезпеки в процеси управління ризиками кібербезпеки суб'єкта, провести їх оцінку та вдосконалення

GV.SC-03 [01] Чи ідентифіковано та узгоджено питання кібербезпеки з управлінням ризиками кібербезпеки суб’єкта?

GV.SC-03 [02] Чи створено зведені набори заходів управління ризиками кібербезпеки та управління ризиками кібербезпеки ланцюга постачання?

GV.SC-03 [03] Управління ризиками кібербезпеки ланцюга постачання інтегровано в процеси вдосконалення?

GV.SC-03 [04] Чи доводиться до відома керівництва суб’єкта важлива інформація про ризики кібербезпеки ланцюга постачання та чи враховується на рівні управління ризиками суб’єкта?

6.4. GV.SC-04 Визначити та пріоритезувати постачальників товарів, робіт, послуг за ступенем критичності

GV.SC-04 [01] Чи розроблено критерії критичності постачальників на основі чутливості даних, які обробляються або зберігаються постачальниками, ступеня доступу до систем суб’єкта та важливості продуктів або послуг для місії суб’єкта?

GV.SC-04 [02] Чи ведеться облік усіх постачальників та чи проведено їх пріоритезацію на основі критеріїв їх критичності?

6.5. GV.SC-05 Встановити вимоги, пов’язані з ризиками кібербезпеки в ланцюгах постачання, та впровадити їх в договори/контракти або інші типи договорів з постачальниками товарів, робіт, послуг та відповідними третіми сторонами

GV.SC-05 [01] Чи визначено вимоги безпеки для постачальників, продуктів і послуг (зокрема, щодо тестування та доведення безпеки продуктів і послуг, що постачаються, протягом їх всього життєвого циклу) відповідно до рівня критичності та потенційного впливу компрометації продуктів та послуг, які ними постачаються?

GV.SC-05 [02] Чи включено до договору всі вимоги до кібербезпеки та ланцюга постачання, обов’язкові для виконання третіми сторонами, а також чи встановлено механізми перевірки дотримання цих вимог?

GV.SC-05 [03] Чи визначено правила та протоколи обміну інформацією між суб’єктом, постачальником та субпідрядником?

GV.SC-05 [04] Чи передбачено, що управління ризиками кібербезпеки щодо включення вимог з безпеки в договорі базується на критичності потенційних наслідків у випадку компрометації поставок?

GV.SC-05 [05] Чи визначено вимоги до безпеки в договорах про рівень обслуговування (SLA) для моніторингу постачальників на предмет прийнятної

продуктивності безпеки протягом усього життєвого циклу відносин з постачальниками?

GV.SC-05 [06] Чи у контрактах від постачальників вимагається:

розкривати функції, функціональні можливості та вразливості їхніх продуктів і послуг протягом усього терміну служби продукту або терміну обслуговування;

надавати та підтримувати актуальний інвентар компонентів (наприклад, перелік програмного або апаратного забезпечення) для критичних продуктів;

перевіряти своїх співробітників і захищатися від внутрішніх загроз;

надавати докази виконання прийнятних практик безпеки, наприклад, через самостійне підтвердження, відповідність чинним стандартам, вимогам сертифікації або інспекції;

вказувати у контрактах та інших договорах права та обов'язки суб'єкта, постачальників та ланцюгів постачання щодо потенційних ризиків кібербезпеки?

6.6. GV.SC-06 Забезпечити планування та комплексну перевірку постачальників товарів, робіт, послуг або інших третіх сторін для зменшення ризиків кібербезпеки перед початком договірних відносин з ними

GV.SC-06 [01] Чи проводяться ретельні перевірки потенційних постачальників, які відповідають рівню ризику кібербезпеки, критичності та складності відносин з кожним потенційним постачальником?

GV.SC-06 [02] Чи оцінено застосовність технологій та їх властивості, а також практики потенційних постачальників щодо управління ризиками кібербезпеки?

GV.SC-06 [03] Чи проведено оцінку ризиків постачальників щодо застосовності вимог з кібербезпеки?

GV.SC-06 [04] Чи проводиться оцінювання автентичності, цілісності та безпеки критичних продуктів перед їх придбанням?

6.7. GV.SC-07 Визначити ризики кібербезпеки, пов'язані з постачальником товарів, робіт, послуг, його продукцією та послугами, які він надає, з іншими третіми сторонами, усвідомити їх, зареєструвати, пріоритезувати та забезпечити реагування на них і контроль протягом всієї співпраці

GV.SC-07 [01] Чи скориговано формати та частоту оцінювання на основі репутації третьої сторони та критичності продуктів чи послуг, які вона надає?

GV.SC-07 [02] Чи оцінено докази відповідності третіх сторін вимогам щодо кібербезпеки за контрактом, як-от самоатестації, гарантії, сертифікати та інші артефакти?

GV.SC-07 [03] Чи забезпечено контроль критично важливих постачальників таким чином, що його результати (перевірки, аудити, випробування чи інші форми оцінювання) підтверджують виконання постачальниками своїх зобов'язань щодо безпеки протягом життєвого циклу відносин із постачальниками?

GV.SC-07 [04] Чи проводиться моніторинг критичних постачальників, послуг та продуктів на предмет змін у їхніх профілях ризику та переоцінюється критичність постачальників і вплив ризиків?

GV.SC-07 [05] Чи заплановано дії на випадок несподіваних перебоїв, пов'язаних з постачальниками та ланцюгами постачання, щоб забезпечити безперервність функціонування суб'єкта?

6.8. GV.SC-08 Забезпечити залучення відповідних постачальників товарів, робіт, послуг та інших третіх сторін до діяльності щодо планування, реагування на кіберінциденти, кібератаки, кіберзагрози та відновлення після них

GV.SC-08 [01] Чи визначено та використовуються правила та протоколи звітування про заходи реагування на кіберінциденти, кібератаки або кіберзагрози та відновлення, а також про статус між суб'єктом та його постачальниками?

GV.SC-08 [02] Чи визначено та затверджено ролі та відповідальність суб'єкта та його постачальників щодо реагування на кіберінциденти, кібератаки або кіберзагрози?

GV.SC-08 [03] Чи залучено критичних постачальників до тренувань та симуляцій?

GV.SC-08 [04] Чи визначено та скоординовано методи комунікацій та протоколи взаємодії, проведено спільний розгляд отриманого досвіду?

GV.SC-08 [05] Чи визначено та забезпечується координація способів кризових комунікацій та протоколів між суб'єктом та критичними постачальниками?

GV.SC-08 [06] Чи визначено та використовуються правила та протоколи звітування про заходи реагування на кіберінциденти, кібератаки або кіберзагрози та відновлення, а також статус між суб'єктом та його постачальниками?

GV.SC-08 [07] Чи проводяться спільні дослідження отриманих результатів навчань з критичними постачальниками?

6.9. GV.SC-09 Інтегрувати практичні заходи щодо забезпечення безпеки ланцюга постачання в програми суб'єкта щодо кібербезпеки та управління ризиками кібербезпеки, контролювати їх ефективність протягом всього життєвого циклу користування продуктами та послугами, які суб'єкт отримує від постачальника товарів, робіт, послуг чи інших третіх сторін

GV.SC-09 [01] Чи вимагають політики та процедури документування походження всіх придбаних технологічних продуктів і послуг?

GV.SC-09 [02] Чи періодично готуються та подаються керівництву звіти про ідентифіковані ризики кібербезпеки, а також про заходи, що підтверджують автентичність і відсутність підробок у придбаних компонентах?

GV.SC-09 [03] Чи впроваджено періодичну комунікацію з відповідальними особами за управління ризиками кібербезпеки та співробітниками, що експлуатують суб'єкт, про потреби в придбанні програмних патчів, оновлень і модернізації виключно від автентифікованих та надійних постачальників програмного забезпечення?

GV.SC-09 [04] Чи переглянуто правила, щоб переконатися, що вони вимагають взаємодії з визначеними співробітниками постачальника при виконанні технічного обслуговування його продуктів?

GV.SC-09 [05] Чи встановлено політиками вимоги та процедури щодо виявлення на дозволеної модернізації апаратного забезпечення суб’єкта?

6.10. GV.SC-10 Передбачити в планах управління ризиками кібербезпеки, пов’язаними з ланцюгами постачання, порядок дій, які необхідно виконати після прийняття рішення щодо партнерства або укладання договору про надання послуг

GV.SC-10 [01] Чи встановлено процеси для припинення критичних відносин як за нормальних, так і за несприятливих обставин?

GV.SC-10 [02] Чи визначено і впроваджено плани підтримки та обслуговування компонентів після закінчення їхнього життєвого циклу та їх фізичного зношення?

GV.SC-10 [03] Чи своєчасно деактивується доступ постачальників до ресурсів суб’єкта, коли він більше не потрібен?

GV.SC-10 [04] Чи перевіряється, що активи, які містять дані суб’єкта, повертаються або належним чином утилізуються вчасно, контрольовано та безпечно?

GV.SC-10 [05] Чи розроблено та виконується план припинення відносин або зміни постачальників, враховуючи ризики кібербезпеки безпеки ланцюга постачання та стійкість?

GV.SC-10 [06] Чи передбачено впровадження компенсаційних заходів для мінімізації рівнів ризиків кібербезпеки, пов’язаних із припиненням співпраці або зміною постачальників, які можуть вплинути на безпеку даних та систем?

GV.SC-10 [07] Чи здійснюється управління ризиками витоку даних, пов’язаних з припиненням відносин з постачальниками?

7. Управління активами (ID.AM)

7.1. ID.AM-01 Забезпечити періодичне проведення інвентаризації обладнання, яким керує суб'єкт

ID.AM-01 [01] Чи проводиться регулярна інвентаризація для всіх типів обладнання суб’єкта, включаючи IT, IoT, OT та мобільні пристрої?

ID.AM-01 [02] Чи запроваджено постійний моніторинг суб’єкта кіберзахисту, щоб виявляти нове обладнання, чи проводиться автоматична реєстрація проведених оновлень?

7.2. ID.AM-02 Забезпечити періодичне проведення інвентаризації програмного забезпечення, послуг і систем, якими керує суб'єкт

ID.AM-02 [01] Чи всі типи програмного забезпечення та послуг, у тому числі із відкритим вихідним кодом, користувацьких програм, служб API та хмарних послуг, ідентифіковано та задокументовано?

ID.AM-02 [02] Чи запроваджено постійний моніторинг всіх платформ, включаючи віртуальні машини, на наявність змін для інвентаризації оновлень для них?

ID.AM-02 [03] Чи проведено інвентаризацію всіх систем суб'єкта?

7.3. ID.AM-03 Забезпечити підтримку використання авторизованих мережевих з'єднань та визначити внутрішні і зовнішні мережеві потоки

ID.AM-03 [01] Чи підтримуються базові лінії зв'язку та потоки даних у дротових та бездротових мережах суб'єкта?

ID.AM-03 [02] Чи проведено інвентаризацію електронних комунікацій, потоків даних, які їх використовують, між суб'єктом та зовнішніми сторонами?

ID.AM-03 [03] Чи розроблено структурну схему інформаційних потоків, яка відображає інфраструктуру взаємодії між основними компонентами?

ID.AM-03 [04] Чи визначено в документації з прив'язкою до кожного порту мережі, протоколу та служби, що вони типово використовуються для авторизованих систем?

7.4. ID.AM-04 Забезпечити періодичне проведення інвентаризації послуг, що надаються постачальниками товарів, робіт, послуг

ID.AM-04 [01] Чи усі зовнішні служби та послуги, які використовуються суб'єктом, включаючи послуги IaaS, PaaS SaaS, API, та інші зовнішні служби додатків ідентифіковано та задокументовано?

ID.AM-04 [02] Чи оновлюються інвентаризаційні дані при використанні нової зовнішньої служби або послуги, щоб забезпечити адекватний моніторинг управління ризиками кібербезпеки?

7.5. ID.AM-05 Провести розподіл активів за пріоритетністю, враховуючи їх класифікацію, критичність, ресурси, вплив на місію суб'єкта

ID.AM-05 [01] Чи встановлено критерії пріоритезації активів?

ID.AM-05 [02] Чи застосовано критерії пріоритезації для кожного активу?

ID.AM-05 [03] Чи переглядаються критерії активів періодично або у разі значних змін суб'єкта?

7.6. ID.AM-07 Забезпечити інвентаризацію даних і пов'язаних з ними метаданих відповідно до визначених типів даних

ID.AM-07 [01] Чи затверджено перелік типів даних (ідентифікаційна інформація, захищена інформація про здоров'я, номери фінансових рахунків, інтелектуальна власність суб'єкта, дані про операційні технології тощо)?

ID.AM-07 [02] Чи проводиться за результатами постійного аналізу даних оновлення (у разі потреби) їх типів?

ID.AM-07 [03] Чи встановлено індикатори віднесення інформації за встановленими типами даних?

ID.AM-07 [04] Чи проводить суб'єкт відстеження походження, власника та геолокації інформації за кожним типом даних?

7.7. ID.AM-08 Забезпечити управління системами, апаратним та програмним забезпеченням, послугами та даними протягом усього їх життєвого циклу

ID.AM-08 [01] Чи розглядаються питання кібербезпеки протягом усього життєвого циклу систем, апаратного забезпечення, програмного забезпечення та послуг?

ID.AM-08 [02] Чи розглядаються питання кібербезпеки протягом життєвого циклу продуктів?

ID.AM-08 [03] Чи виявляються неофіційні використання технологій для досягнення цілей місії (тобто тіньові IT)?

ID.AM-08 [04] Чи виявляються періодично надлишкові системи, апаратне забезпечення, програмне забезпечення та послуги, які непотрібно збільшують поверхню атаки суб'єкта?

ID.AM-08 [05] Чи налаштовано належним чином і захищаються системи, апаратне забезпечення, програмне забезпечення та послуги перед їх упровадженням у виробництво?

ID.AM-08 [06] Чи проводиться оновлення даних інвентаризації, коли системи, апаратне забезпечення, програмне забезпечення та послуги переміщуються або передаються в межах суб'єкта?

ID.AM-08 [07] Чи безпечно знищуються збережені дані відповідно до політики збереження даних суб'єкта, використовуючи передбачений метод знищення; чи ведеться та здійснюється управління записами про знищення?

ID.AM-08 [08] Чи безпечно очищуються сховища даних, коли апаратне забезпечення виводиться з експлуатації, списується, замінюється або відправляється на ремонт чи заміну?

ID.AM-08 [09] Чи визначено методи знищення паперу, носіїв зберігання та інших фізичних форм зберігання даних?

Оцінка ризиків кібербезпеки (ID.RA)

8.1. ID.RA-01 Ідентифікувати, підтверджувати та вести записи щодо вразливих місць активів

ID.RA-01 [01] Чи запроваджено використання технології управління вразливостями для виявлення не налаштованого та неправильно налаштованого програмного забезпечення?

ID.RA-01 [02] Чи проводиться оцінювання архітектури мережі та системи на предмет слабких місць у проектуванні та під час впровадження, які впливають на кібербезпеку?

ID.RA-01 [03] Чи переглянуто, проаналізовано або протестовано програмне забезпечення, розроблене суб'єктом, щоб виявити вразливості в проектуванні, кодуванні та налаштуваннях за замовчуванням?

ID.RA-01 [04] Чи оцінено об'єкти, що містять критичні обчислювальні активи, на предмет фізичних вразливостей та питань стійкості?

ID.RA-01 [05] Чи проводиться моніторинг джерел розвідки кіберзагроз для отримання інформації про нові вразливості в продуктах і послугах?

ID.RA-01 [06] Чи переглянуто процеси та процедури на предмет слабких місць, які можуть бути використані для впливу на кібербезпеку?

8.2. ID.RA-02 Організувати отримання інформації про кіберзагрози та вразливості з платформи обміну інформацією про кіберінциденти, кібератаки, кіберзагрози, з репозитарію інформації про кіберінциденти, інших офіційних джерел

ID.RA-02 [01] Чи налаштовані інструменти та технології кібербезпеки з можливостями виявлення або реагування для безпечного надання та отримання зворотного зв'язку про кіберзагрози?

ID.RA-02 [02] Чи отримуються та аналізуються консультації від авторитетних третіх сторін щодо поточних суб'єктів загроз та їхньої тактики, методів і процедур (ТМП)?

ID.RA-02 [03] Чи проводиться моніторинг джерел інформації про кіберзагрози для отримання інформації про типи вразливостей, які можуть мати новітні технології?

8.3. ID.RA-03 Визначити та задокументувати внутрішні та зовнішні загрози

ID.RA-03 [01] Чи використовується кіберрозвідка для підтримки обізнаності про типи загрозливих акторів, які можуть націлюватися на суб'єкт, та їх тактику, методи і процедури (ТМП)?

ID.RA-03 [02] Чи виконується пошук загроз для виявлення ознак загрозливих акторів у середовищі?

ID.RA-03 [03] Чи реалізовані процеси для ідентифікації внутрішніх суб'єктів загроз?

8.4. ID.RA-04 Визначити та задокументувати потенційні наслідки та вірогідні загрози, пов'язані з експлуатацією кіберзагроз та вразливостей

ID.RA-04 [01] Керівники суб'єкта та фахівці з управління ризиками кібербезпеки працюють разом, щоб оцінити ймовірність та вплив сценаріїв ризиків і зареєструвати їх у реєстрах ризиків?

ID.RA-04 [02] Чи визначено та обраховано потенційний вплив несанкціонованого доступу до комунікацій суб'єкта, систем і даних, які обробляються цими системами?

ID.RA-04 [03] Чи розглядається потенційний вплив каскадних відмов у взаємопов'язаних системах, чи враховується потенційний вплив каскадних збоїв для операційних систем?

8.5. ID.RA-05 Забезпечити використання інформації про вірогідні кіберзагрози, вразливості та можливі наслідки від їх настання для розуміння невід'ємного ризику та інформування про пріоритетність реагування на ризики

ID.RA-05 [01] Чи здійснюється розвиток моделі загроз для більшого розуміння ризиків кібербезпеки, для даних та чи визначаються відповідні заходи реагування на кіберінциденти, кібератаки та кіберзагрози?

ID.RA-05 [02] Чи здійснюється пріоритезація ресурсів, що виділяються, та інвестицій у кібербезпеку на основі оцінених ймовірностей і наслідків?

8.6. ID.RA-06 Визначити заходи реагування на ризики кібербезпеки та встановити їх пріоритетність, забезпечити їх відслідковування та комунікацію щодо них

ID.RA-06 [01] Чи застосовуються критерії плану управління вразливостями для прийняття, передачі, пом’якшення або уникнення ризику кібербезпеки, або вибору компенсаційних заходів для пом’якшення ризику?

ID.RA-06 [02] Чи проводиться відстеження удосконалення процесів реагування на ризики кібербезпеки (наприклад: за затвердженим планом, який містить основні етапи реагування на ризики), чи ведеться реєстр ризиків, чи надається детальний звіт про реагування?

ID.RA-06 [03] Чи використовуються результати оцінки ризиків кібербезпеки для прийняття рішення про реагування на ризик і виконання відповідних дій?

ID.RA-06 [04] Чи інформуються заінтересовані сторони про заплановані заходи реагування на ризик кібербезпеки в пріоритетному порядку?

8.7. ID.RA-07 Забезпечити управління, оцінювання на предмет ризику кібербезпеки, реєстрацію та відстеження змін та винятків до затвердженої документації

ID.RA-07 [01] Чи запроваджено та контролюється дотримання визначених документацією процедур перегляду, оцінювання та затвердження запропонованих змін до неї?

ID.RA-07 [02] Чи здійснюється документування внесення/невнесення кожної запропонованої зміни щодо кожного можливого ризику кібербезпеки?

ID.RA-07 [03] Чи проводиться документування кожної пов’язаної з ризиком кібербезпеки пропозиції та планування реагування на такий ризик?

ID.RA-07 [04] Чи проводиться періодичний перегляд ризиків кібербезпеки, прийнятих на основі запланованих майбутніх дій або етапів?

8.8. ID.RA-08 Визначити процеси отримання, аналізу та реагування на опубліковані повідомлення про виявлені вразливості

ID.RA-08 [01] Чи здійснюється обмін інформацією про вразливості між суб’єктом, постачальниками відповідно до правил і протоколів, визначених у контрактах?

ID.RA-08 [02] Чи встановлено обов’язки щодо перевірки виконання процедур обробки, аналізу впливу та реагування на загрози кібербезпеці, уразливості або розкриття кіберінцидентів постачальниками, клієнтами, партнерами та Держспецзв'язку, іншими уповноваженими державними організаціями з кібербезпеки?

8.9. ID.RA-09 Проводити перевірку автентичності і цілісності обладнання та програмного забезпечення перед його придбанням і використанням

ID.RA-09 [01] Чи проводиться оцінка автентичності та кібербезпеки критично важливих технологічних продуктів і послуг до їх придбання та використання?

8.10. ID.RA-10 Забезпечити проведення оцінювання постачальників перед придбанням у них критично важливих для суб'єкта товарів, робіт і послуг

ID.RA-10 [01] Чи здійснюється оцінювання постачальників товарів, робіт, послуг перед придбанням у них критично важливих для суб’єкта товарів, робіт і послуг?

9. Удосконалення (ID.IM)

9.1. ID.IM-01 Визначити напрями удосконалення за результатами проведеного оцінювання стану кіберзахисту

ID.IM-01 [01] Чи проведено самооцінку критично важливих служб, враховуючи поточні загрози та відомі техніки, тактики та процедури?

ID.IM-01 [02] Чи проведено зовнішнє оцінювання/незалежний аудит ефективності програми кібербезпеки суб’єкта, за результатами якого визначено сфери, що потребують покращення?

ID.IM-01 [03] Чи проводиться оцінювання відповідності суб’єкта встановленим для нього/обраних ним вимог з кібербезпеки за допомогою автоматизованих засобів?

9.2. ID.IM-02 Визначити напрями удосконалення за результатами тестування безпеки та навчальних вправ, включаючи їх виконання у взаємодії з постачальниками товарів, робіт, послуг та відповідними третіми сторонами

ID.IM-02 [01] Чи визначено за результатами аналізу процедур реагування на кіберінциденти, кібератаки або кіберзагрози (у тому числі ТТХ, симуляцій, тестувань, внутрішніх оглядів та незалежного аудиту), які з них і як потребують удосконалення для покращення реагування на кіберінциденти, кібератаки або кіберзагрози у майбутньому?

ID.IM-02 [02] Чи визначаються покращення для майбутніх заходів із забезпечення безперервної діяльності суб’єкта, аварійного відновлення та реагування на кіберінциденти, кібератаки або кіберзагрози на основі навчань, проведених у координації з постачальниками критично важливих послуг та продуктів?

ID.IM-02 [03] Чи залучаються керівництво суб’єкта та його внутрішні заінтересовані сторони (юридичний відділ, відділ кадрів тощо) за потреби до перевірок безпеки та навчань (вправ)?

ID.IM-02 [04] Чи затверджено керівництвом суб’єкта проведення тестування на проникнення у найбільш критичні системи суб’єкта?

ID.IM-02 [05] Чи упроваджено план дій у надзвичайних ситуаціях для реагування та відновлення після виявлення того, що продукти або послуги не походять від постачальника або партнера, з яким укладено контракт, або були змінені до їх отримання?

ID.IM-02 [06] Чи проведено збір та аналіз показників ефективності за допомогою інструментів та сервісів безпеки з метою підвищення ефективності програми кібербезпеки?

9.3. ID.IM-03 Визначати покращення з управління ризиками кібербезпеки під час виконання операційних процесів, процедур і дій

ID.IM-03 [01] Чи проводиться спільне з постачальниками вивчення отриманого досвіду з минулих кіберінцидентів та управління вразливостями?

ID.IM-03 [02] Чи щороку проводиться перегляд політики, процесів та процедур виконання заходів кіберзахисту, які у разі потреби враховують отриманий досвід?

ID.IM-03 [03] Чи визначені та періодично застосовуються показники оцінки ефективності процесів та процедур виконання заходів кіберзахисту?

9.4. ID.IM-04 Розробити, затвердити, довести до відома співробітників, переглядати та удосконалювати план реагування на кіберінциденти, кібератаки або кіберзагрози відповідно до Національного плану реагування на кіберінциденти, кібератаки та кіберзагрози, затвердженого постановою Кабінету Міністрів України від 26 листопада 2025 року № 1533, внутрішні політики кібербезпеки, план кіберзахисту та інші регламентуючі документи, які впливають на діяльність суб’єкта

ID.IM-04 [01] Чи розроблено плани дій у надзвичайних ситуаціях (наприклад, плани реагування на кіберінциденти, кібератаки або кіберзагрози, безперервності діяльності суб’єкта, відновлення після катастроф) для реагування та відновлення після несприятливих подій, які можуть перешкоджати діяльності, викривати конфіденційну інформацію або іншим чином загрожувати місії та функціонуванню суб’єкта?

ID.IM-04 [02] Чи внесено до плану реагування на кіберінциденти, кібератаки або кіберзагрози інформацію щодо контактних осіб та комунікаційних схем, процесів обробки загальних сценаріїв, а також критеріїв для визначення пріоритетів, ескалації та підвищення рівня щодо усіх планів дій у надзвичайних ситуаціях?

ID.IM-04 [03] Чи створено плани управління вразливостями для визначення та оцінювання всіх типів вразливостей для їх пріоритезації, тестування та внесення до плану реагування на ризики кібербезпеки?

ID.IM-04 [04] Чи доведені до відома відповідальних за їх виконання посадових осіб та заінтересованих сторін плани кіберзахисту з урахуванням управління ризиками кібербезпеки (включаючи внесені до них зміни)?

ID.IM-04 [05] Чи затверджують, щороку переглядають та за потреби (зокрема у разі зміни рівня ризику кібербезпеки) оновлюють суб’єкти план кіберзахисту?

10. Управління ідентифікацією, автентифікація та контроль доступу (PR.AA)

10.1. PR.AA-01 Забезпечити на рівні суб'єкта керування обліковими даними для авторизованих користувачів, служб і апаратного забезпечення

PR.AA-01 [01] Чи створена ініціація запитів на отримання або на розширення існуючих прав доступу для співробітників, підрядників та інших осіб, чи вона відстежується, переглядається та надається за потреби і погодженням з власниками системи або даних?

PR.AA-01 [02] Чи видаються, управляються та відкликаються криптографічні сертифікати та ідентифікаційні токени, криптографічні ключі (тобто управління ключами) та інші облікові дані?

PR.AA-01 [03] Чи унікальний ідентифікатор для кожного пристрою обирається з незмінних характеристик апаратного забезпечення або з наданого у захищений спосіб ідентифікатора пристрою?

PR.AA-01 [04] Чи забезпечується фізичне маркування авторизованого обладнання ідентифікатором для цілей інвентаризації та обслуговування?

10.2. PR.AA-02 Забезпечити підтвердження ідентичності користувачів та їх відповідність обліковим записам на основі умов взаємодії

PR.AA-02 [01] Чи визначено суб'єкт, чи проводяться реєстрація та перевірка особи на підставі офіційних документів, що її засвідчують (паспорт, водійські права тощо)?

PR.AA-02 [02] Чи проводиться суб'єктом перевірка унікальності облікових даних для кожної особи і використання облікових даних однієї особи іншими не допускається?

10.3. PR.AA-03 Забезпечити автентифікацію користувачів, служб та апаратного забезпечення

PR.AA-03 [01] Чи впроваджена суб'єктом та використовується багатофакторна автентифікація?

PR.AA-03 [02] Чи передбачено суб'єктом обмеження на мінімальну довжину паролів, PIN-кодів і подібних автентифікаторів?

PR.AA-03 [03] Чи проводиться суб'єктом періодична повторна автентифікація користувачів, служб і апаратного забезпечення на основі ризику кібербезпеки (наприклад, в архітектурах нульової довіри)?

PR.AA-03 [04] Чи підтверджується суб'єктом, що уповноважені співробітники мають можливість доступу до облікових даних під час надзвичайних ситуацій?

10.4. PR.AA-04 Забезпечити перевіряння, захист та передавання інформації про запити на ідентифікацію

PR.AA-04 [01] Чи підтверджена надійність ідентифікації тим, що передача даних автентифікації та інформації користувача проводиться через системи єдиного входу або між державними системами?

PR.AA-04 [02] Чи упроваджено підходи на основі стандартів надійної ідентифікації в усіх контекстах, чи дотримуються усі інструкції щодо створення (наприклад, моделі даних, метаданих), захисту (наприклад, цифровий підпис, шифрування) та перевірки (наприклад, підтвердження підпису) надійності ідентифікації?

10.5. PR.AA-05 Визначити в політиці, дотримуючись принципів найменших привілеїв і розподілу обов'язків, дозволи доступу, повноваження та авторизації, керувати ними, застосовувати та переглядати

PR.AA-05 [01] Чи проводиться перегляд привілеїв логічного та фізичного доступу періодично та щоразу, коли змінюється роль або відбувається звільнення співробітника, або привілеї, які більше не потрібні, скасовуються?

PR.AA-05 [02] Чи враховуються атрибути запитувача для прийняття рішення щодо надання доступу до запитуваного ресурсу (наприклад, геолокація, день/час, стан захищеності обладнання, з якого здійснюється доступ (кінцева точки))?

PR.AA-05 [03] Чи зменшені до необхідного мінімуму доступ і привілеї (наприклад, архітектура нульової довіри)?

PR.AA-05 [04] Чи проводиться періодичний перегляд привілеїв, пов'язаних з критично важливими функціями діяльності суб'єкта, щоб підтвердити належний розподіл обов'язків?

10.6. PR.AA-06 Здійснювати управління та моніторинг фізичного доступу до активів відповідно до ризику кібербезпеки

PR.AA-06 [01] Чи залучено суб'єктом співробітників охорони, застосовуються камери спостереження, замки на вході, системи сигналізації та інші технічні засоби контролю перебування та обмеження доступу?

PR.AA-06 [02] Чи впроваджено суб'єктом додаткові заходи фізичної безпеки для просторів (приміщень), в яких розміщуються активи високого рівня критичності?

PR.AA-06 [03] Чи супроводжує суб'єкт відвідувачів у приміщеннях з активами, критичними для її функціонування?

11. Обізнаність і навчання з питань кіберзахисту (PR.AT)

11.1. PR.AT-01 Систематично проводити інструктажі та тренінги з кібергігієни, а також забезпечити обізнаність і навченість співробітників таким чином, що вони мали знання та навички для виконання основних завдань щодо ризиків кібербезпеки

PR.AT-01 [01] Чи проводяться навчання та тренінги для працівників, підрядників, партнерів, постачальників та інших визначених користувачів непублічних ресурсів суб'єкта для їх обізнаності щодо базових принципів кібербезпеки?

PR.AT-01 [02] Чи запроваджено навчання щодо розпізнавання та протидії спробам застосування методів соціальної інженерії, поширеним атакам,

дотримання прийнятних політик безпеки, дотримання базових принципів кібергігієни (наприклад, виправлення програмного забезпечення, вибір паролів, захист облікових даних), а також інформування про атаки та підозрілу активність?

PR.AT-01 [03] Чи доводиться до відома співробітників суб'єкта інформація про наслідки порушення політики кібербезпеки як для окремих користувачів, так і для суб'єкта в цілому?

11.2. PR.AT-02 Забезпечити обізнаність та навченість співробітників, які безпосередньо виконують завдання із забезпечення кібербезпеки, кіберзахисту таким чином, що вони мали знання та навички для виконання встановлених завдань щодо ризиків кібербезпеки

PR.AT-02 [01] Чи визначено посади, які мають доступ до важливих даних суб'єкта, обіймання яких вимагає проходження додаткового навчання з питань кібербезпеки (співробітники із фізичної та кібербезпеки, фінансовий сектор, керівництво вищого рівня)?

PR.AT-02 [02] Чи проводяться тренінги, навчання та перевіряється рольова обізнаність щодо кібербезпеки для співробітників, які виконують спеціалізовані ролі, а також підрядників, партнерів, постачальників та інших третіх осіб?

PR.AT-02 [03] Чи запроваджено періодичне оцінювання користувачів щодо розуміння практик кібербезпеки відповідно до їхніх спеціалізованих ролей?

PR.AT-02 [04] Чи встановлено вимоги щодо щорічного підвищення кваліфікації для покращення існуючих та впровадження нових практик кібербезпеки?

12. Безпека даних (PR.DS)

12.1. PR.DS-01 Забезпечити конфіденційність, цілісність і доступність даних, що зберігаються в обладнанні систем суб'єкта

PR.DS-01 [01] Чи використовуються шифрування, цифрові підписи та криптографічні хеші для захисту конфіденційності та цілісності збережених даних у файлах, базах даних, образах дисків віртуальних машин, образах контейнерів та інших ресурсах?

PR.DS-01 [02] Чи використовується повне шифрування дисків для захисту даних, що зберігаються на кінцевих пристроях користувачів?

PR.DS-01 [03] Чи здійснюється підтвердження цілісності програмного забезпечення шляхом перевірки цифрових підписів?

PR.DS-01 [04] Чи обмежено використання знімних носіїв для запобігання витоку даних?

PR.DS-01 [05] Чи фізично захищені знімні носії, що містять незашифровану конфіденційну інформацію (наприклад, зберігаються у закритих сейфах або файлових шафах)?

12.2. PR.DS-02 Забезпечити конфіденційність, цілісність і доступність даних, що передаються

PR.DS-02 [01] Чи застосувано шифрування, цифрові підписи та криптографічні хеші для захисту конфіденційності та цілісності при використанні мережевих комунікацій?

PR.DS-02 [02] Чи здійснюється автоматичне шифрування або блокування вихідних електронних листів та інших комунікацій, що містять чутливі дані, залежно від класифікації таких даних?

PR.DS-02 [03] Чи заблокувано доступ до особистої електронної пошти, сервісів обміну файлами, зберігання файлів та інших особистих додатків і сервісів комунікації з організаційних систем і мереж?

PR.DS-02 [04] Чи забезпечено запобігання повторному використанню чутливих даних з продуктивних середовищ (наприклад, записи клієнтів) у інженерних, тестових та інших непродуктивних середовищах?

12.3. PR.DS-10 Забезпечити конфіденційність, цілісність і доступність даних, що використовуються: до яких є доступ, які обробляються та регулярно оновлюються застосунками, користувачами або пристроями суб'єкта

PR.DS-10 [01] Чи здійснено видалення даних, які мають залишатися конфіденційними (наприклад, з процесорів та пам'яті), як тільки вони більше не потрібні?

PR.DS-10 [02] Чи забезпечено захист даних, що використовуються, від доступу інших користувачів та процесів тієї ж платформи?

12.4. PR.DS-11 Забезпечити створення, захист, підтримку та тестування резервних копій даних

PR.DS-11 [01] Чи безперервно здійснювати резервне копіювання критичних даних у наближеному до реального часі?

PR.DS-11 [02] Чи проводиться резервне копіювання інших даних за встановленими графіками?

PR.DS-11 [03] Чи тестування резервних копій та відновлення для всіх типів джерел даних здійснюються принаймні щороку?

PR.DS-11 [04] Чи безпечно зберігати визначені резервні копії офлайн та поза межами суб'єкта, щоб кіберінцидент або катастрофа не пошкодили їх?

PR.DS-11 [05] Чи зберігати резервні копії даних в різних місцях географічно та обмежити доступ до інформації про геолокацію місць зберігання?

13. Безпека платформ (PR.PS)

13.1. PR.PS-01 Встановити та застосовувати методи керування конфігурацією

PR.PS-01 [01] Чи встановлено, протестовано, розгорнуто та підтримуються захищені базові конфігурації, які забезпечують виконання політик кібербезпеки організації та надають лише необхідні можливості (тобто принцип максимально обмеженої функціональності)?

PR.PS-01 [02] Чи переглянуто всі налаштування конфігурацій за замовчуванням, які можуть потенційно вплинути на кібербезпеку при встановленні або оновленні програмного забезпечення?

PR.PS-01 [03] Чи проводиться моніторинг виконуваного програмного забезпечення на предмет виявлення його відхилень від схвалених базових конфігурацій?

13.2. PR.PS-02 Забезпечити належне обслуговування, заміну та видалення програмного забезпечення відповідно до ризику кібербезпеки

PR.PS-02 [01] Чи виконується поточне та екстрене виправлення вразливостей у встановлені терміни, зазначені в плані управління вразливостями?

PR.PS-02 [02] Чи здійснюється оновлення образів контейнерів та розгортання нових екземплярів контейнерів, щоб заміняти, а не оновлювати існуючі екземпляри?

PR.PS-02 [03] Чи здійснюється заміна програмного забезпечення та версії сервісів, що досягли кінця життєвого циклу, на підтримувані та обслуговувані версії?

PR.PS-02 [04] Чи видаляються несанкціоноване програмне забезпечення та сервіси, які становлять надмірні ризики кібербезпеки?

PR.PS-02 [05] Чи видаляються будь-які непотрібні компоненти програмного забезпечення (наприклад, утиліт операційної системи), які можуть бути використані зловмисниками?

PR.PS-02 [06] Чи затверджені та виконуються заходи планів підтримки та обслуговування програмного забезпечення і сервісів, що досягли кінця життєвого циклу?

13.3. PR.PS-03 Забезпечити обслуговування, заміну та видалення обладнання відповідно до ризику кібербезпеки

PR.PS-03 [01] Чи здійснюється заміна апаратного забезпечення, коли воно не має необхідних можливостей безпеки або не може підтримувати програмне забезпечення з необхідними можливостями безпеки?

PR.PS-03 [02] Чи затверджені та виконуються заходи планів підтримки та обслуговування апаратного забезпечення, що досягло кінця життєвого циклу?

PR.PS-03 [03] Чи здійснюється утилізація апаратного забезпечення безпечно, відповідально та з можливістю аудиту?

13.4. PR.PS-04 Створити записи журналів подій, які зроблені доступними для постійного моніторингу

PR.PS-04 [01] Чи налаштовані всі операційні системи, додатки та сервіси (включаючи хмарні ресурси) для генерації записів у журнали подій?

PR.PS-04 [02] Чи налаштовані генератори журналів для безпечного обміну їхніми журналами із системами та службами інфраструктури реєстрації суб’єкта?

PR.PS-04 [03] Чи налаштовані генератори записів журналів подій для запису даних, необхідних для архітектур з нульовою довірою?

13.5. PR.PS-05 Заборонити встановлення та виконання несанкціонованого програмного забезпечення

PR.PS-05 [01] Якщо цього вимагає ризик кібербезпеки, чи обмежено використання програмного забезпечення лише дозволеними продуктами, а використання неавторизованого програмного забезпечення заборонено?

PR.PS-05 [02] Чи перевірені джерело походження та цілісність нового програмного забезпечення перед його встановленням?

PR.PS-05 [03] Чи налаштовано платформи на використання лише затверджених служб DNS, які блокують доступ до відомих шкідливих доменів, та на встановлення лише програмного забезпечення, схваленого суб'єктом?

PR.PS-05 [04] Чи налаштовано платформи для інсталювання лише затвердженого суб'єктом програмного забезпечення?

13.6. PR.PS-06 Інтегрувати практики безпечної розробки програмного забезпечення та контролювати їх виконання протягом життєвого циклу розробленого програмного забезпечення

PR.PS-06 [01] Чи усі компоненти програмного забезпечення, розробленого суб'єктом, захищені від втручання та несанкціонованого доступу?

PR.PS-06 [02] Чи усе програмне забезпечення, розроблене суб'єктом, перевірене на відсутність вразливостей у його оновленнях?

PR.PS-06 [03] Чи обслуговується і безпечно утилізується програмне забезпечення, що використовується у виробничих середовищах, коли воно більше не потрібне?

14. Стійкість технологічної інфраструктури (PR.IR)

14.1. PR.IR-01 Забезпечити захист мережі та середовища від неавторизованого логічного доступу та використання

PR.IR-01 [01] Чи логічно сегментовані мережі суб'єкта та хмарні платформи відповідно до меж довіри та типів платформ (наприклад, IT, IoT, OT, мобільні, гості) і чи необхідні комунікації дозволені лише між сегментами?

PR.IR-01 [02] Чи логічно сегментовані мережі суб'єкта від зовнішніх мереж і дозволені лише необхідні комунікації для входу в мережі суб'єкта із зовнішніх мереж?

PR.IR-01 [03] Чи упроваджено архітектуру нульової довіри для забезпечення принципу мінімальних привілеїв під час доступу до ресурсів системи?

PR.IR-01 [04] Чи перевірено кібербезпеку кінцевих точок перед тим, як їм надано доступ, і використання виробничих ресурсів?

14.2. PR.IR-02 Забезпечити захист технологічних активів від загроз навколишнього середовища

PR.IR-02 [01] Чи забезпечується захист обладнання суб’єкта від відомих екологічних загроз, таких як затоплення, пожежа, вітер, надмірна спека та вологість?

PR.IR-02 [02] Чи забезпечується захист від екологічних загроз та чи включено положення про належну операційну інфраструктуру до вимог до постачальників послуг, які експлуатують системи від імені суб’єкта?

14.3. PR.IR-03 Реалізувати механізми для досягнення вимог стійкості в нормальних і несприятливих ситуаціях

PR.IR-03 [01] Чи проводиться запобігання використанню єдиних точок відмови в системах та інфраструктурі?

PR.IR-03 [02] Чи проводиться балансування навантаження для збільшення потужності та підвищення надійності?

PR.IR-03 [03] Чи використовуються компоненти з високою доступністю, такі як резервне зберігання та джерела живлення, для підвищення надійності системи?

14.4. PR.IR-04 Забезпечити управління пропорційністю та адекватністю застосування ресурсів для їх доступності

PR.IR-04 [01] Чи проводиться моніторинг використання пристроїв зберігання даних, живлення, обчислювальних ресурсів, пропускної здатності мережі та інших ресурсів?

PR.IR-04 [02] Чи упроваджено прогнозування майбутніх потреб і відповідне масштабування ресурсів?

15. Безперервний моніторинг (DE.CM)

15.1. DE.CM-01 Проводити постійний моніторинг мереж і мережевих служб для виявлення потенційно несприятливих подій

DE.CM-01 [01] Чи забезпечено відстеження DNS, BGP та інших мережевих служб на наявність небажаних подій?

DE.CM-01 [02] Чи забезпечено відстеження дротових та бездротових мереж на наявність підключень із неавторизованих кінцевих точок?

DE.CM-01 [03] Чи забезпечено моніторинг засобів на наявність несанкціонованих або шахрайських бездротових мереж?

DE.CM-01 [04] Чи проведено порівняльний аналіз фактичних мережевих потоків з базовими лініями, щоб виявити відхилення?

DE.CM-01 [05] Чи проведено моніторинг мережевих комунікацій для виявлення змін у положеннях безпеки з метою нульової довіри?

15.2. DE.CM-02 Проводити постійний моніторинг фізичного середовища для виявлення потенційно несприятливих подій

DE.CM-02 [01] Чи відстежуються журнали подій систем контролю фізичного доступу (наприклад, зчитувачів бейджів), щоб знайти незвичайні шаблони доступу (наприклад, відхилення від норми) і невдалі спроби доступу?

DE.CM-02 [02] Чи переглянуто та відстежено записи фізичного доступу (наприклад, з реєстрації відвідувачів, аркушів входу)?

DE.CM-02 [03] Чи забезпечено контроль засобів контролю фізичного доступу (наприклад, замки, засувки, петлі, сигналізацію) на наявність ознак втручання?

DE.CM-02 [04] Чи забезпечено контроль фізичного середовища за допомогою систем сигналізації, камер і охоронців?

15.3. DE.CM-03 Проводити постійний моніторинг діяльності співробітників і використання ними технологій для виявлення потенційно несприятливих подій

DE.CM-03 [01] Чи забезпечено використання програмного забезпечення для аналітики поведінки з метою виявлення аномальної активності користувачів, щоб пом’якшити внутрішні загрози?

DE.CM-03 [02] Чи забезпечено відстеження журналів логічних систем контролю доступу, щоб знайти незвичайні шаблони доступу та невдалі спроби доступу?

DE.CM-03 [03] Чи забезпечено відстеження на постійній основі технології обману, включаючи облікові записи користувачів, для будь-якого використання?

15.4. DE.CM-06 Проводити постійний моніторинг діяльності і послуг зовнішнього постачальника товарів, робіт, послуг для виявлення потенційно несприятливих подій

DE.CM-06 [01] Чи забезпечено відстеження віддаленого та локального адміністрування й технічного обслуговування, які зовнішні постачальники виконують у системах суб’єкта?

DE.CM-06 [02] Чи забезпечено моніторинг активності надавачів хмарних послуг, постачальників послуг Інтернету та інших постачальників послуг на наявність відхилень від очікуваної поведінки?

15.5. DE.CM-09 Проводити постійний моніторинг використання комп’ютерного обладнання та програмного забезпечення, середовища їх виконання та даних для виявлення потенційно несприятливих подій

DE.CM-09 [01] Чи забезпечено моніторинг електронної пошти, Інтернету, обміну файлами, служб спільної роботи та інших поширених векторів атак для виявлення зловмисного програмного забезпечення, фішингу, витоку та крадіжки даних та інших небажаних подій?

DE.CM-09 [02] Чи забезпечено відстеження спроби автентифікації, щоб виявити атаки на облікові дані та неавторизоване повторне використання облікових даних?

DE.CM-09 [03] Чи забезпечено відстеження конфігурації програмного забезпечення на наявність відхилень від базових рівнів безпеки?

DE.CM-09 [04] Чи забезпечено контроль апаратного та програмного забезпечення на наявність ознак втручання?

DE.CM-09 [05] Чи забезпечено використання технологій з присутністю на кінцевих точках для виявлення проблем забезпечення кібербезпеки (наприклад,

немає патчів, зараження зловмисним програмним забезпеченням, несанкціоноване програмне забезпечення) з метою перенаправлення кінцевих точок в середовище відновлення до того, як буде авторизовано доступ?

16. Аналіз несприятливих подій (DE.AE)

16.1. DE.AE-02 Впровадити періодичне проведення аналізу потенційно несприятливих подій для кращого розуміння пов'язаних подій

DE.AE-02 [01] Чи впроваджено систему управління інформацією та подіями безпеки (SIEM) або інші інструменти для постійного моніторингу подій у журналі на наявність відомої зловмисної та підозрілої активності?

DE.AE-02 [02] Чи використовується актуальна інформація про кіберзагрози в інструментах аналізу журналів, щоб підвищити точність виявлення та охарактеризувати суб'єкти загрози, їхні методи та показники компрометації?

DE.AE-02 [03] Чи забезпечено регулярне проведення (вручну) перевірки подій журналу для технологій, які не можна належним чином контролювати за допомогою автоматизації?

DE.AE-02 [04] Чи використано інструменти аналізу журналів для створення звітів про свої висновки?

16.2. DE.AE-03 Впровадити періодичне проведення пошуку та зіставлення інформації з кількох джерел

DE.AE-03 [01] Чи забезпечено постійне передавання даних журналу, створених з інших джерел, на відносно невелику кількість серверів журналів?

DE.AE-03 [02] Чи використано технологію кореляції подій (наприклад, SIEM) для збору інформації, отриманої з кількох джерел?

DE.AE-03 [03] Чи використано дані про кіберзагрози, щоб допомогти корелювати події між різними джерелами журналів аудиту та подій?

16.3. DE.AE-04 Забезпечити усвідомлення очікуваного впливу і масштабу несприятливих подій

DE.AE-04 [01] Чи упроваджено SIEM або інші інструменти для оцінки впливу та масштабу, а також чи переглянуто й уточнено оцінки?

DE.AE-04 [02] Чи створено власні оцінки впливу та масштабу?

16.4. DE.AE-06 Забезпечити передавання інформації про несприятливі події до уповноважених суб'єктів для використання відповідного інструментарію

DE.AE-06 [01] Чи використано програмне забезпечення для кібербезпеки, щоб створювати сповіщення та передавати їх до центру безпеки (SOC), служб реагування на кіберінциденти, кібератаки або кіберзагрози, та інструменти реагування?

DE.AE-06 [02] Чи забезпечено доступ служб реагування на кіберінциденти, кібератаки або кіберзагрози та інших уповноважених співробітників до результатів аналізу журналу в будь-який час?

DE.AE-06 [03] Чи забезпечено автоматичне створення та призначення сигналів у системі оповіщення, коли виникають певні типи несприятливих подій?

DE.AE-06 [04] Чи забезпечено ручне створення та призначення сигналів у системі оповіщення суб'єкта, коли технічний співробітник виявляє ознаки компрометації?

16.5. DE.AE-07 Забезпечити збирання, виявлення та аналіз інформації про кіберзагрози та іншої контекстної інформації

DE.AE-07 [01] Чи забезпечено безпечне розповсюдження даних про кіберзагрози, їх інтеграцію в засоби виявлення та доведення до відома персоналу?

DE.AE-07 [02] Чи забезпечено безпечне надання інформації від інвентаризації активів до технологій виявлення процесів і співробітників?

DE.AE-07 [03] Чи забезпечено швидке отримання та швидкий аналіз інформації про вразливості технологічної інфраструктури від постачальників, третіх сторін і сторонніх консультантів із безпеки?

16.6. DE.AE-08 Запровадити належну ідентифікацію кіберінцидентів та кібератак за визначними характеристиками

DE.AE-08 [01] Чи застосовано критерії кіберінциденту до відомих і припущених характеристик діяльності, щоб визначити, чи слід оголошувати кіберінцидент?

DE.AE-08 [02] Чи враховано відомі помилкові спрацьовування під час застосування критеріїв кіберінциденту?

17. Управління кіберінцидентами (RS.MA)

17.1. RS.MA-01 Запровадити виконання плану реагування на кіберінциденти, кібератаки або кіберзагрози в координації з відповідними третіми сторонами одразу після оголошення кіберінциденту

RS.MA-01 [01] Чи забезпечено автоматичне виявлення кіберінцидентів?

RS.MA-01 [02] Чи залучено допомогу з реагування на кіберінциденти, кібератаки або кіберзагрози на основі аутсорсингу?

RS.MA-01 [03] Чи призначено керівника з реагування на кожний кіберінцидент?

RS.MA-01 [04] Чи ініційовано виконання додаткових планів кібербезпеки, якщо це необхідно для підтримки реагування на кіберінциденти, кібератаки або кіберзагрози (наприклад, забезпечення безперервного функціонування та аварійне відновлення)?

17.2. RS.MA-02 Упровадити сортування звітів про кіберінциденти після їх підтвердження

RS.MA-02 [01] Чи переглянуто звіти про кіберінциденти, підтверджено те, що вони пов'язані з кібербезпекою та вимагають заходів з реагування на кіберінциденти, кібератаки або кіберзагрози?

RS.MA-02 [02] Чи застосовано критерії для оцінки кіберінциденту?

17.3. RS.MA-03 Упровадити таксономію та пріоритезацію кіберінцидентів

RS.MA-03 [01] Чи проведено аналіз і класифікацію кіберінцидентів на основі їх таксономії (наприклад, порушення даних, програми-вимагачі, DDoS, компрометація облікового запису)?

RS.MA-03 [02] Чи визначено пріоритетність кіберінцидентів на основі їх масштабу, ймовірного впливу та критичного часу?

RS.MA-03 [03] Чи вибрано стратегію реагування на кіберінциденти, кібератаки або кіберзагрози для активних кіберінцидентів, збалансовано необхідність швидкого відновлення після кіберінциденту з необхідністю спостерігати за зловмисником або проводити більш ретельне розслідування?

17.4. RS.MA-04 Упровадити інформування та підвищення рівнів критичності кіберінцидентів (за потреби)

RS.MA-04 [01] Чи відстежено та перевірено статус усіх поточних кіберінцидентів?

RS.MA-04 [02] Чи забезпечено координацію підвищення рівня критичності кіберінциденту та його ескалацію з визначеними внутрішніми та зовнішніми заінтересованими сторонами?

17.5. RS.MA-05 Упровадити застосування критеріїв для ініціювання відновлення після кіберінциденту

RS.MA-05 [01] Чи застосовано критерії відновлення кіберінциденту до відомих і передбачуваних характеристик кіберінциденту, щоб визначити, чи слід ініціювати процеси відновлення кіберінциденту?

RS.MA-05 [02] Чи враховано можливий збій при виконанні заходів з відновлення кіберінциденту?

18. Аналіз кіберінциденту (RS.AN)

18.1. RS.AN-03 Запровадити проведення аналізу для встановлення того, що відбулося під час кіберінциденту та які джерела виникнення кіберінциденту

RS.AN-03 [01] Чи визначено послідовність подій, що відбулися під час кіберінциденту, і які активи та ресурси були залучені до кожної події

RS.AN-03 [02] Чи проаналізовано вразливості, загрози та суб’єкти загрози, які прямо чи опосередковано залучені до кіберінциденту?

RS.AN-03 [03] Чи проаналізовано кіберінцидент, щоб знайти основні системні причини?

RS.AN-03 [04] Чи перевірено будь-яку технологію шахрайства у кіберпросторі, щоб отримати додаткову інформацію про поведінку зловмисників?

18.2. RS.AN-06 Запровадити запис дій, які виконуються під час розслідування кіберінциденту, та забезпечити цілісність і збереження таких записів

RS.AN-06 [01] Чи забезпечено запис та неможливість перезапису дій кожного спеціаліста з реагування на кіберінциденти, кібератаки або кіберзагрози та інших осіб (наприклад, системних адміністраторів, інженерів з кібербезпеки), які виконують завдання з реагування на кіберінциденти?

RS.AN-06 [02] Чи забезпечено наявність особи, яка веде розслідування виникнення кіберінциденту, документує деталі кіберінциденту і несе відповідальність за збереження цілісності документації та джерел усієї інформації, яка задокументована?

18.3. RS.AN-07 Запровадити здійснення збору та забезпечити цілісність та збереження даних про кіберінциденти та метаданих

RS.AN-07 [01] Чи забезпечено збирання, зберігання та захист цілісності усіх відповідних даних про інциденти та метаданих (наприклад, джерело даних, дата/час збору) на основі процедур поводження та зберігання доказів?

18.4. RS.AN-08 Запровадити оцінювання масштабу кіберінциденту або кібератаки та документально його підтверджувати

RS.AN-08 [01] Чи переглянуто інші потенційні цілі кіберінциденту, щоб знайти індикатори компрометації та докази в наполегливості?

RS.AN-08 [02] Чи можна автоматично запускати інструменти на цільових об'єктах для пошуку індикаторів компрометації та доказів стійкості?

19. Звітування про реагування на кіберінциденти, кібератаки, кіберзагрози та комунікація (RS.CO)

19.1. RS.CO-02 Запровадити сповіщення внутрішніх та зовнішніх заінтересованих сторін про кіберінциденти, кібератаки та кіберзагрози

RS.CO-02 [01] Чи дотримано визначеної процедури оповіщення щодо порушення даних після виявлення кіберінциденту з порушенням даних, включаючи сповіщення постраждалих клієнтів?

RS.CO-02 [02] Чи повідомлено ділових партнерів і клієнтів про кіберінциденти відповідно до вимог контракту?

RS.CO-02 [03] Чи повідомлено правоохоронні органи та уповноважені органи про кіберінциденти на основі затверджених критеріїв плану реагування на кіберінциденти, кібератаки або кіберзагрози?

19.2. RS.CO-03 Запровадити надання інформації визначеним внутрішнім і зовнішнім заінтересованим сторонам

RS.CO-03 [01] Чи забезпечено безпечний обмін інформацією відповідно до планів на кіберінциденти, кібератаки та кіберзагрози та договорів про обмін інформацією?

RS.CO-03 [02] Чи добровільно поширено інформацію з видаленням усіх конфіденційних даних серед центрів обміну та аналізу інформації про спостережувані TTP зловмисників?

RS.CO-03 [03] Чи сповіщено відділ кадрів про випадки зловмисної внутрішньої діяльності?

RS.CO-03 [04] Чи забезпечено регулярне інформування керівництва вищого рівня про статус великих кіберінцидентів?

RS.CO-03 [05] Чи забезпечено координацію методів комунікації в кризових ситуаціях між суб'єктом та його критично важливими постачальниками?

RS.CO-03 [06] Чи забезпечено дотримання правил і протоколів, визначених у контрактах, щодо обміну інформацією про кіберінциденти між суб'єктом та його постачальниками?

20. Пом'якшення кіберінциденту (RS.MI)

20.1. RS.MI-01 Забезпечити локалізацію кіберінцидентів

RS.MI-01 [01] Чи забезпечено автоматичне виконання дій стримування за допомогою технологічних рішень (наприклад, антивірусне програмне забезпечення) та інших технологій (наприклад, операційні системи, пристрої мережевої інфраструктури), які мають функції забезпечення кібербезпеки?

RS.MI-01 [02] Чи надано дозвіл службам реагування на кіберінциденти, кібератаки або кіберзагрози вручну вибирати та виконувати дії стримування?

RS.MI-01 [03] Чи надано дозвіл третій стороні (наприклад, постачальнику послуг Інтернету, постачальнику послуг управління безпекою) виконувати дії зі стримування від імені суб'єкта?

RS.MI-01 [04] Чи забезпечено автоматичне перенесення скомпрометованих кінцевих точок у віртуальну локальну мережу (VLAN) для відновлення?

20.2. RS.MI-02 Забезпечити ліквідацію кіберінцидентів

RS.MI-02 [01] Чи забезпечено автоматичне виконання завдань стримування за допомогою впроваджених технологій кіберзахисту та інших технологій, які мають такі функції (наприклад, операційні системи, мережа пристроїв інфраструктури)?

RS.MI-02 [02] Чи надано дозвіл службам реагування на кіберінциденти, кібератаки або кіберзагрози вручну вибирати та виконувати дії зі стримування кіберінциденту?

RS.MI-02 [03] Чи надано дозвіл третій стороні (наприклад, постачальнику послуг управління безпекою) виконувати дії зі стримування від імені суб'єкта?

21. Виконання плану відновлення після кіберінциденту (RC.RP)

21.1. RC.RP-01 Забезпечити виконання передбачених планом реагування на кіберінциденти, кібератаки або кіберзагрози заходів щодо відновлення одразу після їх ініціалізації в ході реагування на кіберінциденти, кібератаки та кіберзагрози

RC.RP-01 [01] Чи розпочато процедури відновлення під час або після процесів реагування на кіберінциденти, кібератаки або кіберзагрози?

RC.RP-01 [02] Чи ознайомлено всіх осіб, які відповідають за відновлення, про плани відновлення та повноваження, необхідні для виконання кожного аспекту планів?

21.2. RC.RP-02 Забезпечити відбір, визначення обсягу, пріоритетність та виконання заходів з відновлення

RC.RP-02 [01] Чи обрано дії з відновлення на основі критеріїв, визначених у плані реагування на кіберінциденти, кібератаки та кіберзагрози, і доступних ресурсів?

RC.RP-02 [02] Чи змінено обрані дії з відновлення на основі переоцінки потреб суб'єкта і ресурсів?

21.3. RC.RP-03 Переконатися у цілісності резервних копій та інших ресурсів, які підлягають відновленню, перед їх використанням для відновлення

RC.RP-03 [01] Чи перевірено відновлені активи на наявність ознак компрометації, пошкодження файлів та інших питань цілісності активів перед їх використанням?

21.4. RC.RP-04 Переглянути критичні для місії суб'єкта функції для встановлення операційних норм після кіберінцидентів і кібератак

RC.RP-04 [01] Чи використано записи про вплив на суб'єкт і категоризацію системи (включно з цілями надання послуг), щоб підтвердити, що основні послуги відновлюються у відповідному порядку?

RC.RP-04 [02] Чи забезпечено співпрацю з власниками систем, щоб підтвердити успішне відновлення систем і повернення до штатного режиму функціонування?

RC.RP-04 [03] Чи відстежено продуктивність відновлених систем, щоб перевірити адекватність відновлення?

21.5. RC.RP-05 Переконатися в цілісності відновлених активів, відновленні систем та служб і підтвердити їх робочий стан

RC.RP-05 [01] Чи перевірено відновлені активи на наявність індикаторів компрометації та усунення основних причин кіберінциденту перед їх штатним використанням?

RC.RP-05 [02] Чи перевірено правильність і адекватність дій з відновлення, вжитих перед запуском відновленої системи в режимі онлайн?

21.6. RC.RP-06 Задекларувати завершення відновлення після кіберінциденту, кібератаки і підтвердження критеріїв та пов'язаної з кіберінцидентом документації

RC.RP-06 [01] Чи підготовлено звіт про завершення дії, в якому задокументовано сам кіберінцидент, вжиті заходи реагування та відновлення, а також отриманий досвід?

RC.RP-06 [02] Чи оголошено про закінчення відновлення після кіберінциденту та досягнення відповідних критеріїв?

22. Комунікація з відновлення після кіберінциденту (RC.CO)

22.1. RC.CO-03 Забезпечити інформування визначених внутрішніх і зовнішніх заінтересованих сторін про заходи з відновлення та прогрес у відновленні операційних спроможностей

RC.CO-03 [01] Чи забезпечено безпечний обмін інформацією про відновлення, включаючи хід відновлення, відповідно до планів реагування на кіберінциденти, кібератаки та кіберзагрози та договорів про обмін інформацією?

RC.CO-03 [02] Чи забезпечено регулярне інформування керівництва вищого рівня про стан відновлення та хід відновлення для великих кіберінцидентів?

RC.CO-03 [03] Чи дотримано вимоги правил і протоколів, визначених у контрактах між суб'єктом та його постачальниками, щодо обміну інформацією про кіберінциденти?

RC.CO-03 [04] Чи скоординовано кризову комунікацію між суб'єктом та його критично важливими постачальниками?

22.2. RC.CO-04 Запровадити інформування суспільства про відновлення після кіберінциденту, кібератаки, використовуючи затверджені методи та повідомлення, відповідно до Порядку публічного інформування або звітування про реагування на кіберінциденти, кібератаки, усунення їх наслідків, затвердженого постановою Кабінету Міністрів України від 26 листопада 2025 року № 1533

RC.CO-04 [01] Чи дотримано процедури інформування про кіберінциденти, кібератаки та кіберзагрози?

RC.CO-04 [02] Чи здійснюється інформування про кіберінциденти, кібератаки та кіберзагрози безперервно в режимі, наближеному до реального часу, з використанням платформи обміну інформацією про кіберінциденти, кібератаки, кіберзагрози та механізму «єдиного вікна» для інформування, дотримання загальних правил обміну інформацією про кіберінциденти, кібератаки, кіберзагрози (протокол TLP)?

RC.CO-04 [03] Чи здійснюється публічне інформування щодо кіберінцидентів, кібератаки від середнього рівня критичності та вище?

RC.CO-04 [04] Чи описано кроки, які вживалися для відновлення після кіберінциденту та запобігання його повторенню?

_____