System wewnętrznego zgłaszania zdarzeń związanych z bezpieczeństwem informacji **(IS.I.OR.215 ; (IS.D.OR.215)**

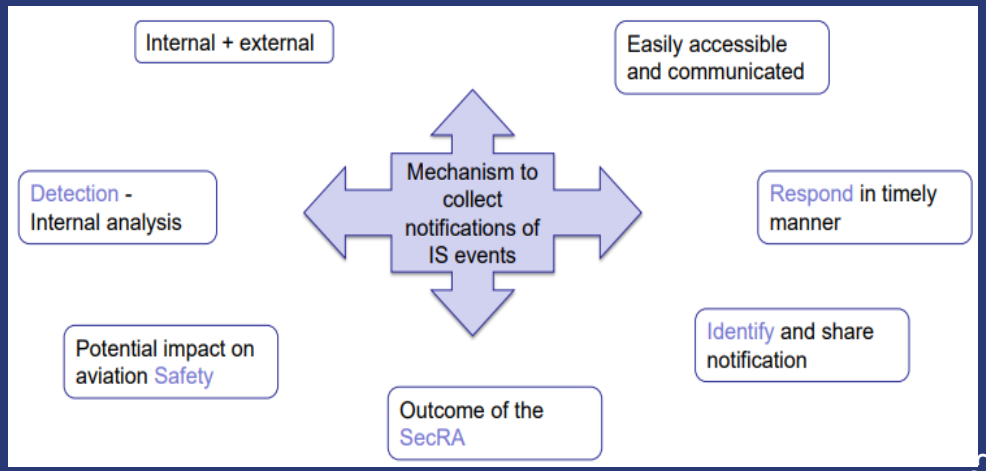
Urząd Lotnictwa Cywilnego

15.09.2025

Co mówi przepis IS.D.OR.215 / IS.I.OR.215

a) Organizacja ustanawia system wewnętrznego zgłaszania zdarzeń, aby móc gromadzić informacje o zdarzeniach związanych z bezpieczeństwem informacji, w tym o zdarzeniach zgłaszanych na podstawie pkt IS.I.OR.230, oraz oceniać takie zdarzenia.

AMC1 IS.I.OR.215 Główne elementy:
- Źródło incydentów zgodnie IS.I.OR.220 (A)
- Mechanizm gromadzenia powiadomień (wewnętrzny + zewnętrzny)
- Łatwo dostępny i zakomunikowany.
- Zidentyfikowani wszyscy wewnętrzni interesariusze



(Bardziej szczegółowo - **AMC1 IS.I.OR.215**)

Organizacje powinny wykorzystywać jako źródło incydenty wykryte podczas prowadzonych działań, aby wykazać zgodność z IS.I.OR.220(a).
Organizacje powinny posiadać mechanizm gromadzenia powiadomień o zdarzeniach od personelu i ze źródeł zewnętrznych, w tym dostawców, partnerów, klientów, oprogramowania open source i badaczy bezpieczeństwa informacji.
Mechanizm gromadzenia informacji przez personel i źródła zewnętrzne powinien być łatwo dostępny i zakomunikowany.

AMC1 IS.I.OR.215

Organizacje powinny wykorzystywać jako źródło incydenty wykryte podczas prowadzonych działań, aby wykazać zgodność z IS.I.OR.220(a).

Organizacja powinna gromadzić wszystkie zdarzenia zebrane za pomocą środków wykrywania do analizy wewnętrznej.
Każde zdarzenie powinno zostać przeanalizowane w celu ustalenia, czy podlega zgłoszeniu, a jeśli tak, to jaki będzie jego potencjalny lub rzeczywisty wpływ na bezpieczeństwo lotnicze.

Zdarzenia związane z bezpieczeństwem informacji należy rozpatrywać w połączeniu z innymi zdarzeniami, aby zapewnić korelację i zidentyfikować incydenty lub luki w zabezpieczeniach, które mogą mieć potencjalny wpływ na bezpieczeństwo lotnicze.
Organizacja powinna uwzględnić wynik oceny ryzyka oraz możliwość wykorzystania nowych luk w zabezpieczeniach wykrytych podczas działań detekcyjnych prowadzonych zgodnie ze środkami wymaganymi w IS.I.OR.220(a).

Organizacja powinna zidentyfikować wszystkich wewnętrznych interesariuszy, którzy wymagają powiadomienia o konkretnym incydencie lub luce w zabezpieczeniach, i zapewnić, że otrzymają oni wszystkie niezbędne informacje na temat incydentu lub luki w zabezpieczeniach, aby mogli działać skutecznie i terminowo, wspierając wymagane okresy wykrywania i reagowania.

GM1 IS.I.OR.215 (a) i (b)

ZWIĄZEK MIĘDZY ZGŁASZANIEM WEWNĘTRZNYM A ZEWNĘTRZNYM

- Organizacje powinny gromadzić i zgłaszać wewnętrznie incydenty i luki w zabezpieczeniach, mając na celu uwzględnienie wszystkich kwestii objętych zakresem niniejszego rozporządzenia.

- Zarówno zgłaszanie wewnętrzne, jak i zewnętrzne jest niezbędne dla kompletnego i skutecznego systemu zgłaszania.

- Zgłoszenia wewnętrzne powinny być oceniane terminowo, a w przypadku, gdy potencjalny wpływ na bezpieczeństwo jest stanem niebezpiecznym, organizacje powinny zainicjować zgłaszanie tych wewnętrznych zgłoszeń zgodnie z IS.I.OR.230.

(*IS.I.OR.230 Przykładowo: ocena w terminie – ocena potencjalnego wpływu na bezpieczeństwo – zgłoszenie zewnętrzne do właściwego organu , Organizacji Projektującej, posiadaczowi zatwierdzenia projektu*)

Co mówi przepis IS.D.OR.215 (b)/ IS.I.OR.215 (b)

b) Dzięki temu systemowi i procesowi, o którym mowa w pkt IS.I.OR.220, organizacja może:

- określić, które zdarzenia zgłoszone na podstawie lit. a) uznaje się za incydenty związane z bezpieczeństwem informacji lub podatność o potencjalnym wpływie na bezpieczeństwo lotnicze;

- określić przyczynę incydentów związanych z bezpieczeństwem informacji i podatności zidentyfikowanych zgodnie z pkt 1 oraz czynniki przyczyniające się do ich wystąpienia, a także uwzględnić je w procesie zarządzania ryzykiem związanym z bezpieczeństwem informacji zgodnie z pkt IS.I.OR.205 (ocena ryzyka) i IS.I.OR.220 (wykrywanie, reagowanie, działania naprawcze);

- zapewnić ocenę wszystkich znanych, istotnych informacji dotyczących incydentów związanych z bezpieczeństwem informacji i podatności zidentyfikowanych zgodnie z ppkt 1;

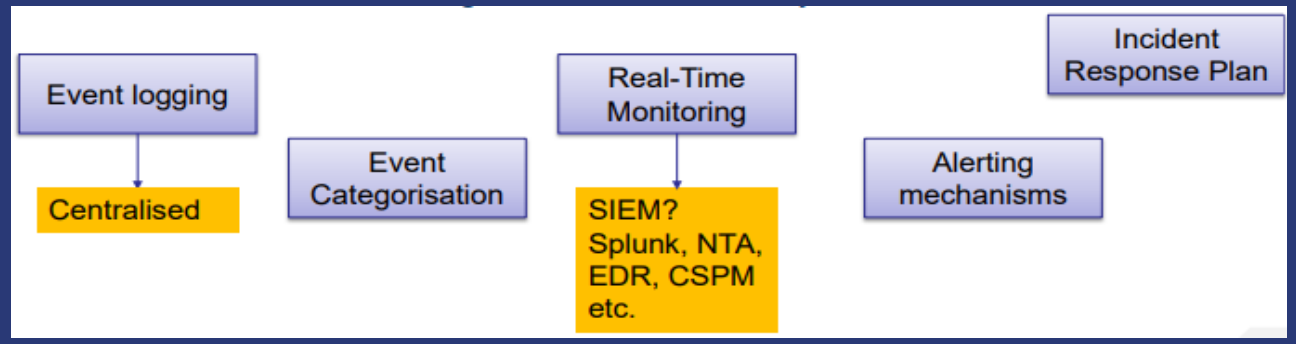
- w razie potrzeby zapewnić wdrożenie metody wewnętrznej dystrybucji informacji.

GM2 IS.I.OR.215(a) i (b)

Organizacja gromadzenia i oceny zdarzeń bezpieczeństwa informacji

GM2 IS.I.OR.215(a) i(b) Główne elementy:

- Centralizacja operacji bezpieczeństwa informacji w centrum operacji bezpieczeństwa (SOC)
- Wdrożenie systemu zarządzania informacjami i zdarzeniami bezpieczeństwa informacji (SIEM).
- Organizacje mogą zdecydować się na korzystanie z SOC dla zdarzeń istotnych dla Części IS w izolacji lub w połączeniu ze zdarzeniami niepodlegającymi Części IS (zdarzeniami związanymi z interesami biznesowymi).
- Zdarzenia mogą być automatycznie agregowane, korelowane i analizowane w celu wykrywania nietypowych zachowań prowadzących do incydentów bezpieczeństwa informacji

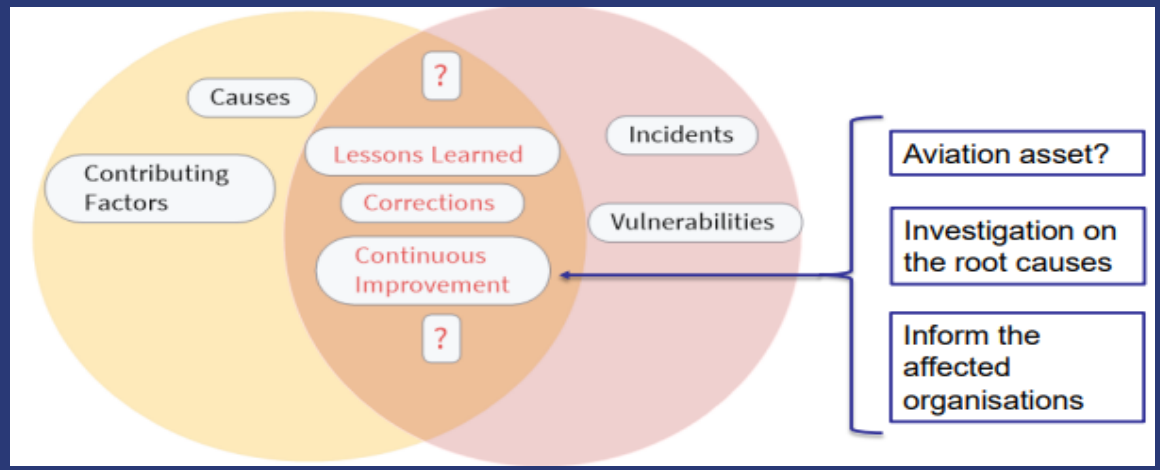


GM3 IS.I.OR.215(a) i (b)

ISTOTNE INFORMACJE DOTYCZĄCE INCYDENTÓW I PODATNOŚCI

Zrozumienie przyczyn i czynników przyczyniających się do incydentów bezpieczeństwa informacji oraz podatności istotnych dla Części IS pozwala na wyciągnięcie wniosków i wprowadzenie korekt do procesów i projektowania aktywów. Jednak zrozumienie przyczyn i czynników przyczyniających się nie zawsze jest możliwe lub może nie sprzyjać ciągłej poprawie bezpieczeństwa lotniczego.

W przypadku, gdy podatności wynikają z aktywów opracowanych wyłącznie lub głównie na potrzeby lotnictwa, oczekuje się, że możliwe będzie przeprowadzenie niezbędnego dochodzenia w celu ustalenia przyczyn źródłowych. Przyczyny te pozwolą dotkniętym organizacjom ulepszyć procesy i projektowanie aktywów w celu usunięcia podatności i zapewnienia, że takie podatności nie pojawią się w innych zasobach. Zrozumienie przyczyn źródłowych podatności pozwala również społeczności lotniczej uczyć się i tym samym unikać podobnych podatności w przyszłości.



Co mówi przepis IS.D.OR.215 / IS.I.OR.215

c) Każda organizacja przyjmująca zlecenia, która może narazić organizację na ryzyko związane z bezpieczeństwem informacji o potencjalnym wpływie na bezpieczeństwo lotnicze, jest zobowiązana do zgłaszania organizacji zdarzeń związanych z bezpieczeństwem informacji.
Takie zgłoszenia są dokonywane z użyciem procedur ustanowionych w drodze szczegółowych uzgodnień umownych oraz podlegają ocenie zgodnie z lit. b).

GM1 IS.I.OR.215(c)

Jeżeli organizacje, którym udzielono zlecenia, również podlegają niniejszemu rozporządzeniu, wymiana informacji i raportowanie powinny być objęte zarządzaniem wspólnym ryzykiem oraz poprzez zawarcie porozumienia zewnętrznego między organizacjami. Wskazówki dotyczące opracowywania porozumień zewnętrznych można znaleźć w dokumencie EUROCAE ED-201A, rozdział 4.4 Porozumienia zewnętrzne.

Ogólnie rzecz biorąc, i we wszystkich innych przypadkach, każda umowa o świadczenie usług powinna zawierać standardowe klauzule dotyczące zobowiązań organizacji, której udzielono zlecenia, do:

— zgłaszania w uzgodnionym terminie incydentów związanych z bezpieczeństwem informacji, które mogą mieć wpływ na organizację, która udzielono zlecenia. Incydenty i luki w zabezpieczeniach, które mogą prowadzić do niebezpiecznych warunków, powinny być zgłaszane jak najszybciej i w sposób zapewniający wypełnienie obowiązku zgłaszania zewnętrznego zgodnie z IS.I.OR.230;

GM1 IS.I.OR.215(c) - cd.

— wyznaczenia punktu kontaktowego do spraw zarządzania incydentami i ewentualnego zarządzania kryzysowego.

W niektórych przypadkach organizacje zlecające usługi, takie jak dostawcy usług z rozproszonymi zasobami, mogą nie być w stanie oferować raportów ad hoc. W takich przypadkach wymóg raportowania wewnętrznego może zostać spełniony za pomocą innych środków, które spełniają cel tego przepisu. Na przykład, organizacje zlecające usługi mogą dostarczyć aktualną listę luk w zabezpieczeniach wpływających na systemy w zakresie usług objętych umową. Lista ta powinna być monitorowana przez organizację zlecającą usługi w ramach wewnętrznego raportowania zdarzeń związanych z bezpieczeństwem informacji.

- Contractual Agreements
- Event Definition
- Communication Protocol
- Timeliness
- Event Details
- Severity Classification
- Feedback Mechanism
- Follow-Up

- Reporting Format:
- Training and Awareness:
- Escalation Procedures
- Documentation:
- Review and Improvement
- Regulatory Compliance:

Co mówi przepis IS.D.OR.215 (d) / IS.I.OR.215 (d)

d) Organizacja współpracuje w ramach badań z każdą inną organizacją, która w sposób istotny przyczynia się do bezpieczeństwa informacji dotyczącego działalności własnej.

GM1 IS.I.OR.215(d) Główne elementy**:**

- Udostępnianie elementów z rejestrów incydentów
- Zobowiązania umowne
- Formalne porozumienia (MoU)
- Spotkania
- Wspólne działania rozwojowe
- Udostępnianie wskaźników naruszeń (IoC) w czasie rzeczywistym
- Aktywny udział w ISAC
- Subskrypcja CERT w celu otrzymywania alertów o podatnościach i zagrożeniach

- Sharing elements from incident records
- Contractual obligations
- Formal agreements (MoU)
- Governance meetings
- Joint development activities
- Real-time indicators of compromise (IoC) sharing
- Active participation in ISAC(s)
- Subscription to CERTs to receive vulnerability and threat alerts

(Bardziej szczegółowo - **GM1 IS.I.OR.215(d)**)
Współpraca w ramach punktu IS.I.OR.215(d) może być uzasadniona poprzez udostępnianie elementów z rejestrów incydentów, które mogą wspierać działania innych organizacji w zakresie bezpieczeństwa informacji. W przypadku, gdy organizacje są związane zobowiązaniami umownymi, umowa ta może również zawierać zobowiązanie do współpracy.

GM1 IS.I.OR.215(d) cd.

(Bardziej szczegółowo - **GM1 IS.I.OR.215(d)**)

Organizacje mogą rozważyć opracowanie formalnych porozumień (np. protokołu ustaleń) określających role i obowiązki w zakresie współpracy w zakresie bezpieczeństwa informacji, takich jak spotkania dotyczące zarządzania, wspólne działania rozwojowe oraz udostępnianie wskaźników naruszeń (IoC) w czasie rzeczywistym.

Ponadto zobowiązanie do współpracy można również osiągnąć poprzez aktywny udział organizacji w inicjatywach dotyczących udostępniania bezpieczeństwa informacji, na przykład w ramach ISAC. Dodatkowo, dla własnej świadomości, organizacje mogą również zapisać się na otrzymywanie alertów o lukach w zabezpieczeniach i zagrożeniach, takich jak te dystrybuowane przez CERT.

Co mówi przepis IS.D.OR.215 (e)/ IS.I.OR.215 (e)

e) Organizacja może zintegrować taki system zgłaszania zdarzeń z innymi systemami zgłaszania, które już wdrożyła.

Korzyści z Integracji:

- Wydajność
- Spójność
- Łatwość komunikacji
- Oszczędność czasu
- Optymalizacja zasobów
- Jakość danych

BENEFITS:

- Efficiency
- Consistency
- Ease of Communication
- Time Saving
- Resource optimization
- Data quality

Incydenty związane z bezpieczeństwem informacji – wykrywanie, reagowanie i działania naprawcze

(IS.I.OR.220 i IS.D.OR.215)

Urząd Lotnictwa Cywilnego

15.09.2025

Co mówi przepis IS.D.OR.220 (a) / IS.I.OR.220 (a)

a) Na podstawie wyniku oceny ryzyka przeprowadzonej zgodnie z pkt IS.I.OR.205 i wyniku procesu zmniejszania ryzyka przeprowadzonego zgodnie z pkt IS.I.OR.210 organizacja wdraża środki służące wykrywaniu incydentów i podatności, które wskazują na ewentualne urzeczywistnienie się niedopuszczalnego ryzyka i mogą mieć potencjalny wpływ na bezpieczeństwo lotnicze. Dzięki tym środkom wykrywania organizacja może:

1) identyfikować odstępstwa od wcześniej określonych wartości bazowych dotyczących osiągów funkcjonalnych;

2) wysyłać ostrzeżenia służące uruchomieniu odpowiednich środków reagowania w przypadku każdego odstępstwa.

AMC1 IS.I.OR.220 (a) Główne elementy:

- Zdefiniowanie i wdrożenie polityki wykrywania (detection)
- Obejmij wszystkie znane zagrożenia InfoSec dla zasobów (aktywów)

- W ramach polityki wykrywania:
  - Określ listę scenariuszy zagrożeń (patrz: ocena ryzyka)
  - Zidentyfikuj zasoby, które w przypadku naruszenia przyczyniają się do tych scenariuszy, biorąc pod uwagę środki wprowadzone podczas postępowania z ryzykiem (I.OR.210)

(Bardziej szczegółowo - **AMC1 IS.I.OR.220 - Wykrywanie**)

WYKRYWANIE

Spełniając wymóg określony w IS.I.OR.220(a), organizacja powinna zdefiniować i wdrożyć politykę wykrywania incydentów bezpieczeństwa informacji, które mogą mieć potencjalny wpływ na bezpieczeństwo.
Należy to zrobić w taki sposób, aby przynajmniej polityka wykrywania obejmowała wszystkie znane zagrożenia bezpieczeństwa informacji dla jej aktywów, które mogą zmaterializować się w postaci zagrożenia bezpieczeństwa o niedopuszczalnych konsekwencjach.

POLITYKA WYKRYWANIA

Aby określić zakres wykrywania zdarzeń, organizacja powinna:

(a) zidentyfikować listę scenariuszy zagrożeń spośród ryzyk zidentyfikowanych zgodnie z IS.I.OR.205;

(b) zidentyfikować co najmniej te aktywa, które w przypadku naruszenia przyczyniają się do scenariusza(-ów), który(-e) może(-gą) zmaterializować się w warunkach niebezpiecznych. W celu identyfikacji aktywów należy również uwzględnić środki wprowadzone zgodnie z IS.I.OR.210.

GM1 - **IS.I.OR.220 (a) – Wykrywanie (Detect)**

Zdefiniuj warunki, które uruchamiają proces, który na przykład wymagałby interwencji personelu i dalszej analizy.

- Odchylenia od oczekiwanego poziomu bazowego funkcjonalności;
- Odchylenia od oczekiwanego poziomu bazowego bezpieczeństwa informacji (działanie mechanizmów kontroli)
- Nietypowe zachowanie;
- Korelacja wielu niezależnych zdarzeń. (np. SIEM).

Co należy wdrożyć i sprawdzić:

- Czy Twoja organizacja zdefiniowała i wdrożyła politykę wykrywania?
- Czy uwzględniono wszystkie znane zagrożenia InfoSec dla zasobów?
- Czy zdefiniowano listę wiarygodnych scenariuszy zagrożeń?
- Czy stworzono inwentaryzację zasobów przyczyniających się do scenariusza zagrożenia z możliwym negatywnym wpływem na bezpieczeństwo?
- Czy jasno zdefiniowano warunki, które wymagają interwencji człowieka i dalszej analizy?
- Czy wdrożono narzędzie do korelacji wielu niezależnych zdarzeń?

Co mówi przepis IS.D.OR.220 (b) / IS.I.OR.220 (b) - Reagowanie

b) Organizacja wdraża środki reagowania na wszelkie zdarzenia zidentyfikowane zgodnie z lit. a), które mogą przerodzić się lub już przerodziły się w incydent związany z bezpieczeństwem informacji. Dzięki tym środkom reagowania organizacja może:

1) rozpocząć działanie w reakcji na ostrzeżenia, o których mowa w lit. a) ppkt 2, poprzez uruchomienie wcześniej określonych zasobów i sposobu postępowania;

2) ograniczyć rozprzestrzenianie ataku i uniknąć pełnego urzeczywistnienia się scenariusza zagrożenia;

3) kontrolować tryb awaryjny uszkodzonych elementów określonych w pkt IS.I.OR.205 lit. a).

AMC1 IS.I.OR.220 (b) Główne elementy:

W przypadku incydentów:

- Role i obowiązki
- Procedura reagowania:
  - Ocena alertów i ostrzeżeń pod kątem ich potencjalnego wpływu na bezpieczeństwo lotnicze
  - Polityka powstrzymywania incydentów dla każdego zasobu/kategorii incydentów, w tym kryteria wskazujące na zakończenie powstrzymywania
- Czas reakcji adekwatny do poziomu wpływu

AMC1 IS.I.OR.220 (b) - Główne elementy - Reagowanie

• Środki reagowania oparte na procedurze reagowania
• Czas reakcji i środki podejmowane dopiero po pełnej weryfikacji, że nie spowodują one dodatkowych, natychmiastowych skutków dla bezpieczeństwa

W przypadku luk w zabezpieczeniach:
- Opracowanie polityki zarządzania lukami w zabezpieczeniach (podatnościami)

GM1 IS.I.OR.220 (b) - Reagowanie

Atak uznaje się za opanowany po zidentyfikowaniu granic incydentu.
- Dalsze wskazówki znajdują się w dokumencie EUROCAE ED-206, rozdział 5 „Analiza zdarzeń bezpieczeństwa”.

• Termin „ostrzeżenie/warning” należy rozumieć jako „alarm/alert”.
• Możliwość wdrożenia technik „oszustwa”, takich jak honeypoty (dezorientacja, spowolnienie lub odwrócenie uwagi atakujących).
• Wskazówki dotyczące polityki zarządzania podatnościami znajdują się w dokumencie EUROCAE ED-206, rozdział 3.4.

GM - Definicje (1)

Zarządzanie incydentami

Zdolność do efektywnego zarządzania nieoczekiwanymi (nie)zakłócającymi zdarzeniami, w celu minimalizacji skutków i utrzymania lub przywrócenia normalnego funkcjonowania w określonych ramach czasowych.

Reagowanie na incydenty – podzbiór zarządzania incydentami

Zdolność operacyjna zarządzania incydentami, która:

- identyfikuje incydenty, przygotowuje się do nich i reaguje na nie w celu kontrolowania i ograniczania szkód
- zapewnia możliwości prowadzenia analiz kryminalistycznych i dochodzeniowych; oraz
- utrzymuje, odzyskuje i przywraca normalne funkcjonowanie zgodnie z definicją zawartą w umowach o poziomie usług (SLA)

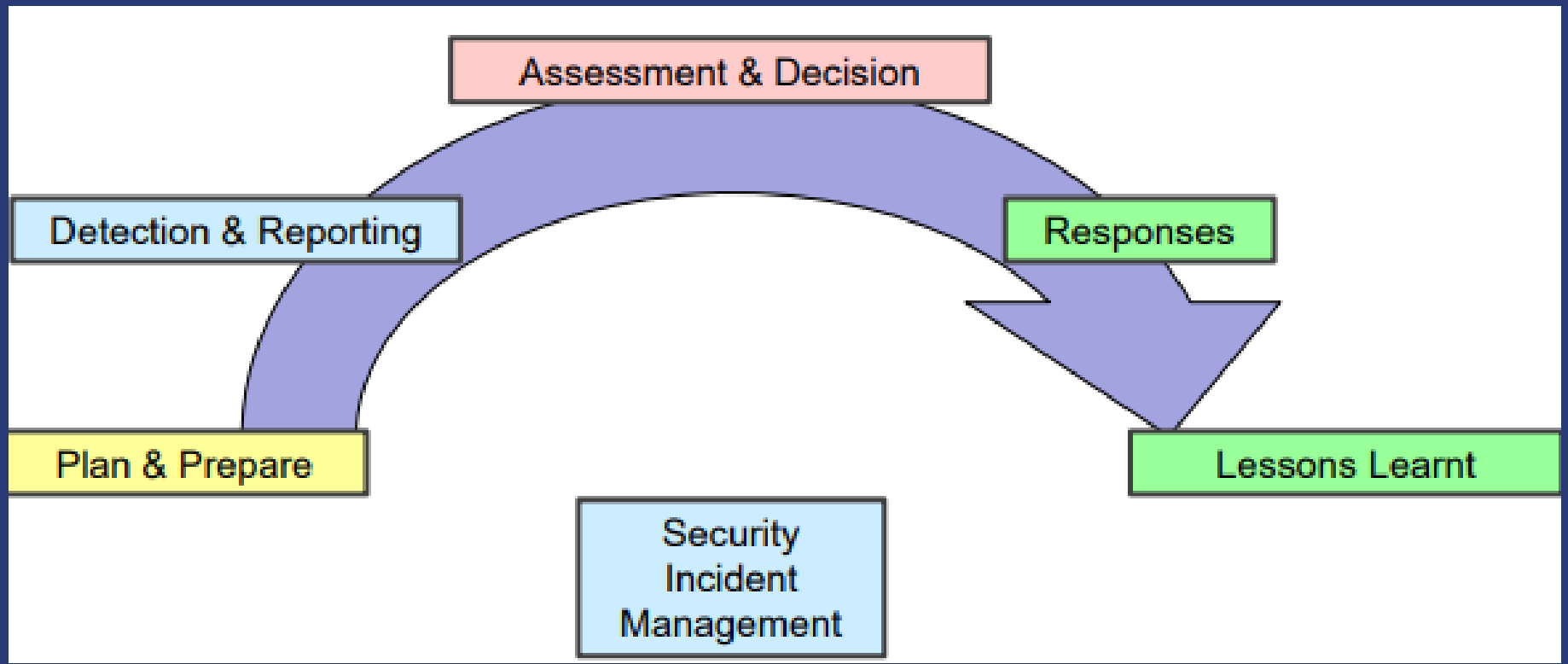
GM - Definicje (2)

Zdolność reagowania:

- Polityka powstrzymywania różnych incydentów
- Plan komunikacji (przykład: tabela RACI)
    - Odpowiedzialność, Rozliczalność (Accountable), Konsultacje, Poinformowanie
- Procedury odzyskiwania zgodne z
    - Planami Ciągłości Działania (BCP)
    - Planami Odzyskiwania Po Awarii (DRP)
- Uzyskane wsparcie kierownictwa
- Wdrożone wymagane narzędzia

Fazy zarządzania incydentami (ISO/IEC 27035)

Fazy zarządzania incydentami (ISO/IEC 27035)



- Incident Management Policy
  - Processes
  - Procedures
  - …
- Support (technical, operations)
- Response team established
- Awareness & training
- ToRs
- Contact information

Event :
Detection
- Human / automatic
- Alerts, Alarms
- Log event information
- Report vulnerabilities
- Record in database

Reporting

- Assessment
- Type of Incident?
- Assets affected?
- Who does what?
- Prioritize
- Assess unexploited vulnerabilities
- Record in database

- Incident under control?
- Escalate to crisis management?
- External organisations impacted? Communicate
- Forensic analysis
- Recovery
- Reconfigure
- Patch
- Re-install

Post-incident review
- Forensic analysis
- Identify lessons learnt
- Document
- Report to management

Plan Improvements :
- Risk assessment
- Management review
- Incident management process

IS.D.OR.220 (b) / IS.I.OR.220 (b) - Reagowanie - **Podsumowanie**

Co należy wdrożyć i sprawdzić.

- Zdefiniowano proces aktywacji predefiniowanych zasobów i działań multidyscyplinarnych w przypadku wystąpienia incydentu;
- Zdefiniowano role i obowiązki w zakresie reagowania;
- Zdefiniowano politykę powstrzymywania incydentów;
- Zdefiniowano maksymalny akceptowalny poziom pogorszenia bezpieczeństwa;
- Wprowadzono mechanizm weryfikacji, aby zapobiec potencjalnemu natychmiastowemu negatywnemu wpływowi na bezpieczeństwo podczas podejmowania działań;
- Ustalono kryteria, które pozwalają uznać incydent za opanowany;
- Opracowano politykę zarządzania podatnościami

Co mówi przepis IS.D.OR.220 (c) / IS.I.OR.220 (c) – Działania Naprawcze

Organizacja wdraża środki służące przywróceniu stanu sprzed incydentów związanych z bezpieczeństwem informacji, w tym w razie potrzeby środki reagowania w sytuacjach zagrożeń. Dzięki tym środkom naprawczym organizacja może:

1) wyeliminować stan będący źródłem incydentu lub ograniczyć go do dopuszczalnego poziomu;
2) doprowadzić do bezpiecznego stanu uszkodzone elementy określone w pkt IS.I.OR.205 lit. a) w czasie naprawy wcześniej określonym przez organizację.

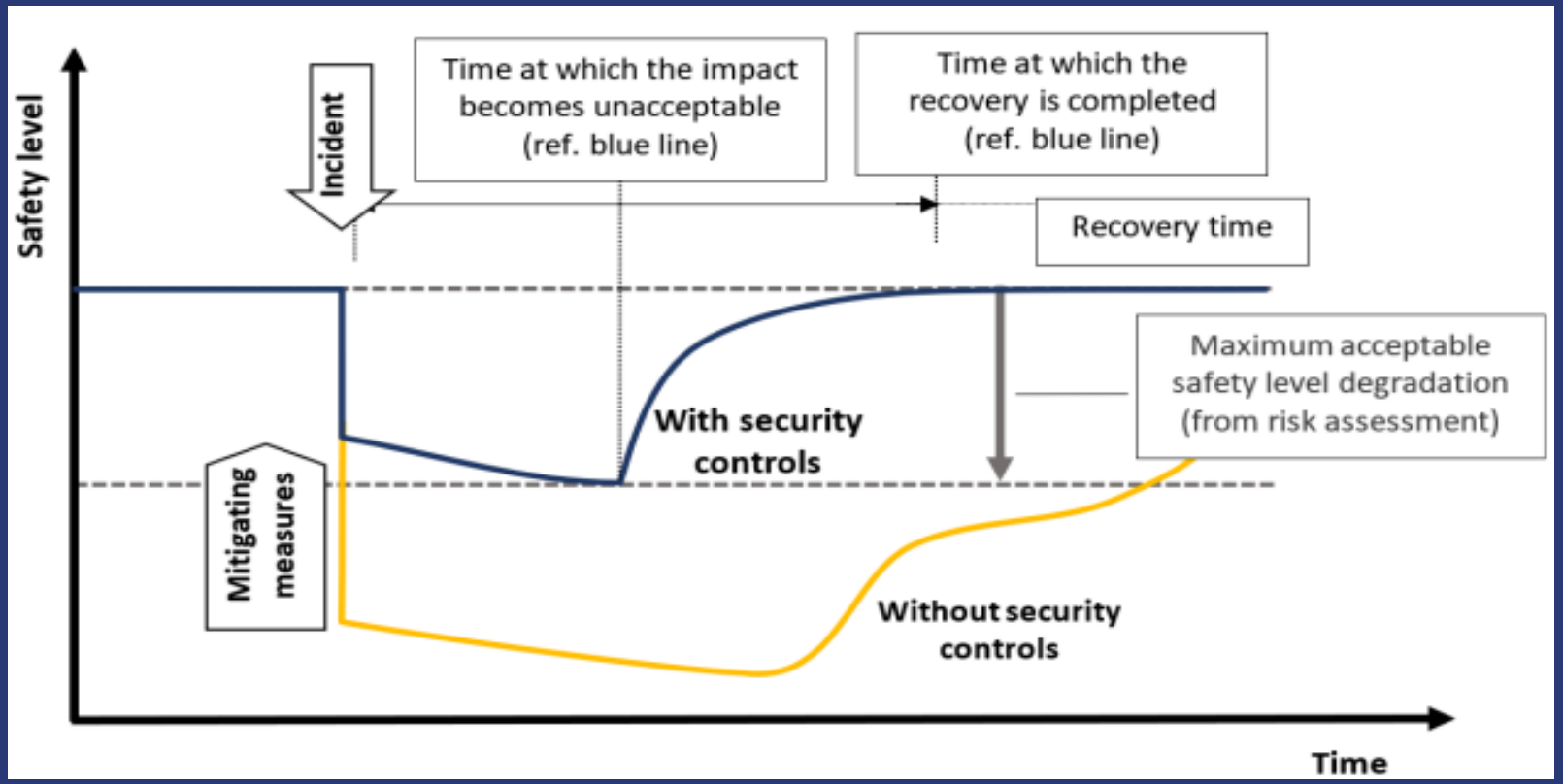
AMC1 IS.I.OR.220 (c) Główne elementy:

Spełniając wymóg określony w IS.I.OR.220(c), organizacja powinna opracować procedurę odzyskiwania po incydencie, obejmującą co najmniejnastępujące elementy:

- listę zasobów, które umożliwiają bezpieczne działanie, a także zależności między nimi, stanowiących zakres odzyskiwania;
- opis procesu wraz z niezbędnymi działaniami priorytetowymi, które należy wykonać w celu przywrócenia stanu bezpiecznego zasobów objętych zakresem odzyskiwania;
- zasoby wymagane do wykonania działań określonych w lit. b), aby zapewnić łatwą dostępność tych zasobów po wystąpieniu incydentu;
- cele dotyczące czasu odzyskiwania, które należy ustalić w odniesieniu do krytyczności bezpieczeństwa zasobów objętych zakresem odzyskiwania.

GM IS.D.OR.220 (c) / IS.I.OR.220 (c) – Działania Naprawcze

- Konieczność wdrożenia środków reagowania i odzyskiwania w celu zapewnienia, że bezpieczeństwo operacyjne utrzymuje się powyżej minimalnego akceptowalnego poziomu
- Należy zapoznać się z Rysunkiem 1, aby zdefiniować cele reagowania i odzyskiwania, w tym czas odzyskiwania
- Cele dotyczące czasu odzyskiwania można wyrazić jako listę zasobów i usług, które mają zostać przywrócone według priorytetu
- Wytyczne dotyczące celów dotyczących czasu odzyskiwania można znaleźć w dokumencie EUROCAE ED-206, rozdział 7.3.5



Rysunek 1

IS.D.OR.220 (c) / IS.I.OR.220 (c) – Działania Naprawcze- Podsumowanie

Co należy wdrożyć i sprawdzić.

Czy istnieje procedura odzyskiwania po incydencie, obejmująca co najmniej:

- Listę zasobów umożliwiających bezpieczne działanie i ich zależności?
- Opis procesu wraz z priorytetowymi działaniami mającymi na celu powrót do stanu bezpiecznego?
- Zasoby do wykonania działań podczas reagowania i odzyskiwania?
- Cele dotyczące czasu odzyskiwania, ustalone w odniesieniu do krytyczności bezpieczeństwa zasobów.

System zewnętrznego zgłaszania zdarzeń związanych z bezpieczeństwem informacji

(IS.I.OR.230 i IS.D.OR.230)

Urząd Lotnictwa Cywilnego

15.09.2025

Co mówi przepis IS.D.OR.230 / IS.I.OR.230

a) Organizacja wdraża system zgłaszania zdarzeń związanych z bezpieczeństwem informacji, który jest zgodny z wymaganiami określonymi w rozporządzeniu (UE) nr 376/2014 i w jego aktach delegowanych i wykonawczych, jeżeli rozporządzenie to ma zastosowanie do danej organizacji.

b) Bez uszczerbku dla obowiązków określonych w rozporządzeniu (UE) nr 376/2014 organizacja zapewnia, aby każdy incydent związany z bezpieczeństwem informacji lub podatność, które mogą stanowić poważne ryzyko dla bezpieczeństwa lotniczego, zgłaszano właściwemu organowi, któremu podlega. Ponadto:

1) jeżeli taki incydent lub taka podatność ma wpływ na statek powietrzny lub powiązany system lub komponent, organizacja zgłasza taki incydent lub taką podatność również posiadaczowi zatwierdzenia projektu;

2)jeżeli taki incydent lub taka podatność ma wpływ na system lub część składową wykorzystywane przez organizację, organizacja ta zgłasza taki incydent lub taką podatność organizacji odpowiedzialnej za projekt danego systemu lub danej części składowej.

Co mówi przepis IS.D.OR.230 / IS.I.OR.230

c) organizacja zgłasza stan, o których mowa w lit. b), w następujący sposób:
- **zgłasza do właściwego organu (CA)**
- **raport należy złożyć do właściwego organu (72 godziny)**
- **raport uzupełniający należy złożyć do właściwego organu**

AMC1 IS.I.OR.230 (a)

Aby spełnić przepisy IS.I.OR.230 (a) i (b), organizacja powinna zgłaszać:

(a) każde zdarzenie objęte rozporządzeniem (UE) nr 376/2014, które wynikało z celowych nieautoryzowanych interakcji elektronicznych;

(b) incydenty związane z bezpieczeństwem informacji stanowiące potencjalnie znaczne ryzyko dla bezpieczeństwa lotniczego, nieobjęte rozporządzeniem (UE) nr 376/2014;

(c) luki w zabezpieczeniach, które stanowią znaczne ryzyko dla bezpieczeństwa lotniczego i nie zostały jeszcze odpowiednio ograniczone zgodnie z zatwierdzoną strategią zarządzania lukami w zabezpieczeniach (patrz AMC1 IS.I.OR.220(b))

GM1 IS.I.OR.230 (a)

Organizacje są zobowiązane do zgłaszania zdarzeń swojemu właściwemu organowi.

PRZYKŁADY

Organizacje projektowe zatwierdzone przez EASA: EASA jest właściwym organem.
Przewoźnicy lotniczy certyfikowani przez właściwy organ państwa członkowskiego: właściwy organ państwa członkowskiego jest właściwym organem.

PRZYPADKI SZCZEGÓLNE

W sytuacji, gdy organizacja posiada dwa certyfikaty przewoźnika lotniczego (AOC) wydane przez dwa różne państwa członkowskie UE (państwo A i B), zdarzenia dotyczące statków powietrznych eksploatowanych w ramach AOC państwa A muszą być zgłaszane właściwemu organowi państwa A; natomiast zdarzenia dotyczące statków powietrznych eksploatowanych w ramach AOC państwa B muszą być zgłaszane właściwemu organowi państwa B.

GM1 IS.I.OR.230(a) i(b)

ZWIĄZEK MIĘDZY IS.I.OR.230(b) A ROZPORZĄDZENIEM (UE) NR 376/2014

Zgodność z pktIS.I.OR.230(b) nie zwalnia organizacji z obowiązku przestrzegania rozporządzenia (UE) nr 376/2014.
W przypadku każdej kategorii zgłaszającego rozporządzenie (UE) 2015/1018 określa charakter zdarzeń, które podlegają obowiązkowemu zgłaszaniu.

Ponadto zgodność z rozporządzeniem (UE) nr 376/2014 nie zwalnia organizacji z obowiązku przestrzegania pkt IS.I.OR.230(b). Nie powinno to jednak prowadzić do powstania dwóch równoległych systemów raportowania, a pkt IS.I.OR.230(b) i rozporządzenie (UE) nr 376/2014 należy postrzegać jako uzupełniające się w tym zakresie.

Te obowiązki raportowania można zrealizować za pośrednictwem jednego kanału raportowania. Ponadto każda osoba fizyczna lub prawna, która pełni więcej niż jedną rolę podlegającą obowiązkowi raportowania, może zrealizować wszystkie te obowiązki za pośrednictwem jednego raportu. Zachęca się organizacje do odpowiedniego opisania tego w swoim podręczniku organizacji, aby uwzględnić przypadki, w których obowiązki są realizowane w imieniu organizacji

GM1 IS.I.OR.230(a) i(b)

ANALIZA NASTĘPCZA

Jeżeli analiza zdarzenia zgłoszonego zgodnie z rozporządzeniem (UE) nr 376/2014 wykaże później, że przyczyną źródłową lub czynnikiem przyczyniającym się do zdarzenia była celowa, nieautoryzowana interakcja elektroniczna, organizacja powinna zaktualizować swoje zgłoszenie do właściwego organu.

ZNACZĄCE RYZYKO DLA BEZPIECZEŃSTWA LOTNICZEGO

Zgodnie z definicją zdarzenia zawartą w art. 2 ust. 7 rozporządzenia (UE) nr 376/2014, każdy incydent lub luka w zabezpieczeniach bezpieczeństwa informacji, które mogą stanowić istotne zagrożenie dla bezpieczeństwa lotniczego, powinny być uznawane za zdarzenie podlegające zgłoszeniu. Znaczące ryzyko dla lotnictwa oznacza stan niebezpieczny, tj. taki, który może doprowadzić do wypadku lub poważnego incydentu (zgodnie z definicją zawartą w załączniku 13 ICAO).

Uwaga: Oceniając możliwość, że skutki incydentu bezpieczeństwa informacji mogą doprowadzić do niebezpiecznego stanu, organizacja powinna rozważyć kombinację skutków, jeśli incydent dotyczy wielu systemów; w rzeczywistości niektóre założenia dotyczące niezależności systemów, które mogą być ważne w przypadku zdarzeń losowych, mogą zostać naruszone przez celowe działania.

GM1 IS.I.OR.230(c)

Wytyczne dotyczące zgłaszania incydentów bezpieczeństwa informacji i luk w zabezpieczeniach można znaleźć w EUROCAE ED-206, rozdział 6.4.2.2 — Harmonogram zgłaszania i rozdział 6.4.5 — Zgłaszanie informacji.

Nie jest to jedyne źródło, w którym można znaleźć wytyczne, a organizacja może odwołać się do innych wytycznych, bardziej odpowiednich dla jej zastosowania.

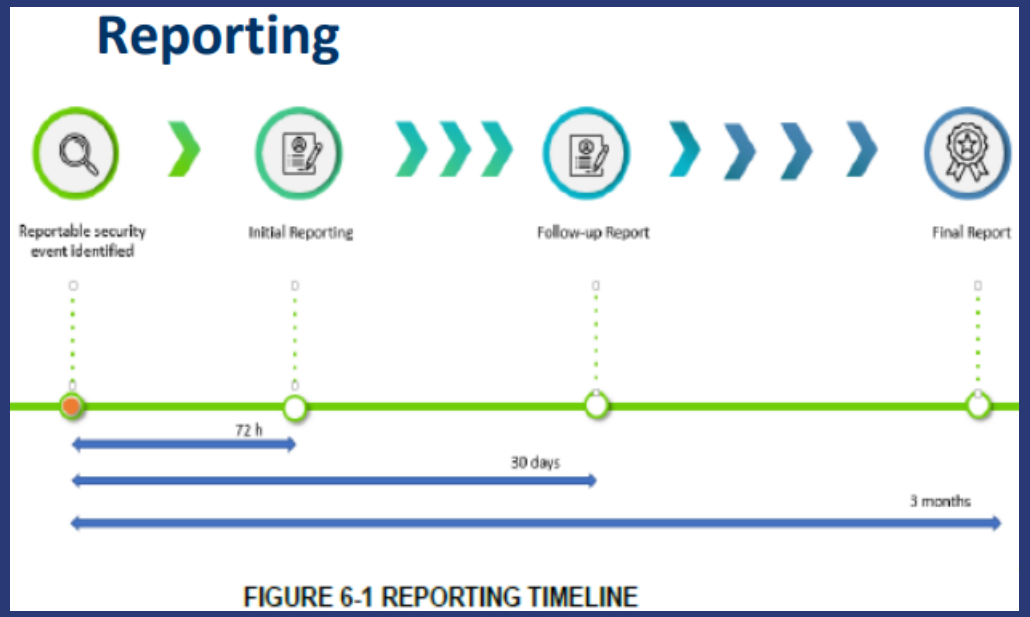


FIGURE 6-1 REPORTING TIMELINE

Incydent bezpieczeństwa informacji

Incydent bezpieczeństwa informacji to niepożądane lub nieoczekiwane zdarzenie, które może zakłócić normalne funkcjonowanie systemu informatycznego lub zagrozić poufności, integralności i dostępności danych.

Obejmuje to szeroki zakres zdarzeń, od błędów technicznych i ludzkich, przez cyberataki, wirusy, phishing, po kradzież fizycznych nośników danych.

Przykłady incydentów bezpieczeństwa obejmują:
nieautoryzowany dostęp do systemów (ataki hakerskie), wycieki lub utratę danych, ataki złośliwego oprogramowania (takie jak wirusy czy ransomware), ataki DDoS, phishing i socjotechnikę (próby wyłudzenia danych), a także fizyczną kradzież nośników danych oraz błędy ludzkie prowadzące do naruszenia bezpieczeństwa.

Podatność

Podatność to słabość w systemie komputerowym, oprogramowaniu, sprzęcie, sieci lub procedurach, która może zostać wykorzystana przez atakującego do uzyskania nieautoryzowanego dostępu, zmiany danych lub innej niechcianej działania, prowadząc do incydentu bezpieczeństwa.

Podatności mogą wynikać z błędów w projekcie lub implementacji, nieprawidłowej konfiguracji, braku aktualizacji lub słabych polityk bezpieczeństwa.

DZIĘKUJĘ ZA UWAGĘ

Piotr KACZMARCZYK

Naczelnik Inspektoratu Zarządzania Bezpieczeństwem Lotniczym
Departament Zarządzania Bezpieczeństwem w Lotnictwie Cywilnym
tel. +48 (22) 520 72 93, tel. kom. +48 694 409 507
e-mail: placzmarczyk@ulc.gov.pl

SUPPORTING EUROPEAN AVIATION

Prezentacja przygotowana z wykorzystaniem wybranych materiałów EUROCONTROL

15.09.2025