

Zarządzanie bezpieczeństwem informacji wg normy BS 7799 – Wprowadzenie

Wojciech Dworakowski

SecuRing S.C.

e-mail: wojciech.dworakowski@securing.pl

Streszczenie

Norma BS 7799 (polski odpowiednik: PN-I-07799) dotyczy zarządzania bezpieczeństwem informacji. W związku z rosnącym znaczeniem bezpieczeństwa informacji w kontaktach handlowych, coraz częściej certyfikacja na zgodność z tą normą staje się wymogiem formalnym przy zawieraniu kontraktów z partnerami zagranicznymi (i nie tylko), podobnie jak powszechny już wymóg potwierdzenia zgodności z normami serii ISO 9000. W ciągu ostatniego roku większość liczących się na rynku polskim podmiotów certyfikacyjnych wprowadziło do swojej oferty certyfikację na zgodność z BS 7799. Coraz więcej firm działających na rynku polskim rozważa konieczność certyfikacji swojego systemu zarządzania bezpieczeństwem informacji. W związku z tym, prawdopodobnie większość pracowników działów IT (i nie tylko) w najbliższym czasie będzie miało styczność z wyżej wymienioną normą.

Wykład będzie miał na celu przybliżenie słuchaczom normy BS 7799 w kontekście praktycznych zastosowań w firmach różnej wielkości. Postaram się wyjaśnić wszelkie niejasności wynikające z błędnego zrozumienia tych regulacji. Zostaną omówione: różnice między pierwszą częścią normy BS 7799 (odpowiednik krajowy: PN ISO/IEC 17799) i częścią drugą BS 7799-2 (PN-I-07799), zakres stosowania norm oraz poszczególne rozdziały dotyczące różnych środków bezpieczeństwa. Zostanie także omówiony model PDCA (Plan - Do - Check - Act) na którym opiera się wdrożenie i utrzymanie systemu bezpieczeństwa informacji, oraz kroki jakie należy podjąć, aby wdrożyć ISO 17999 i ewentualnie uzyskać certyfikację systemu zarządzania na zgodność z BS 7799-2 (PN-I-07799). W powszechnym mniemaniu norma ta przeznaczona jest dla dużych organizacji. Postaram się pokazać, że również małe i średnie firmy mogą ją wdrożyć stosunkowo małym nakładem sił i odnieść korzyści z uporządkowania zarządzania informacją.

Informacja o autorze

Ekspert ds. bezpieczeństwa IT w firmie SecuRing. Koordynator prac zespołu i osoba odpowiedzialna za sporządzanie raportów. Osiem lat doświadczenia praktycznego w zakresie bezpieczeństwa IT. Od pięciu lat zajmuje się również problemami bezpieczeństwa produktów Oracle. Prelegent na licznych konferencjach poświęconych bezpieczeństwu IT (m.in. CERT Secure, PLOUG, Open Source Security, Windows Security). Prowadzi rubrykę poświęconą bezpieczeństwu w Biuletynie PLOUG. Posiada certyfikat Audytora Wiodącego Systemu Zarządzania Bezpieczeństwem Informacji wg BS 7799.

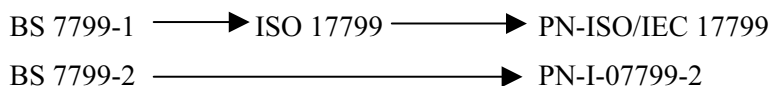
1. Wstęp

Norma BS 7799 (polski odpowiednik: PN-ISO/IEC 17799 i PN-I-07799) dotyczy zarządzania bezpieczeństwem informacji. W związku z rosnącym znaczeniem bezpieczeństwa informacji w kontaktach handlowych, co raz częściej certyfikacja na zgodność z tą normą staje się wymogiem formalnym przy zawieraniu kontraktów z partnerami zagranicznymi (i nie tylko), podobnie jak powszechny już wymóg potwierdzenia zgodności z normami serii ISO 9000. W ciągu ostatniego roku większość liczących się na rynku polskim podmiotów certyfikacyjnych wprowadziło do swojej oferty certyfikację na zgodność z BS 7799. Coraz więcej firm działających na rynku polskim rozważa konieczność certyfikacji swojego systemu zarządzania bezpieczeństwem informacji. W związku z tym, prawdopodobnie większość pracowników działów IT (i nie tylko) w najbliższym czasie będzie miało styczność z wyżej wymienioną normą.

2. BS 7799, ISO 17799, PN-ISO/IEC 17799, PN-I-07799, ...

Dla kogoś kto pierwszy raz styka się z normami wywodzącymi się z BS 7799 pewien problem mogą sprawiać różne mutacje norm i sposoby numeracji normy z tej serii. Spróbujmy to wyjaśnić.

Po pierwsze wszystkie normy pochodne (ISO, Polska Norma) bezpośrednio wywodzą się z normy brytyjskiej BS 7799 ustanowionej przez BSI (British Standards Institution). Po drugie, są dwie części normy, w oryginale oznaczane jako BS 7799-1 oraz BS 7799-2. Pierwsza część jest spisem zasad dobrej praktyki albo inaczej mówiąc – swojego rodzaju katalogiem zabezpieczeń. Druga część to wytyczne do wdrażania normy oraz znajdująca się w załączniku A lista kontrolna. Pierwsza część została przyjęta przez organizację ISO jako standard ISO 17799 i dalej przyjęta do systemu „Polska Norma” jako PN-ISO/IEC 17799. Druga część normy (BS 7799-2) nie została przyjęta do systemu norm ISO, natomiast została przyjęta do systemu „Polska Norma” pod numerem PN-I-07799-2.



Wkrótce ta nieco skomplikowana numeracja ma zostać ujednolicona. Trwają prace nad wprowadzeniem obu części normy BS do drzewa norm ISO pod numerami ISO 27001 i 27002.

3. Zakres stosowania normy BS 7799

Normę BS 7799 stosuje się w odniesieniu do systemu zarządzania bezpieczeństwem informacji (funkcjonuje tu skrót angielski: ISMS - Information Security Management System). Jej zapisy dotyczą zarówno informacji „papierowej” jak i informacji przechowywanej w systemach informatycznych. Jednakże zakres stosowania normy instytucja wybiera sobie sama. Zakres może obejmować całość informacji przetwarzanej w danej instytucji (nie tylko w systemach komputerowych) ale z reguły instytucje wdrażające ograniczają się tylko do systemu teleinformatycznego. Warto podkreślić że w takim wypadku zapisy normy stosuje się również do informacji „papierowej” związanej z systemem teleinformatycznym (np. dokumentacja systemu, wydruki, itp.).

Normę można również wdrożyć dla jednego wydzielonego systemu (np. system księgowy w firmie, czy system bankowości elektronicznej w banku) jednak w takim wypadku system ten musi być dość ściśle oddzielony od innych systemów eksploatowanych w danej instytucji. Zarówno na poziomie organizacyjnym jak i fizycznym i technicznym. W przeciwnym wypadku podczas wdrażania systemu zarządzania bezpieczeństwem informacji dla takiego wydzielonego podsystemu można spotkać się z wieloma problemami. Przykładowo: Jeśli w serwerowni w której jest

część zabezpieczanego systemu A stoją również serwery innych systemu B, to administratorzy systemu B również muszą podlegać wdrażanym procedurom dostępu do serwerowni dla systemu A. To znowu rodzi z reguły problemy natury organizacyjnej (np. czy zwierzchnik systemu A może nakazać coś administratorom systemu B?).

4. Środki bezpieczeństwa

Poza zdefiniowaniem modelu zarządzania bezpieczeństwem informacji, norma BS 7799 zawiera opis zabezpieczeń, które należy stosować w celu ograniczenia ryzyka. Pierwsza część normy (PN-ISO/IEC 17799) „Praktyczne zasady zarządzania bezpieczeństwem informacji” zawiera swojego rodzaju katalog zabezpieczeń. Znajdują się tam zarówno zabezpieczenia organizacyjne, proceduralne jak i techniczne. Norma operuje na dość dużym stopniu ogólności. Przykładowo mówi o konieczności ochrony przed wrogim kodem a nie o konieczności stosowania systemów antywirusowych w określonej architekturze. Zapisy ogólne są po prostu bardziej uniwersalne, zwłaszcza jeśli weźmiemy pod uwagę dynamiczny rozwój technologii informatycznych oraz powstawanie nowych zagrożeń. Zabezpieczenia proponowane przez normę są podzielone na 10 zakresów:

1. Polityka bezpieczeństwa
2. Organizacja bezpieczeństwa
3. Klasyfikacja i kontrola aktywów
4. Bezpieczeństwo osobowe
5. Bezpieczeństwo fizyczne i środowiskowe
6. Zarządzanie systemami i sieciami
7. Kontrola dostępu do systemu
8. Rozwój i utrzymanie systemu
9. Zarządzanie ciągłością działania
10. Zgodność

Dla osób nie mających na codzień do czynienia z omawianą normą (a zwłaszcza dla osób o doświadczeniu technicznym) dziwne może się wydać, że to co tradycyjnie wiążemy z bezpieczeństwem systemów informatycznych jest ujęte tylko w trzech z dziesięciu zakresów normy (6, 7, 8). Norma nie ignoruje tematów technicznych ale też przesadnie ich nie przecenia. Równie ważne jak posiadanie sprawnego firewalla jest to żeby był zabezpieczony fizyczny dostęp do niego a dalece ważniejsze jest to żeby istniały procedury regulujące sposób tworzenia reguł na tym firewallu, procedury kontroli jego skuteczności oraz wyznaczenie osób odpowiedzialnych za ten element systemu bezpieczeństwa. Norma BS 7799 jest kompleksowa i stara się obejmować wszystkie aspekty bezpieczeństwa informacji. Poszczególne zabezpieczenia możemy porównać do elementów płotu, natomiast system zarządzania bezpieczeństwem informacji do kompletnego ogrodzenia. Jeżeli zastosujemy tylko niektóre zabezpieczenia to nasze ogrodzenie będzie dziurawe a co za tym idzie nieskuteczne.

5. Budowa i utrzymanie systemu zarządzania bezpieczeństwem informacji wg BS 7799

5.1. Model „Planuj – Wykonuj – Sprawdź – Działaj”

Tworzenie, wdrażanie i eksploatawanie systemu zarządzania bezpieczeństwem informacji wg BS 7799 odbywa się w cyklu składającym się z czterech etapów: Planuj, Wykonuj, Sprawdź,

Działaj (w literaturze powszechnie funkcjonuje skrót PDCA – ang: Plan-Do-Check-Act). Norma PN-I-07799-2 opisuje te etapy w sposób następujący¹:

- | | |
|----------------|---|
| Planuj | Ustanowienie polityki bezpieczeństwa, cele, zakres stosowania, procesy i procedury odpowiadające zarządzaniu ryzykiem oraz zwiększające bezpieczeństwo informacji, tak aby uzyskać wyniki zgodne z ogólnymi zasadami i celami instytucji. |
| Wykonuj | Wdrożenie i eksploatacja polityki bezpieczeństwa, zabezpieczeń, procesów i procedur. |
| Sprawdź | Szacowanie oraz tam, gdzie ma zastosowanie, pomiar wykonania procesów w odniesieniu do polityki bezpieczeństwa, cele i praktyczne doświadczenia oraz przekazywanie kierownictwu wyników przeglądu. |
| Działaj | Podjęcie działań korygujących i prewencyjnych w oparciu o wyniki przeglądu realizowanego przez kierownictwo, tak aby osiągnąć stałe doskonalenie ISMS. |

Z takiego podejścia wynikają najistotniejsze cechy systemu zarządzania bezpieczeństwem informacji:

- **Podjęcie decyzji na podstawie jasnych przesłanek.** BS 7799 nakazuje podejmowanie decyzji o zastosowaniu zabezpieczeń na podstawie analizy ryzyka. Pierwsza część normy (PN-ISO/IEC 17799) zawiera opis różnego rodzaju zabezpieczeń. Instytucja wdrażająca nie musi stosować wszystkich możliwych zabezpieczeń ale decyzja o tym czy dane zabezpieczenie zastosować czy też nie musi być podjęta na podstawie analizy ryzyka. Celem nadrzędnym powinno być przy tym zachowanie ciągłości działania instytucji. Tylko takie podejście gwarantuje zastosowanie zabezpieczeń wystarczających w przypadku konkretnej instytucji a więc osiągnięcie wyznaczonych celów przy minimalnych możliwych nakładach. W tym miejscu warto zauważyć, że podejście do wdrożenia BS 7799 polegające na powieleniu pewnego rodzaju szablonowych działań, które „działają” w ogólnym wypadku nie ma szans powodzenia. Z reguły doprowadzi to do przeinwestowania lub niedoinwestowania w bezpieczeństwo a co gorsza do pominięcia zakresów zagrożeń charakterystycznych dla danej instytucji. Należy na to zwrócić szczególną uwagę korzystając z różnego rodzaju zewnętrznych doradców i konsultantów.
- **Zdolność do „samonaprawiania” systemu.** System zarządzania bezpieczeństwem informacji powinien być zbudowany w ten sposób, żeby był zdolny do wykrywania niedociągnięć oraz do ciągłego doskonalenia systemu. Oznacza to, że w system zarządzania bezpieczeństwem muszą być wbudowane procedury reagowania na zauważone problemy i niezgodności oraz procedury okresowych przeglądów. Ponadto w razie wykrycia niezgodności muszą istnieć procedury zmierzające zarówno do bieżącego usunięcia problemu jak i do zmodyfikowania systemu zarządzania bezpieczeństwem tak żeby ograniczyć ryzyko wystąpienia problemu w przyszłości.

Poszczególne etapy modelu Planuj-Wykonuj-Sprawdź-Działaj są opisane w drugiej części normy (PN-I-07799) w rozdziale 4.2 (Ustanawianie i zarządzanie ISMS). W rozdziale tym opisane są działania jakie instytucja musi podjąć na każdym z tych etapów. Warto podkreślić że każde z tych działań jest bezwzględnie wymagane przez normę. Czyli jeśli chcemy żeby nasz system był zgodny z BS 7799 to nie możemy ominąć żadnego z wymienionych tam działań. Poniżej pokrótce opisano każdy z tych etapów:

¹ Polska Norma PN-I-07799-2 – „Systemy zarządzania bezpieczeństwem informacji – Specyfikacja i wytyczne do stosowania”; PKN 2005

5.2. Planuj: Ustanowienie ISMS

Wdrażanie ISMS powinno rozpocząć się od zdefiniowania zakresu jakiego będzie dotyczyć system zarządzania bezpieczeństwem informacji. Następnie należy określić politykę ISMS (często zwaną „polityką bezpieczeństwa”), przy czym wg BS 7799 jest to dokument ogólny, który „wyznacza ogólny kierunek i zasady działania w odniesieniu do bezpieczeństwa informacji”, a nie jak to często widuje się w różnorodnych opracowaniach – książka zawierająca wszystkie możliwe procedury. Dokument ten jedynie wyznacza kierunek działania w zakresie bezpieczeństwa informacji. Powinien brać pod uwagę wymagania biznesowe i prawne dotyczące danej instytucji, określać kryteria według których będzie szacowane ryzyko oraz określać strukturę organizacyjną. Bardzo ważne jest żeby dokument ten został przyjęty i zaakceptowany przez kierownictwo firmy.

Po zdefiniowaniu polityki bezpieczeństwa należy zdefiniować i przeprowadzić analizę ryzyka. Ważne przy tym, żeby był to proces powtarzalny. Norma nakazuje zdefiniowanie i opisanie procesu analizy ryzyka oraz wyznaczenie kryteriów akceptowania ryzyka. Warto przy tym zaznaczyć że norma nie narzuca żadnej konkretnej metody analizy ryzyka. Wymaga jedynie żeby proces ten był formalnie opisany i powtarzalny. W związku z powyższym w niewielkich firmach proces analizy ryzyka może być bardzo uproszczony.

Następnie należy przeprowadzić analizę ryzyka zgodnie z przyjętą metodą. Analiza ryzyka to temat na osobny wykład. Tutaj chciałbym tylko zaznaczyć, że aby przeprowadzić jakąkolwiek analizę ryzyka należy:

- Określić aktywa, a więc przeprowadzić inwentaryzację zarówno informacji, wyposażenia, oprogramowania jak i usług związanych z zakresem dla którego wdrażamy ISMS.
- Zidentyfikować zagrożenia dla tych aktywów (np. pożar, choroba administratora, atak hackera z Internetu).
- Zidentyfikować podatności, które mogą być wykorzystane przez te zagrożenia (np. brak kopii archiwalnych, brak osoby zastępującej administratora, „dziurawe” oprogramowanie).
- Określić skutki jakie może mieć wykorzystanie podatności przez zagrożenia (utrata poufności, integralności lub dostępności informacji)

Jak widać przeprowadzenie analizy ryzyka nie jest sprawą trywialną ale nie należy się tego przesadnie bać. W dobrze zorganizowanej instytucji, w której są opisane procesy biznesowe oraz jest aktualny spis zasobów potrzebnych dla działania tych procesów, jest to proces stosunkowo łatwy. Z reguły firmy i instytucje które wdrożyły normy z zakresu zarządzania jakością (ISO 9000) lub zarządzania środowiskowego (ISO 14000) są dość dobrze przygotowane do procesu analizy ryzyka. W firmach o niższej kulturze organizacyjnej również nie musi to być proces ciężki do przeprowadzenia. Ważne żeby przyjęta metoda szacowania ryzyka nie była zbyt skomplikowana do wykonania w danej instytucji a jednocześnie żeby była skuteczna.

Po zidentyfikowaniu ryzyka, należy określić co robimy z każdym z wykrytych ryzyk. Mamy tutaj do wyboru:

- Ograniczenie ryzyka przez zastosowanie zabezpieczeń. Lista zabezpieczeń znajduje się w załączniku A do drugiej części normy. Ponadto wszystkie zabezpieczenia są szczegółowo opisane w pierwszej części normy. Warto przy tym zaznaczyć że norma mówi wprost o tym, że nie należy ograniczać się tylko do tych zabezpieczeń, które są tam opisane. Jeśli uznamy to za konieczne, możemy wdrożyć również inne zabezpieczenia. Jest to o tyle ważne, że spis zabezpieczeń ujęty w normie może nie nadążać za rozwojem technologii.
- Przeniesienie ryzyka (np. na ubezpieczyciela lub dostawcę)
- Unikanie ryzyka

- Zaakceptowanie ryzyka. Współczesne podejście do bezpieczeństwa mówi wprost o tym, że nie ma systemów w 100% bezpiecznych. Zawsze, pomimo zastosowania najbardziej wyszukanych zabezpieczeń istnieje pewne ryzyko szczątkowe, które instytucja akceptuje. Ważne jest jednak żeby instytucja zdawała sobie sprawę z istnienia tego ryzyka i żeby zaakceptowała je w sposób świadomy. Przykładowo: Zabezpieczanie się przed ryzykiem zniszczenia lokalizacji podstawowej przez stworzenie i utrzymywanie zapasowego centrum przetwarzania danych ma sens tylko w instytucjach dla których dostępność systemów jest kluczowa (np. banki). W innych instytucjach wystarczy przechowywanie kopii archiwalnych poza siedzibą główną a dla jeszcze innych nawet to może nie mieć uzasadnienia ze względu na to, że system informatyczny nie jest kluczowy dla zachowania ciągłości działania firmy.

W ostatnim punkcie doszliśmy do kluczowej zasady jaka powinna rządzić sposobem dobierania zabezpieczeń w myśl BS 7799. Otóż podstawowym celem wdrożenia systemu zarządzania bezpieczeństwem informacji powinno być zapewnienie ciągłości działania firmy. To znaczy przy wyborze sposobu traktowania danego zagrożenia należy przede wszystkim wziąć pod uwagę to jakie skutki na zachowanie ciągłości działania firmy będzie miało zrealizowanie tego zagrożenia. Przykładowo: Jeśli główna serwerownia firmy zostanie zniszczona, to czy firma będzie w stanie funkcjonować? Jak długi przestój (brak dostępności systemu informatycznego) jest akceptowalny?

Produktem etapu ustanowienia systemu zarządzania bezpieczeństwem informacji jest dokumentacja systemu (norma narzuca minimalną zawartość dokumentacji systemu)

Na koniec procesu ustanowienia systemu zarządzania bezpieczeństwem informacji należy uzyskać akceptację kierownictwa. Dotyczy to przede wszystkim zaakceptowania ryzyk szczątkowych oraz wydania rozporządzeń wewnętrznych dających możliwość wdrożenia ustanowionego systemu. Zaangażowanie kierownictwa w zarządzanie bezpieczeństwem informacji jest z punktu widzenia normy tak ważne, że poświęcono temu osobny rozdział (druga część normy – rozdział 5 „Odpowiedzialność kierownictwa”).

5.3. Wykonuj: Wdrożenie i eksploatacja ISMS

Na tym etapie naturalnie należy wdrożyć zabezpieczenia wybrane na etapie ustanawiania ISMS. Przede wszystkim należy jednak wdrożyć procedury zapewniające sprawne działania całego systemu zarządzania bezpieczeństwem informacji, a więc: procedury związane z zarządzaniem ryzykiem, procedury zarządzania eksploatacją i zasobami oraz procedury i zabezpieczenia zdolne do jak najszybszego wykrycia incydentów związanych z naruszeniem bezpieczeństwa i podjęcia reakcji. Bardzo ważnym elementem wdrażania systemu zarządzania bezpieczeństwem informacji są szkolenia zarówno dotyczące wdrażanych procedur jak i szkolenia uświadamiające obejmujące całość personelu.

5.4. Sprawdź: Monitorowanie i przegląd ISMS

Bardzo ważną cechą systemu zarządzania bezpieczeństwem informacji wg BS 7799 jest zdolność do samodoskonalenia. Żeby to osiągnąć, w system muszą być wbudowane mechanizmy reagowania na błędy systemu i incydenty związane z bezpieczeństwem, oraz procedury okresowych przeglądów ISMS. Proces reagowania na błędy i incydenty jest wykonywany jeśli taka sytuacja zaistnieje. Tak więc w tym wypadku ciężko jest tu mówić o jakimś etapie, który ma początek i koniec. Natomiast okresowo (w zdefiniowanych odstępach czasu) należy dokonywać przeglądów ISMS czyli:

- Przeglądów efektywności ISMS – zgodnie z przyjętymi celami wdrożenia ISMS, można przy tym wziąć pod uwagę wyniki audytów zewnętrznych i wewnętrznych, informacje powstające w trakcie obsługi incydentów, sugestie dotyczące modyfikacji ISMS pochodzące od pracowników, itp.

- Przeglądów ryzyka akceptowalnego. Każda instytucja zmienia się w czasie. Zmienia się także jej otoczenie (np. technologia). W związku z tym założenia co do akceptowalnego ryzyka muszą być okresowo weryfikowane i w razie potrzeby modyfikowane.
- Audytów wewnętrznych ISMS. Czyli sprawdzenie całości systemu zarządzania bezpieczeństwem informacji według założeń BS 7799.
- Przeglądów ISMS realizowanych przez kierownictwo.

5.5. Działaj: Utrzymanie i doskonalenie ISMS

Procedury reagowania na błędy, incydenty oraz niezgodności wykryte na drodze przeglądów muszą skutkować podjęciem działań korygujących lub prewencyjnych. Procedury działań korygujących powinny również być udokumentowane. Poza działaniami korygującymi, w miarę możliwości powinny być również podjęte działania prewencyjne w celu ochrony przed powstaniem niezgodności w przyszłości. Przykładowo: Jeśli coroczny audyt wewnętrzny wykazał dużo niezgodności to należy rozważyć częstsze przeglądy bezpieczeństwa.

6. Podsumowanie

Jak widać procesy „Sprawdź” i „Działaj” są w praktyce wynikiem zastosowania procedur spisanych na etapie „Planuj” i wdrożonych na etapie „Wykonuj”. Dlatego też najistotniejszym elementem systemu bezpieczeństwa jest jego dokumentacja opracowana na pierwszym etapie. Zawiera ona zarówno działania związane z wdrożeniem zabezpieczeń jak i procedury kontroli i procedury zmierzające do podjęcia działań korygujących.

Na koniec chciałbym zaznaczyć że norma to nie wszystko. Budując system zarządzania bezpieczeństwem informacji należy zachować zdrowy rozsądek. Przede wszystkim na etapie planowania należy zwrócić baczną uwagę na biznesowe aspekty działania firmy. System zarządzania bezpieczeństwem informacji nie może stanowić kuli u nogi w codziennej działalności firmy. Musi pomagać a nie przeszkadzać. Dlatego też rozważając budowę systemu zarządzania bezpieczeństwem informacji należy stosować podejście zindywidualizowane, dostosowane do konkretnej instytucji a nie podejście szablonowe. Jeśli korzysta się z zewnętrznych konsultantów, to należy dać im szansę „nauczenia się” firmy, poznania najważniejszych procesów i celów biznesowych. Wszystkie osoby zaangażowane w tworzenie systemu zarządzania bezpieczeństwem, również zespół wewnętrzny powinny przyjąć zasadę nadrzędną: „po pierwsze – nie szkodzić”.