PRIANTO

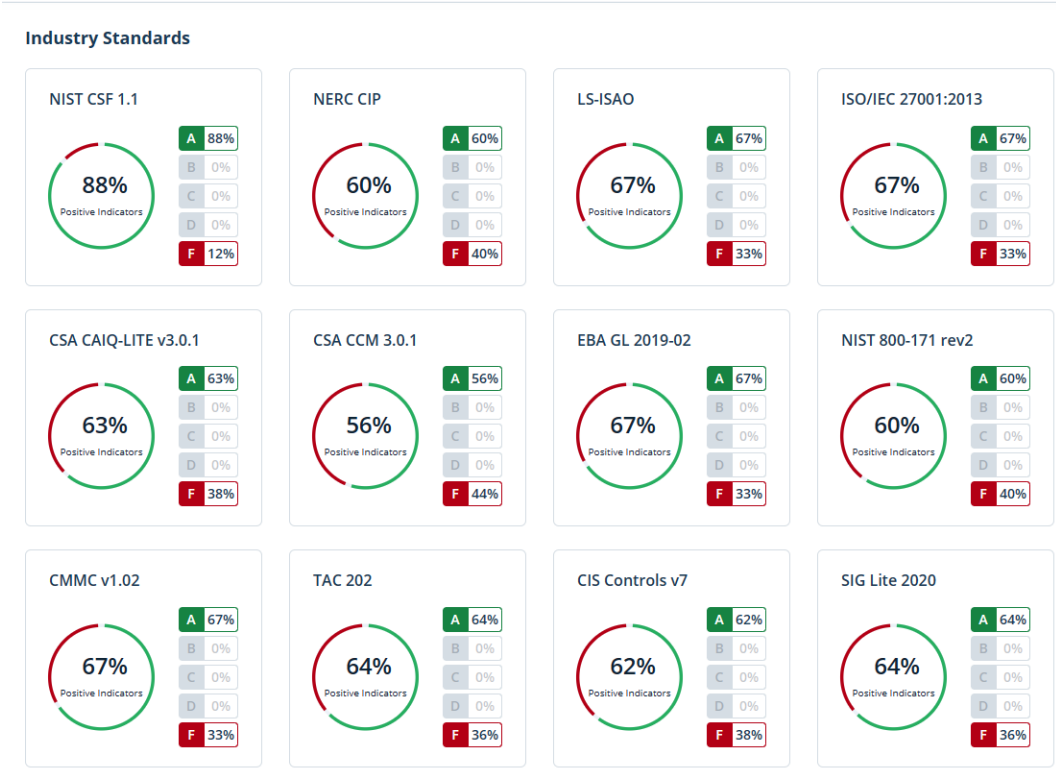
Zarządzanie ryzykiem cybernetycznym stron trzecich

Czym jest zarządzanie zgodnością ?

Zarządzanie zgodnością polega na regularnym monitorowaniu i ocenie systemów oraz sieci w celu zapewnienia ich zgodności z normami bezpieczeństwa, standardami branżowymi oraz zasadami i wymaganiami regulacyjnymi korporacyjnymi. Ryzyko braku zgodności to prawdopodobieństwo, że korporacja poniesie kary prawne lub finansowe, zakłócenia operacyjne lub utratę reputacji z powodu naruszeń przepisów i standardów branżowych. Dzieje się tak, gdy organizacja nie przestrzega obowiązujących zasad i wymogów regulacyjnych, w tym związanych z przeciwdziałaniem praniu pieniędzy, prywatnością danych, praktykami pracowniczymi i ochroną środowiska.

Kluczowe elementy skutecznego zarządzania zgodnością

Platforma **RiskRecon** firmy **Mastercard** może pomóc Twojej firmie w stworzeniu i utrzymaniu skutecznych ram zgodności, które umożliwią Ci uzyskanie przewagi konkurencyjnej. Obejmuje to przeprowadzenie kompleksowej oceny ryzyka związanego ze zgodnością w celu wykrycia potencjalnych zagrożeń dla Twojej firmy i opracowania odpowiednich środków zaradczych zgodnie z daną normą.



Dystrybucja: **Prianto Polska Sp. z o.o.** Trzcinowa 27, 02-446 Warszawa www.prianto.pl

riskrecon
mastercard

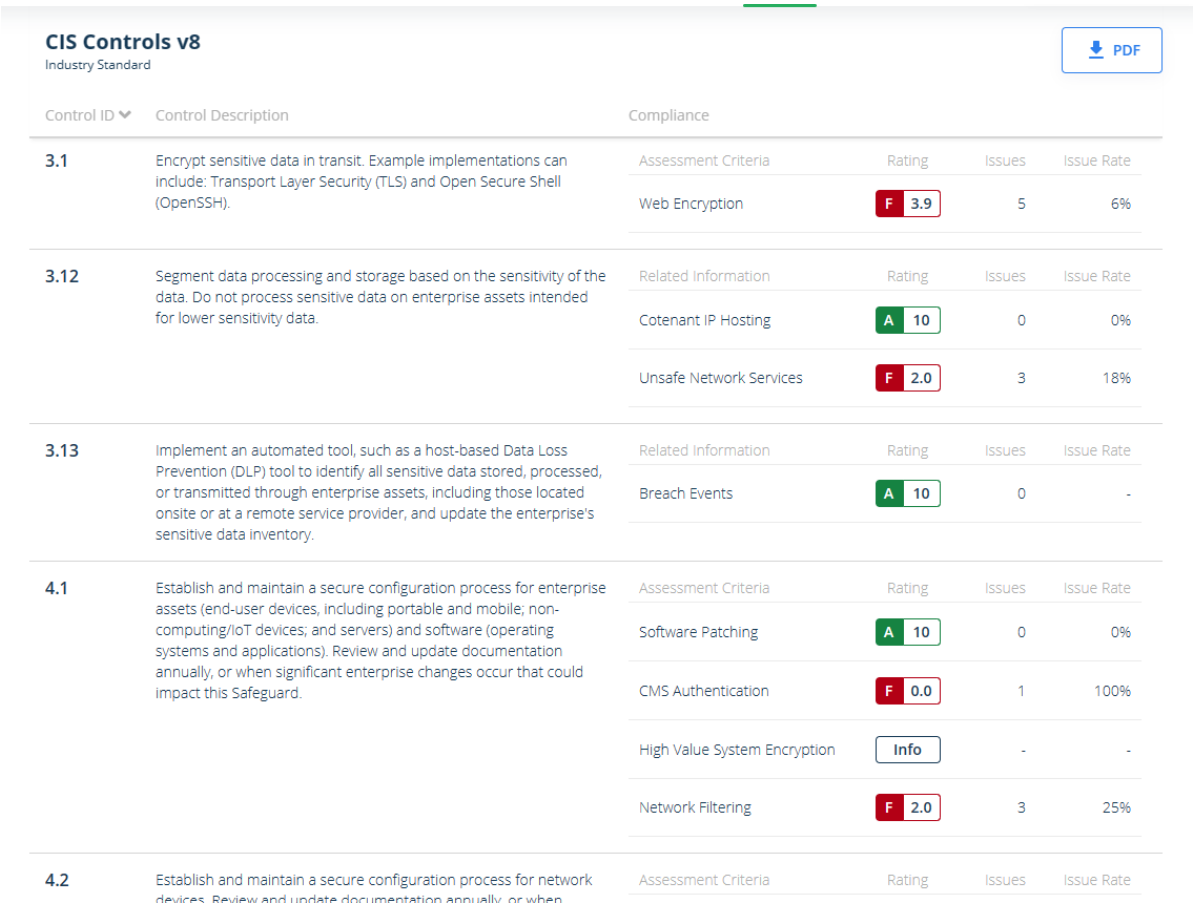
Wyzwania i typowe pułapki

- *Stale zmieniające się krajobrazy zgodności i bezpieczeństwa:* Zagrożenia cybernetyczne i problemy ze zgodnością szybko ewoluują, co wymaga szybkiej reakcji na nowe zagrożenia i zmieniające się przepisy.
- *Zarządzanie dostawcami:* Często jest to dość trudne, ponieważ nie można monitorować zarządzania dostawcami w czasie rzeczywistym. W związku z tym wcześniejsze badania na początku relacji z firmą zewnętrzną i dostawcami są koniecznością, aby zapewnić zaspokojenie potrzeb Twojej organizacji. Jednak upewnienie się, że dostawca robi to, co powinien, staje się bardziej zadaniowe. Oczywiste jest, że nie możesz zarządzać procesami swoich zewnętrznych dostawców usług. To, co możesz zrobić, to powiadomić wszystkich zewnętrznych dostawców usług, że pracujesz zgodnie ze swoimi standardami zgodności, poprosić ich o pełne dostosowanie się do nich i przedstawić dowód, że to robisz.
- *Duże zespoły i środowiska:* Skomplikowana infrastruktura i duże zespoły mogą zakłócić koordynację w całej organizacji. Złożoność infrastruktury i systemu może zwiększyć koszty naruszeń danych.
- *Ocena potencjalnego ryzyka:* Zdarzenia ryzyka w łańcuchu dostaw mogą zagrozić organizacji i jej klientom. Niemniej jednak zdarzenie ryzykowne może wystąpić w dowolnym punkcie łańcucha dostaw, zagrażając wszystkiemu. Podstawowym elementem zarządzania ryzykiem braku zgodności jest identyfikacja i ocena ryzyk oraz działania naprawcze, które należy podjąć.
- *Środowiska rozproszone na różnych platformach:* W miarę jak systemy i infrastruktury stają się coraz bardziej rozproszone na platformach chmurowych i lokalnych, uzyskanie pełnego przeglądu środowiska oraz wszelkich zagrożeń i luk w zabezpieczeniach, które mogą być obecne, staje się zniechęcające.
- *Brak ustrukturyzowanego zarządzania:* Chociaż przedsiębiorstwa mogą dysponować istotnymi mechanizmami kontroli, często potrzebują ram ryzyka i ustrukturyzowanego zarządzania, które potwierdzają zakres ryzyka oraz dostosowanie ich kontroli i procesów do wymogów regulacyjnych. Brak udokumentowanych i ustrukturyzowanych procesów może skutkować brakiem racjonalizacji w zakresie architektury i kontroli bezpieczeństwa cybernetycznego firmy, potencjalnymi martwymi punktami ekspozycji i rezygnacją w odpowiadaniu na pytania regulacyjne lub pytania interesariuszy. Dyrektorzy ds. informatyki i inni specjaliści ds. zgodności powinni wspierać ogólną strukturę zarządzania, która łączy zespoły ds. architektury korporacyjnej, bezpieczeństwa informacji, infrastruktury i aplikacji w sposób, który osadza zarządzanie ryzykiem braku zgodności z dostarczaniem technologii już na etapie projektowania.
- *Przypisywanie poziomu ryzyka:* Obejmuje to przegląd sprawozdań organów regulacyjnych i zarządzających. Identyfikuje również podsumowania krytycznych danych. Przypisanie poziomu ryzyka do każdego potencjalnego ryzyka lub szansy pomaga organizacjom ustalić priorytety tego, czym należy się zająć. Aby uzyskać

zgodność, firma musi ocenić swoje czynniki ryzyka pod kątem nowych przepisów i regulacji. Po tej ocenie firma może stworzyć podejście, które zapewni zgodność z przepisami. Organizacje mogą monitorować zagrożenia w dynamicznie zmieniających się środowiskach dzięki odpowiedniemu zarządzaniu ryzykiem stron trzecich, zgodności z przepisami i zgodności z umowami.

Doraźne wsparcie Riskrecon Mastercard - przykład CIS Security Controls

CIS Critical Security Controls to zestaw priorytetowych, dobrze sprawdzonych i skutecznych działań obronnych, które można podjąć, aby zapobiec najczęstszym cyberatakom. Struktura składa się z 18 kontrolek, od podstawowych po organizacyjne. Te mechanizmy kontroli ułatwiają wykonywanie różnych zadań, takich jak inwentaryzacja i kontrola zasobów, bezpieczne zarządzanie konfiguracją, ocena luk w zabezpieczeniach i reagowanie na zdarzenia.



CIS Controls v8
Industry Standard

PDF

Control ID	Control Description	Compliance			
3.1	Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).	Assessment Criteria	Rating	Issues	Issue Rate
		Web Encryption	F 3.9	5	6%
3.12	Segment data processing and storage based on the sensitivity of the data. Do not process sensitive data on enterprise assets intended for lower sensitivity data.	Related Information	Rating	Issues	Issue Rate
		Cotenant IP Hosting	A 10	0	0%
		Unsafe Network Services	F 2.0	3	18%
3.13	Implement an automated tool, such as a host-based Data Loss Prevention (DLP) tool to identify all sensitive data stored, processed, or transmitted through enterprise assets, including those located onsite or at a remote service provider, and update the enterprise's sensitive data inventory.	Related Information	Rating	Issues	Issue Rate
		Breach Events	A 10	0	-
4.1	Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile; non-computing/IoT devices; and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	Assessment Criteria	Rating	Issues	Issue Rate
		Software Patching	A 10	0	0%
		CMS Authentication	F 0.0	1	100%
		High Value System Encryption	Info	-	-
		Network Filtering	F 2.0	3	25%
4.2	Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when	Assessment Criteria	Rating	Issues	Issue Rate

Wdrożenie ram przewidzianych w mechanizmach kontroli CIS może być trudnym zadaniem. Wstępna inwentaryzacja i kontrola zasobów oprogramowania może okazać się rozległa, wymagająca skrupulatnego katalogowania zasobów cyfrowych. Może być

potrzebna pomoc w rozróżnieniu między niezbędnym oprogramowaniem a nadmiarowymi aplikacjami, co utrudnia opracowanie kompleksowej inwentaryzacji zasobów. Dzięki rozwiązaniu Riscrecon Mastercard jesteśmy w stanie określić obecny stopień zgodności ze standardem oraz odpowiednio zmierzyć wskaźniki ryzyka dla każdego z punktów CIS, jednoznacznie informując o działaniach wymaganych do podjęcia celem

Autoryzowany Partner

Dystrybucja: **Prianto Polska Sp. z o.o.** Trzcinowa 27, 02-446 Warszawa www.prianto.pl

riskrecon
mastercard