MATERIAŁY OPRACOWANE PRZEZ
Michał Ligęza, Jakub Marszałek
W RAMACH
Bezpieczeństwo Systemów Informatycznych, ćwiczenia projektowe,
Informatyka Techniczna, stopień II, niestacjonarne, WIMiIP AGH

Audyt wewnętrznego rozwiązania developerskiego wspierającego pracę programistyczną dla rozwiązania Autodesk

Michał Ligęza, Jakub Marszałek
Bezpieczeństwo Systemów Informatycznych
Informatyka Techniczna, stopień II, niestacjonarne
2020/2021

MATERIAŁY OPRACOWANE PRZEZ
Michał Ligęza, Jakub Marszałek
W RAMACH
Bezpieczeństwo Systemów Informatycznych, ćwiczenia projektowe,
Informatyka Techniczna, stopień II, niestacjonarne, WIMiIP AGH

1. Metodologia

Jako podstawę do audytu wykorzystano standardowy formularz *Enterprise Cloud Oversight Service (ECOS)* Assessment udostępniany przez *Virginia Information Technologies Agency*, który został uzupełniony przez jednego z pracowników firmy, i jednocześnie członka grupy projektowej, za zgodą władz firmy. Ze względu na komercyjne zastosowanie audytowanego rozwiązania oraz istnienie chronionych prawnie informacji objętych poufnością, audyt rozwiązania został przeprowadzony w granicach nie naruszających praw i bezpieczeństwa rozwiązania i firmy. Podejście zostało potwierdzone z prowadzącym zajęcia. Niniejszy dokument zawiera opis rozwiązania, podsumowanie zabezpieczeń, wnioski oraz rekomendacje. Przy każdym punkcie który odwołuje się do formularza ECOS, w nawiasach podawane są identyfikatory z kolumny „NIST control" formularza.

Przyjęty punkt audytowania na poziomie „enterprise" przerasta obecne działanie rozwiązania, jednak uznano za stosowne zastosować tak wymagające kryteria oceny ze względu na plany potencjalnego rozwoju rozwiązania w celu ustandaryzowania i przekształcenia w wewnętrzny produkt.

2. Opis rozwiązania

Audytowane rozwiązanie jest zespołem wewnętrznych aplikacji, działających jako dopełnienie środowiska programistycznego dla produktu Autodesk. Różne jego komponenty mają różne funkcje, w tym: automatycznego budowanie środowiska do testów oprogramowania, lub przeprowadzania porównań modeli 3D używając zaawansowanych obliczeń wymagających użycia GPU. Głównym celem rozwiązania jest usprawnienie procesu tworzenia i testowania kodu, przez przeniesienie testów i wymagających obliczeń do chmury.

Audytowane rozwiązanie jest rozwiązaniem chmurowym do wewnętrznego użytku zespołu developerskiego (poniżej 10 osób), udostępniane jako prywatna wewnętrzna chmura. Rozwiązanie jest dostępne wyłącznie z sieci firmowej, a dostęp z Internetu nie jest możliwy (EC-1, EC-2). Rozwiązanie jest wykorzystywane przez niewielki zespół developerów oraz testerów. Podstawą rozwiązania jest Autodesk Entertainment Creation Suite[1], usługa dostarczana przez Autodesk, która w tym szczególnym przypadku działa w oparciu o system CentOS połączony tunelowaniem z siecią firmową. Połączenie z rozwiązaniem odbywa się poprzez API – zależnie od funkcji, jest to REST API (tworzenie testów) lub SOAP API (analiza modeli 3D w oparciu o obliczenia GPU).

[1] https://knowledge.autodesk.com/support/maya/learn-explore/caas/simplecontent/content/entertainment-creation-suites-2020-release-notes.html

3. Standardy procedur oraz procesy bezpieczeństwa

3.1. Kontrola dostępu

Dostęp do rozwiązania jest kontrolowany; polityki i procedury kontroli dostępu są wdrożone oraz są aktualizowane corocznie lub w wyniku potrzeb wynikających ze zmian rozwiązania lub zmian wymogów prawnych (AC-1). Rozwiązanie nie posiada identyfikacji użytkowników; przykładem szczegółowym jest brak przyporządkowania wywoływanych zapytań do użytkowników (AC-2, pyt. 1) czy brak kont administratorów (AC-2, pyt.2). Istnieją zaimplementowane metody dostępu do kodu źródłowego (AC-2, pyt. 3), który jest udostępniany tylko po odpowiedniej zgodzie i zgodnie z zasadą *need-to-know*.

Istnieją wdrożone procedury odwołania dostępu, będące częścią ogólnych procedur firmy. W przypadku odejścia z firmy lub zwolnienia, pracownik automatycznie traci dostęp do sieci firmowej, co oznacza jednocześnie utratę jakiegokolwiek dostępu do rozwiązania (AC-2, pyt. 5). Rozwiązanie jest dostępne tylko dla pracowników, dlatego nie istnieje proces kontroli dostępu dla najemców (AC-2, pyt. 8, AC-6). Rozwiązanie nie jest dostępne na rynku (AC-2, pyt. 4 i 6).

Rozwiązanie nie używa systemu kont, jednak do jego używania w praktyce konieczne jest konto Autodesk, pozwalające na interpretację wyników. Samo rozwiązanie nie tworzy i nie przechowuje własnych użytkowników, jednocześnie nie wymagając certyfikacji / szkoleń z jego używania (AC-2, pyt. 7, 9 - 12). Wszelkie istniejące polityki użytkowania są częścią rozwiązania Autodesk, i nie są badane w ramach tego audytu.

Dostęp do sieci firmowej oraz do rozwiązania posiadają jedynie pracownicy firmy po uprzedniej autoryzacji ze strony przedstawiciela kierownictwa firmy na podstawie odpowiednich procedur (IA-1, pyt.1). Procedury dostępu są regularnie aktualizowane (IA-1, pyt. 2)

3.2. Zarządzanie konfiguracją

Kod źródłowy jest zabezpieczony. Wyłącznie pracownicy którzy otrzymali dostęp mogą mieć wgląd i na nim pracować. Dostęp do serwerów na których działa kod także mają ograniczony dostęp. W praktyce jedynie grupa wyznaczonych administratorów może pracować z kodem lub konfiguracją serwerów (AC-5). Proces tworzenia aplikacji skonstruowany jest w taki sposób, by każda część kodu koniecznego do developmentu i debuggowania została usunięta (CM-1, pyt. 4). Procedury zabezpieczające system przed instalowaniem niepożądanego oprogramowania lub sprzętu w sieci są częścią standardowych procedur firmy oraz kontroli dostępu do rozwiązania (CM-2, CM-2-COV, CM-3, CM-3-COV, CM-7, pyt.2).

3.2.1. Dokumentacja

Jest prowadzona dedykowana dokumentacja rozwiązania w formie plików read-me zapisywanych wraz z kodem w systemie git (CM-1, pyt. 1-2). Zastosowanie mają standardowe procedury firmy dotyczące śledzenia błędów i podatności bezpieczeństwa (CM-1, pyt. 3).

3.3. Zabezpieczenie prawne

Każdy użytkownik jako pracownik przechodzi szkolenie dotyczące swojej roli oraz polityki i standardów bezpieczeństwa (AT-1), które zostaje potwierdzone podpisaniem oświadczenia o ukończeniu szkolenia i stosowaniu się do wszelkich zasad bezpieczeństwa (AT-2). Pracownicy w ramach umowy z Autodesk podpisują umowę o poufności (non-disclosure agreement – NDA), która dotyczy także audytowanego rozwiązania (AT-2-COV). Szkolenia bezpieczeństwa są przeprowadzane regularnie, wraz z odpowiednim oświadczeniem o ukończeniu szkolenia.

3.3.1. Etykietowanie danych

Dane nie są etykietowane. Nie został rozpoznany żaden sposób oceny danych z punktu widzenia bezpieczeństwa i ich etykietowania (AC-3).

3.4. Procedury audytowe

Badane rozwiązanie nie posiada rozpoznanego procesu audytowego (AU-1, pyt. 1-2). Autodesk posiada własne procedury audytowe które nie będą rozważane w ramach niniejszego dokumentu. Rozwiązanie nie posiada procedury oceny przez zewnętrzną stronę (AU-1, pyt. 3-7).

Rozwiązanie nie pozwala na śledzenie wszystkich zmian i zachodzących wydarzeń w systemie (AU-2, pyt. 1), aczkolwiek jest w stanie śledzić wydarzenia administracyjne (AU-2, pyt. 2). Każda proponowania zmiana w rozwiązaniu przechodzi analizę / code review (CM-2, CM-2-COV, CM-3, CM-3-COV, CM-7, pyt.3).

Nie istnieją dedykowane procedury oceny ryzyka w kontekście infrastruktury, ani w kontekście danych i ich zabezpieczenia (CA-1, CA-3, CA-7). Zastosowanie mają standardowe procedury firmy oraz procedury rozwiązania Autodesk.

Wyniki audytów i skanów bezpieczeństwa i podatności nie są udostępniane zewnętrznie (SI-2, RA-5, RA-5-COV, pyt. 4).

3.5. Procedury na wypadek incydentów

W wypadku wystąpienia incydentów bezpieczeństwa, zastosowanie mają ogólne przepisy, polityki i procedury firmy. Nie istnieją dedykowane procedury zarządzania incydentami (IR-4, IR-5, IR-6). Aktualizacje poprawiające bezpieczeństwo mogą być wdrażane bardzo szybko (SI-2, RA-5, RA-5-COV, pyt. 5).

3.6. Archiwizowanie danych

Rozwiązanie nie posiada procedur archiwizacji danych (AU-11).

4. Bezpieczeństwo infrastruktury

4.1. Bezpieczeństwo fizyczne

Dostęp do sieci firmowej oraz do rozwiązania posiadają jedynie pracownicy firmy po uprzedniej autoryzacji ze strony przedstawiciela kierownictwa firmy na podstawie odpowiednich procedur (IA-1, pyt.1). Fizyczny dostęp do elementów rozwiązania oraz do wiedzy na jego temat jest ograniczony na podstawie roli i pozycji (PE-2(1), PE-2(3), PE-3 pyt. 1). Przestrzenie dostępnie dla nie-pracowników są fizycznie odizolowane od przestrzeni w którym możliwy jest dostęp do rozwiązania (PE-3, pyt. 2).

4.2. Bezpieczeństwo środowiskowe

Z racji lokalnego zastosowania, rozwiązanie nie posiada kopii bezpieczeństwa w różnych regionach geograficznych (CP-2, CP4, CP-6, CP-7, CP-9, CP-9-COV, CP-10, SA-9-COV, pyt. 1). Działają serwery zapasowe, a rozwiązanie posiada kopie zapasowe (CP-2, CP4, CP-6, CP-7, CP-9, CP-9-COV, CP-10, SA-9-COV, pyt. 3, pyt. 6). Użytkownicy nie mają wpływu na geo-lokalizację serwerów rozwiązania, jednak region działania rozwiązania jest znany administratorom (PE-18-COV, SA-9-COV-1, pyt. 1-2). Dane nie są przemieszczanie między regionami (PE-18-COV, SA-9-COV-1, pyt. 3).

4.3. Nadzorowanie stanu rozwiązania

Istnieje sposób na monitorowanie stanu żywotności (health check) rozwiązania, natomiast nie jest to monitoring stały (CA-1, CA-3, CA-7). Jest wdrożony sposób ciągłego monitorowania zgodności rozwiązania z zasadami bezpieczeństwa (CM-2, CM-2-COV, CM-3, CM-3-COV, CM-7, pyt.1). Monitorowanie warstwy aplikacji odbywa się raz na kilka miesięcy (CM-2, CM-2-COV, CM-3, CM-3-COV, CM-7, pyt.2).

Aktualizacje systemu operacyjnego CentOS maszyn odbywa się raz na kilka miesięcy (SI-2, RA-5, RA-5-COV, pyt. 3).

Nadzorowanie stanu sieci odbywa się zgodnie ze standardami firmy. Nadzorowanie usługi chmurowej oraz jej połączenia z siecią firmową spoczywa na dostawcy usług chmurowych (SI-2, RA-5, RA-5-COV, pyt. 1).

4.4. Dostępność

Nie jest badana dostępność rozwiązania, jednak z rozmowy przeprowadzonej z pracownikiem firmy wynika że rozwiązanie nie jest stale dostępne i posiada tendencję do odmawiania współpracy. Przez brak monitorowania dostępności nie można dokładnie ocenić dostępności, jednak można przyjąć że mieści się ono między 50 a 95% dostępności, ponieważ poniżej 50% dostępności nie zostałoby opisane jako „czasem nie działające" tylko „zwykle/ często nie działające", natomiast przy dostępności powyżej 95% problemy z rozwiązaniem nie byłyby aż tak widoczne i zauważalne.

4.5. Działanie awaryjne oraz przywracanie systemu

Rozwiązanie nie posiada procedur działania awaryjnego (CP-2, CP4, CP-6, CP-7, CP-9, CP-9-COV, CP-10, SA-9-COV, pyt. 2), jednakże istnieją procedury tworzenia kopii zapasowych oraz przywracania danych, a także utrzymywane są serwery zapasowe (CP-2, CP4, CP-6, CP-7, CP-9, CP-9-COV, CP-10, SA-9-COV, pyt. 4).

4.6. Interoperacyjność i możliwości dostosowania

Istniejące API są opisane w dokumentacji i nie są publiczne udostępnianie (CHFS -1). Dane przechowywane są w formacie JSON (CHFS -2). Inne firmy nie mogą obecnie korzystać z rozwiązania (CHFS -3). Nie istnieje możliwość

migracji danych do ani z rozwiązania (CHFS -4). Do komunikacji wykorzystywane są ogólnie przyjęte bezpieczne protokoły sieciowe, a ich dokumentacja nie jest udostępniana na zewnątrz (CHFS -5, CHFS -6). Wirtualizacja wymaga niemodyfikowanego systemu wraz z kilkoma wymaganymi instalacjami, m.in. git i Docker (CHFS-7, CHFS-8). Rozwiązanie nie stosuje standardowych frameworków bezpieczeństwa ani metodologii audytowania oraz testowania (CHFS -9, CHFS -10).

5. Bezpieczeństwo oprogramowania

5.1. Spójność danych

Firma zapewnia używanie ogólnie przyjętych standardów ochrony przed malware w tym mechanizmów detekcji opartych na sygnaturach (SI-3, SI-3-COV, pyt. 1). Ochrona przed malware jest centralnie zarządzania i regularnie automatycznie aktualizowana (SI-3, SI-3-COV, pyt. 2).

5.2. Przesyłanie danych

Przesyłanie danych w rozwiązaniu nie wykorzystuje otwartych technologii szyfrowania (AES, TLS), ponieważ nie jest dostępne publicznie (AC-2, pyt. 8). Istnieją zabezpieczenia zapory oraz przepływu danych wewnątrz sieci, a poprawność danych jest sprawdzana przed ich przekazaniem dalej (SC-7, pyt. 1).

Wprowadzone jest ograniczenie ilości istniejących maszyn przeprowadzających testy, a rozwiązanie nie przyjmuje kolejnych zapytań, jeśli wszystkie maszyny są zajęte.

5.3. Dostęp do danych

Wdrożone procedury dostępu do danych nie opierają się na zasadzie *need-to-know*. Mimo ograniczonego bezpośredniego dostępu, są one także przekazywane dalej w formie, w której inni pracownicy mogą mieć do nich dostęp (AC-3).

Audytowane rozwiązanie nie posiada metody definiowania wymogów do haseł, blokowania logowania, czy dodatkowych polityk bezpieczeństwa (AC-7) (IA-2, IA-2-COV, IA-5, pyt. 6-8), z racji że rozwiązanie może być używane jedynie razem z rozwiązaniami udostępnionymi przez Autodesk, które posiada własne zabezpieczenia i polityki w tym obszarze.

Systemy autoryzacji opierają się o rozwiązanie Autodesk i nie są bezpośrednio zaimplementowane do audytowanego rozwiązania. Autodesk posiada zaimplementowane standardy federacji tożsamości (SAML)[2] oraz integracji logowania (SSO)[3] (IA-2, IA-2-COV, IA-5, pyt. 1-3). Audytowane rozwiązanie nie posiada opcji MFA; rozwiązanie Autodesk posiada możliwość wykorzystania 2FA[4].

Rozwiązanie zapewnia detekcję naruszenia bezpieczeństwa, blokując wykonanie akcji przed sprawdzeniem przez zaporę (SC-7, pyt. 2).

5.4. Przechowywanie danych

Dane produkowane jako wynik działania rozwiązania nie są szyfrowane ani w przekazywaniu, ani w przechowywaniu (SC-1, SC-8, SC-8-COV, SC-23, SC-28, pyt.1-2, pyt. 4-5)(SC-12 SC-12-COV, SC-13, SC-13-COV, pyt 1-4). Danie nie są przemieszczane pomiędzy sieciami / maszynami wirtualnymi (SC-1, SC-8, SC-8-COV, SC-23, SC-28, pyt. 3). Dane produkcyjne nie są przekazywane ani replikowane na innych środowiskach; istnieją oddzielne serwery, między którymi nie następuje żadna wymiana danych (SA-11).

[2] https://knowledge.autodesk.com/search-result/caas/CloudHelp/cloudhelp/ENU/SSOGUIDE-Okta-Guide/files/SSOGUIDE-Okta-Guide-About-Implementing-SSO-html-html.html
[3] https://knowledge.autodesk.com/search-result/caas/CloudHelp/cloudhelp/ENU/SSOGUIDE-Okta-Guide/files/SSOGUIDE-Okta-Guide-About-Single-Sign-on-SSO-html-html.html
[4] https://knowledge.autodesk.com/customer-service/account-management/account-profile/account-security/two-step-verification

5.5. Raportowanie i automatyczne audytowanie

Rozwiązanie nie posiada możliwości przeprowadzania automatycznych raportów lub testów bezpieczeństwa; nie posiada także możliwości scentralizowanego przeglądania, analizowania i oceniania wydarzeń w systemie; nie istnieje możliwość powiadomienia administratorów o podejrzanym zachowaniu (AU-6).

5.6. Procedury wycofywania przestarzałych danych

Rozwiązanie posiada zaimplementowane skrypty które usuwają przestarzałe dane (MP-6, MP-6-COV, pyt. 1).

6. Ocena: najczęstsze zagrożenia rozwiązań chmurowych

Chcąc ocenić rozwiązanie, prócz kontekstu oraz zebranych danych, należy ocenić także ocenić czy rozwiązanie wychodzi naprzeciw najczęstszym zagrożeniom rozwiązań chmurowych. Opierając się na liście prezentowanej przez OWASP[5] [6], sprawdzono podatność na najczęstsze ryzyka, oraz oceniono dane aspekty w kontekście potencjalnego rozwoju i rozbudowania grupy docelowej.

6.1. Odpowiedzialność i własność danych

Rozwiązanie jest używane wewnętrznie i nie przetwarza danych wrażliwych lub osobowych. Firma jest właścicielem całego rozwiązania jak i przetwarzanych i uzyskiwanych danych. Odpowiedzialność za rozwiązanie spoczywa na pracownikach firmy, którzy posiadają dostęp do rozwiązania. W obecnej sytuacji należy uznać że ten aspekt rozwiązania można ocenić pozytywnie.

W kontekście rozwoju, jeżeli rozwiązanie byłoby skierowane wyłącznie do pracowników firmy, dalej firma powinna pozostać właścicielem danych, jednak wymagałoby to werbalizacji zasad w formie regulaminu i informacji o własności danych. Natomiast jeżeli rozwiązanie miałoby być oferowane jako produkt dla zewnętrznych klientów, wymagałoby to sprecyzowania rozwiązania oraz stworzenia matrycy odpowiedzialności i własności.

6.2. Federacyjna identyfikacja użytkowników

Rozwiązanie jest wykorzystywane przez mały zespół, w obecnym stanie nie potrzebuje więc federacyjnej identyfikacji użytkowników.

Jednocześnie, w kontekście ewentualnego rozrostu, można oprzeć identyfikację użytkowników na rozwiązaniach używanych w Autodesk.

6.3. Zgodność z przepisami

Rozwiązanie nie jest dostępne publicznie czy udostępnianie wewnątrz firmy; przez swoje obecne zastosowanie służy wyłącznie do wspomagania pracy deweloperów, przez co nie dotyczą go przepisy o ofertach, marketingu i obsłudze klienta. Rozwiązanie nie przetwarza danych osobowych. W kontekście zgodności z przepisami, należy uznać że ten aspekt nie dotyczy audytowanego rozwiązania.

W przypadku rozwoju rozwiązania w kierunku produktu wewnętrznego lub zewnętrznego, należałoby zapewnić zgodność stanu przyszłego z istniejącymi wymogami prawnymi.

6.4. Ciągłość biznesu i odporność

Rozwiązanie nie jest krytyczne biznesowo, a z racji swojej funkcji jako narzędzie deweloperskie skierowane do małej grupy, nie wymaga wysokiej stabilności i odporności.

W kontekście rozwojowym, koniecznym krokiem w celu zapewnienia ciągłości biznesowej byłoby wprowadzenie monitorowania infrastruktury i rozwiązania, a także zbadanie i ewentualne ulepszenie zdolności autoregeneracji systemu.

---

[5] https://www.packetlabs.net/cloud-security/

[6] https://owasp.org/www-pdf-archive/Cloud-Top10-Security-Risks.pdf

6.5. Prywatność

Obecnie rozwiązanie nie przetwarza danych osobowych lub kont użytkowników, więc ten aspekt go nie dotyczy.

W kontekście rozwoju aplikacji, koniecznym jest wprowadzenie identyfikacji użytkowników oraz wprowadzenie takiego sposobu prezentacji danych który zapewni wymagany poziom prywatności.

6.6. Integracja usług i danych

Rozwiązanie istnieje jako wsparcie i koniecznym jest rozwiązanie Autodesk które pozwoli przygotować wejście do systemu. Dzięki istnieniu API, integracja rozwiązania z innymi usługami jest przygotowana na potencjalne integracje.

6.7. Obsługa wielu najemców i bezpieczeństwo fizyczne

Obecnie nie istnieje i nie jest konieczna obsługa wielu najemców. Bezpieczeństwo fizyczne jest zapewnione przez dostęp wyłącznie z sieci firmowej oraz przez powierzenie odpowiedzialności dostawcy usług chmurowych.

Dalszy potencjalny rozwój w kierunku produktu wewnętrznego nie wymagałby zmian, jednak rozwój w kierunku produktu zewnętrznego wymagałby zaplanowania stanu przyszłego w formie umożliwiającej obsługę wielu najemców.

6.8. Analiza incydentów i wsparcie w nadzorowaniu

W obecnej sytuacji nie jest wymagana ustrukturyzowana analiza incydentów, jednak widocznym problemem jest brak rozbudowanych logów, przetrzymywanie ich wewnątrz maszyny oraz brak monitorowania działania rozwiązania. Konieczne są zmiany naprawiające ten problem.

W kontekście rozwoju, rozwiązanie wymaga zaprojektowania systemu incydentów i wsparcia monitorowania od podstaw.

6.9. Bezpieczeństwo infrastruktury

Infrastruktura jest wystarczająco zabezpieczona w kontekście obecnego użycia, jednakże w kontekście rozwoju należałoby wdrożyć procedury zarządzania infrastrukturą i konfiguracją.

6.10. Ekspozycja środowisk nieprodukcyjnych

Audytowane rozwiązanie nie posiada środowisk produkcyjnych. Dostępne środowiska są przeznaczone do celów wyłącznie deweloperskich; są one dostępne tylko z sieci wewnętrznej firmy i nie posiadają ekspozycji publicznej. Wewnątrz sieci firmowej są one dostępne, jednak nie są one promowane a informacje o nich posiadają wyłącznie członkowie zespołów: deweloperów i testerów (łącznie poniżej 10 osób). Ogólna ocena rozwiązania w kontekście ekspozycji środowisk nieprodukcyjnych jest pozytywna.

7. Ocena rozwiązania

Z punktu widzenia audytu oraz założonego poziomu, rozwiązanie nie jest w żadnym wypadku gotowe lub na drodze by uznać je za rozwiązanie klasy enterprise, jednakże wykazuje potencjał do stosunkowo łatwej poprawy bezpieczeństwa wraz ze skalą, poprzez oparcie się na rozwiązaniu Autodesk i przy odpowiednim wykorzystaniu istniejących tam zabezpieczeń oraz procesów i procedur bezpieczeństwa i wsparcia.

Oceniając rozwiązane z punktu widzenia obecnego zastosowania, tj. do wykorzystania przez małą grupę osób w ramach procesu tworzenia oprogramowania, kwestie bezpieczeństwa są zaadresowane w stopniu przeciętnym, z kilkoma obszarami wprost wymagającymi poprawy. Jednocześnie, nawet niewielki dalszy wzrost rozwiązania (przykładowo, do 20-30 osób), wymagałby zaadresowania też innych tematów, które na obecnym etapie nie są konieczne.

8. Rekomendacje

Bazując na zebranych informacjach oraz ocenie poszczególnych aspektów, zespół audytujący rekomenduje bezpośrednie działania:

- Rozbudowa funkcjonalności tworzenia logów systemu, które pozwalałyby na ocenę działania logiki aplikacji oraz monitorowania stanu rozwiązania (app health info) oraz zabezpieczało logi przed ewentualną utratą.
- Zaimplementowanie co najmniej podstawowej autentykacji użytkowników; w kontekście firmy można wykorzystać ślad sieciowy np. adres IP, prostą nazwę-hasło (oba stosunkowo łatwe do zaimplementowania) lub odwołując się do AD firmy (wymagające większego nakładu pracy).
- Ujednolicenie dostępu do różnych funkcjonalności dostępnych przez różne API

Analizując potencjalny rozwój rozwiązania i jego wzrost, koniecznym byłoby zaprojektowanie modelu w bezpieczny sposób, z uwzględnieniem możliwości wykorzystania istniejących rozwiązań bezpieczeństwa firmy (w kontekście rozwoju do produktu wewnętrznego) i/lub zabezpieczeń Autodesk (w kontekście rozwoju do produktu zewnętrznego).

9. Wnioski

Podsumowując:

- rozwiązanie jest stosowane w małej grupie i nie jest dostępne w szerszym gronie;
- rozwiązanie nie jest krytyczne z punktu widzenia biznesowego – nie przynosi bezpośrednich zysków ani nie poprawia rentowności innych działań w dużej skali
- możliwe są proste do wprowadzenia elementy które poprawią bezpieczeństwo rozwiązania.

Dodatkowym aspektem oceny rozwiązania są kwestie biznesowe. Należałoby ocenić koszty wprowadzania rozbudowanych środków bezpieczeństwa, oraz przewidywane zyski osiągane z podejmowanych działań. Na obecnym etapie wydaje się sensowne, by poprawić bezpieczeństwo przez wprowadzenie prostych zmian zgodnych z rekomendacjami.

MATERIAŁY OPRACOWANE PRZEZ
Michał Ligęza, Jakub Marszałek
W RAMACH
Bezpieczeństwo Systemów Informatycznych, ćwiczenia projektowe,
Informatyka Techniczna, stopień II, niestacjonarne, WIMiIP AGH

Appendix A: formularz ECOS

SaaS Security Control Group	NIST control	Control Specification	Assessment Question	Answer : YES	Answer : NO	Answer : N/A
Cloud Classification & Configuration	EC -1	Ensures appropriate information security guards are established.	Is the cloud solution you are proposing a Software as a Service, Platform as a Service, or Infrastructure as a Service Delivery Model?	X		
Cloud Classification & Configuration	EC - 2	Establishing, monitoring, and operating IT systems in a manner consistent with Commonwealth of Kentucky Information Security policies and standards	Are you offering Public, Private or Government cloud? Please describe the solution support model.	X		
Access Control: *Policies & Procedures*	AC-1	Develops, documents, and disseminates to all organization personnel, contractors, and service providers with a responsibility to implement access controls:	Does the provider have access control policies and procedures that are reviewed and/or updated at least annually or required due to environmental changes?	X		
Access Control - Account Management	AC-2	User access policies and procedures shall be established, and supporting business processes and technical measures implemented, for restricting user access as per defined segregation of duties to address business risks associated with a user-role conflict of interest.	Does the solution have the capability to identify and select the following types of accounts: Individual, Group, System, Service, Application, Guest/Anonymous and Temporary?		X	
			Does the provider have the capability to segment and identify administrative accounts by tenant?		X	
			Are controls in place to prevent unauthorized access to your application, program or object source code, and assure it is restricted to authorized personnel only?	X		
			Does provider document how access to tenant data is granted and approved?			X
			Is timely deprovisioning, revocation or modification of user access to the organization's systems, information assets and data implemented upon any change in status of employees, contractors, customers, business partners or involved third parties?	X		
			Do you provide tenants with documentation on how segregation of duties within proposed cloud service offering are maintained? Please provide copy of procedure(s)		X	
		Control Enhancements for Sensitive Systems Removal of Temporary/Emergency Accounts.	Does the provider or solution automatically terminate temporary and emergency accounts after a predetermined period which is not to exceed 30-days in accordance with sensitivity and risk? Please provide copy of procedure(s)		X	
			Do you provide open encryption methodologies (3.DES, AES, TLS etc.) to tenants in order for them to protect their data if it is required to move through public networks (e.g., the Internet)?		X	
			Do you require at least annual certification of entitlements for all system users and administrators (exclusive of users maintained by your tenants)?		X	
			If users are found to have inappropriate entitlements, are all remediation and certification actions recorded/documented? If different actions are taken for Admin and User Accounts, please provide information on both.	X		
		Disable Inactive Accounts	Does the provider or solution automatically disable inactive accounts after 90 consecutive days of non-use?		X	
		Inactivity logout	Does the solution logout users automatically when the session inactivity time has exceeded 30 minutes?		X	
Access Control - Access Enforcement	AC-3	The information system enforces approved authorizations for logical access to information and system resources in	Are policies and procedures established for labeling, handling and the security of data and objects that contain data?			X

		accordance with applicable access control policies.				
Access Control - Separation of Duties	AC-5	User access policies and procedures shall be established, and supporting business processes and technical measures implemented, for restricting user access as per defined segregation of duties to address business risks associated with a user-role conflict of interest.	Are controls in place to prevent unauthorized access to your application, program or object source code, and assure it is restricted to authorized personnel only? Provide documentation on controls in place to prevent unauthorized access.	X		
			Are controls in place to prevent unauthorized access to tenant application, program or object source code, and assure it is restricted to authorized personnel only? Provide documentation on controls in place to prevent unauthorized access.	X		
Access Control - Least Privilege	AC-6	The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.	Do you document how you grant and approve access to tenant data? Please procedure for doing this.		X	
			Do you have a method of aligning provider and tenant data classification methodologies for access control purposes?		X	
			Will you share user entitlement remediation and certification reports with your tenants, if inappropriate access may have been allowed to tenant data?		X	
Access Control - Unsuccessful Logon Attempts	AC-7	Enforces a limit of 3 consecutive invalid logon attempts by a user during a 15 minute period;	Do you allow tenants/customers to define password and account lockout policies for their accounts? Provide system password requirements and policies.			X
		Automatically locks the account/node for a minimum of a 30 minute period when the maximum number of unsuccessful attempts is exceeded.	Do you support password (pass phrase, minimum length, age, history, complexity) and account lockout (lockout threshold, lockout duration) policy enforcement? Please provide policies for both standard and admin accounts.			X
		Password Policy must meet or exceed current password policy defined in Commonwealth Office of Technology CIO-072 Identity and Access Management Policy.	Do you support tenant defined password complexity policies including pass phrases? Specify your password length and complexity requirements.			X
Awareness and Training - Policy and Procedures	AT-1 AT-2 AT-2-COV AT-3 AT-4	Employment agreements shall incorporate provisions and/or terms for adherence to established information governance and security policies and must be signed by newly hired or on-boarded workforce personnel (e.g., full or part-time employee or	Do you specifically train your employees regarding their specific role and the information security controls they must fulfill?	X		
			Do you document employee acknowledgment of training they have completed?	X		
			Are all personnel required to sign NDA or Confidentiality Agreements as a condition of employment to protect customer/tenant information?	X		
			Is successful and timely completion of the training program considered a prerequisite for acquiring and maintaining access to sensitive systems?	X		
			Are personnel trained and provided with customer defined awareness programs at least once a year?	X		

		contingent staff) prior to granting workforce personnel user access to corporate facilities, resources, and assets.				
Audit and Control -Audit and Accountability	AU-1	Audit plans shall be developed and maintained to address business process disruptions. Auditing plans shall focus on reviewing the effectiveness of the implementation of security operations. All audit activities must be agreed upon prior to executing any audits.	Do you produce audit assertions using a structured, industry accepted format (e.g., Cloud Audit/A6 URI Ontology, Cloud Trust, SCAP/CYBEX, GRC XML, ISACA's Cloud Computing Management Audit/Assurance Program, etc.)?			X
			Are your audits performed at least annually? if no, please describe in the comments section.			X
		Independent reviews and assessments shall be performed at least annually to ensure that the organization addresses nonconformities of established policies, standards, procedures, and compliance obligations.	Do you allow tenants to view your SOC2 Type2/ISO 27001 or similar third-party audit or certification reports?		X	
			Do you conduct network penetration tests of your cloud service infrastructure regularly as prescribed by industry best practices and guidance?		X	
			Do you conduct application penetration tests of your cloud infrastructure regularly as prescribed by industry best practices and guidance?		X	
			Are the results of the penetration tests available to tenants at their request?		X	
			Are the results of internal and external audits available to tenants at their request?		X	
Audit and Control: *Audit Events*	AU-2	An event is any observable occurrence in an organizational information system. Organizations identify audit events as those events which are significant and relevant to the security of information systems and the environments in which those systems operate in order to meet specific and ongoing audit needs.	Is the solution capable of auditing the following events? Successful and unsuccessful account logon events, account management events, object access, policy change, privilege functions, process tracking, and system events.		X	
		Audit events on Web Applications	Is the solution capable of auditing the following events, for Web applications? All administrator activity, authentication checks, authorization checks, data deletions, data access, data changes, and permission changes.	X		
Audit and Control: Audit Review, Analysis, and Reporting	AU-6	Audit Review, Analysis, and Reporting	Is the solution capable of automated mechanisms to centrally review, analyze and correlate audit and log records from multiple components of the solution to support organizational processes for investigation, alerting and response to suspicious activities? Is the information available to your tenants?		X	
Audit and Control:	AU-11		Is the solution capable of maintaining all audit records in accordance with commonwealth record retention policies found at the following URL? https://kdla.ky.gov/records/recretentionschedules/Pages/stateschedules.aspx			X
Control Assessment	CA-1 CA-3 CA-7	Risk assessments associated with data governance	Do you provide security control health data in order to allow tenants to implement industry standard Continuous Monitoring (which allows continual tenant validation of your physical and logical control status)?		X	

and Authorization		requirements shall be conducted at planned intervals and shall consider the following: • Awareness of where sensitive data is stored and transmitted across applications, databases, servers, and network infrastructure • Compliance with defined retention periods and end-of-life disposal requirements • Data classification and protection from unauthorized use, access, loss, destruction, and falsification	Do you conduct risk assessments associated with data governance requirements at least once a year?		X	
Configuration Management - Policy and Procedures	CM-1	Organization shall follow a defined quality change control and testing process (e.g., ITIL Service Management) with established baselines, testing, and release standards which focus on system availability, confidentiality, and integrity of systems and services	Do you provide your tenants with documentation that describes your quality assurance process?		X	
			Is documentation describing known issues with your products/services available to tenants?		X	
			Are there policies and procedures in place to triage and remedy reported bugs and security vulnerabilities for product and service offerings? Are tenants provided with documentation on remedied issues?	X		
			Are mechanisms in place to ensure that all debugging and test code elements are removed from released software versions? Are there technical controls in place to prevent backdoors and surreptitious code?	X		
	CM-2 CM-2-COV CM-3 CM-3-COV CM-7	The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.	Do you have a capability to continuously monitor and report the compliance of your infrastructure against your information security baselines?	X		
			Do you have controls in place to restrict and monitor the installation of unauthorized software onto your systems and hardware on your network?	X		
			Can you provide evidence that the proposed solution adheres to a security baseline, which is based on least functionality?			X
			Are all changes to proposed solution authorized according to change management policies?	X		
Contingency Planning - Information System backup	CP-2 CP4 CP-6 CP-7 CP-9 CP-9-COV CP-10 SA-9-COV	A consistent unified framework for business continuity planning and plan development shall be established, documented, and adopted to ensure all business continuity plans are consistent in addressing priorities for testing, maintenance, and information security requirements. Requirements for business continuity plans include the following: • Defined purpose and scope, aligned	Do you provide tenants with geographically resilient hosting options? Are these hosting options FedRAMP certified?		X	
			Do you provide tenants with infrastructure service failover capability to other providers?		X	
			Are business continuity plans subject to test at planned intervals or upon significant organizational or environmental changes to ensure continuing effectiveness?	X		
			Can the solution provide and maintain a backup of Commonwealth data that can be recovered in an orderly and timely manner within a predefined frequency consistent with recovery time and recovery point objectives?	X		
			Can the solution store a backup of Commonwealth data, at least daily, in an off-site “hardened” facility, located within the continental United States, maintaining the security of Commonwealth data?		X	
			Can the solution partition, in aggregate for this proposal, all Commonwealth data submitted into the solution by the data owner in such a manner that it will not be impacted or forfeited due to E-discovery, search and seizure or other actions by third parties obtaining or attempting to obtain records, information or commonwealth data for	X		

		with relevant dependencies • Accessible to and understood by those who will use them • Owned by a named person(s) who is responsible for their review, update, and approval • Defined lines of communication, roles, and responsibilities • Detailed recovery procedures, manual work-around, and reference information • Method for plan invocation	reasons or activities that are not directly related to the business of the data owner?	X		
Identification and Authentication; Organizational Users	IA-1	Vendor should have an identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance	Does your management provision the authorization and restrictions for user access (e.g., employees, contractors, customers (tenants), business partners and/or suppliers) prior to their access to data and any owned or managed (physical and virtual) applications, infrastructure systems and network components?	X		
		Procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls	Do you require at least annual updates and reviews of your access policies for all system users and administrators (excluding users maintained by your tenants)?	X		
Identification and Authentication; Authenticator Management	IA-2 IA-2-COV IA-5		Do you support use of, or integration with, existing customer-based Single Sign On (SSO) solutions to your service?	X		
			Do you support identity federation standards (SAML, SPML, WS-Federation, etc.) as a means of authenticating/authorizing users?	X		
			Do you have an identity management system (enabling classification of data for a tenant) in place to enable both role-based and context-based entitlement to data?	X		
			Do you provide tenants with strong (multifactor) authentication options (digital certs, tokens, biometrics, etc.) for user access?		X	
			Do you allow tenants to use third-party identity assurance services?		X	
			Do you support password (minimum length, age, history, complexity) and account lockout (lockout threshold, lockout duration) policy enforcement? Do you support pass phrases?	X		
			Do you support the ability to force password changes upon first logon?	X		
			Do you have mechanisms in place for unlocking accounts that have been locked out (e.g., self-service via email, defined challenge questions, manual unlock)?	X		
Incident Response	IR-4 IR-5 IR-6	Identify immediate mitigation procedures, including specific instructions, based on information security incident categorization level, on whether or not to shut down or	Do you have a documented security incident response plan?		X	
			Do you integrate customized tenant requirements into your security incident response plans?		X	
			Do you publish a roles and responsibilities document specifying what you vs. your tenants are responsible for during security incidents?		X	
			Have you tested your security incident response plans in the last year?		X	

		disconnect affected IT systems. Establish procedures for information security incident investigation, preservation of evidence, and forensic analysis.				
		The organization tracks and documents information system security incidents.	Do you monitor and quantify the types, volumes and impacts on all information security incidents?		X	
			Will you share statistical information for security incident data with your tenants upon request?		X	
		Requires personnel to report suspected security incidents to the organizational incident response capability within 24 hours from when the agency discovered or should have discovered their occurrence; and Reports security incident information to designated authorities.	Do you have a defined and documented incident notification process for reporting suspected security incidents within 24 hours?		X	
			Does your Security Information and Event Management (SIEM) system merge data sources (app logs, firewall logs, IDS logs, physical access logs, etc.) for granular analysis and alerting?		X	
			Do you maintain liaisons and points of contact with local authorities in accordance with contracts and appropriate regulations?		X	
			Do you enforce and attest to tenant data separation when producing data in response to legal subpoenas?	X		
Media Protection Policy and Procedures: *Media Sanitization*	MP-6 MP-6-COV	Policies and procedures shall be established with supporting business processes and technical measures implemented for the secure disposal and complete removal of data from all storage media, ensuring data is not recoverable by any computer forensic means.	Do you support secure deletion (e.g., degaussing/cryptographic wiping) of archived and backed-up data as determined by the tenant?	X		
			Does supplier meet all data disposal requirements as outlined in the current Removal of Commonwealth Data from Electronic Media per CIO-092 Media Protection Policy? Can you provide a published procedure for exiting the service arrangement, including assurance to sanitize all computing resources of tenant data once a customer has exited your environment or has vacated a resource?		X	
Physical and Environmental Protection: Physical Access Authorizations	PE-2(1) PE-2(3)	The organization authorizes physical access to the facility where the information system resides based on position or role.	Do you restrict physical access to information assets and functions by position and role?	X		
Physical and Environmental Protection: *Physical Access Control*	PE-3	Ingress and egress points such as service areas and other points where unauthorized personnel may enter the premises shall be monitored, controlled and, if possible, isolated from data storage and processing facilities to prevent unauthorized data corruption, compromise, and loss.	Do you restrict physical access to information assets and functions by users and support personnel?	X		
			Are ingress and egress points, such as service areas and other points where unauthorized personnel may enter the premises, monitored, controlled and isolated from data storage and process?	X		
Physical and Environmental	PE-18-COV	All information system components	Do you allow tenants to define acceptable geographical locations for data routing or resource instantiation?		X	

Protection: *Physical Location*	SA-9-COV-1	and services remain within the continental United States. All physical components associated with an information system or service classified as sensitive with respect to confidentiality or integrity must be housed within the same storage location dedicated for the exclusive use of the organization and are clearly marked. Each hypervisor can only host one tier of the application architecture and no hypervisor may host the application interface and the data storage component for any information system, even if the components in question do not interact within the same information system.	Can you provide the physical geographical location of the storage in advance for a tenants data?	X		
			Can you provide the physical geographical location of a tenants data upon request?	X		
			Can you ensure that data does not migrate beyond a defined geographical residency?	X		
			Do you have the capability to restrict the storage of customer data to specific countries or geographic locations?	X		
			Does the solution have the capability to set affinity on tiered systems, no one hypervisor can host the application and the data storage?			X
System and Information Integrity: *Vulnerability / Patch Management (Flaw Remediation)*	SI-2 RA-5 RA-5-COV	Policies and procedures shall be established, and supporting processes and technical measures implemented, for timely detection of vulnerabilities within organizationally-owned or managed applications, infrastructure network and system components (e.g., network vulnerability assessment, penetration testing) to ensure the efficiency of implemented security controls. A risk-based model for prioritizing remediation of identified vulnerabilities shall be used. Changes shall be managed through a change management process for all vendor-	Do you conduct network-layer vulnerability scans regularly as prescribed by industry best practices? Provide the frequency.	X		
			Do you conduct application-layer vulnerability scans regularly as prescribed by industry best practices? Provide the frequency	X		
			Do you conduct local operating system-layer vulnerability scans regularly as prescribed by industry best practices? Provide the frequency	X		
			Will you make the results of vulnerability scans available to tenants at their request?		X	
			Do you have a capability to rapidly patch vulnerabilities across all of your computing devices, applications and systems?	X		
			Will you provide your risk-based systems patching time frames to your tenants upon request?		X	

		supplied patches, configuration changes, or changes to the organization's internally developed software. Upon request, the provider informs customer (tenant) of policies and procedures and identified weaknesses especially if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control.				
System and Information Integrity: *Malicious Code protection*	SI-3 SI-3-COV	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of malware on organizationally-owned or managed user end-point devices (i.e., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.	Does the provider ensure that they will utilize industry standard malware protection, incorporating both signature and non-signature-based detection mechanisms, on all systems with access to Commonwealth data?	X		
			Does the provider ensure that malware protection will be centrally managed and receive regular automatic updates to malicious code protection mechanisms and data files from the software vendor?	X		
System and Communications Protection: *Boundary Protection*	SC-7	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for the use of encryption protocols for protection of sensitive data in storage (e.g., databases) and data in transmission (e.g., system interfaces, over public networks, and electronic messaging) as per applicable legal, statutory, and regulatory compliance obligations.	Does the provider ensure that the solution will utilize industry standard firewalls regulating all data entering the internal data network from any external source which will enforce secure connections between internal and external systems and will permit only authorized data to pass through?	X		
			Does the offeror ensure that external connections incorporated into the solution have appropriate security controls including industry standard intrusion detection and countermeasures that will detect and terminate any unauthorized activity prior to entering the firewall maintained by offeror?	X		
System and Communications Protection; *Encryption*	SC-1 SC-8 SC-8-COV SC-23 SC-28		Do you encrypt tenant data at rest (on disk/storage) within your environment?		X	
			Do you use encryption for storing and transmitting email attachments?		X	
			Do you leverage encryption to protect data and virtual machine images during transport across and between networks and hypervisor instances?			X
			Do you support tenant-generated encryption keys or permit tenants to encrypt data to an identity without access to a public key certificate (e.g., identity-based encryption)?		X	
			Do you have documentation establishing and defining your encryption management policies, procedures and guidelines?		X	
Systems and Communication Protection; *Cryptographic Key Establishment and Management*	SC-12 SC-12-COV SC-13 SC-13-COV	The organization establishes and manages cryptographic keys for required cryptography employed within the information system	Do you have platform and data appropriate encryption that uses open/validated formats and standard algorithms?		X	
			Do you support encryption keys being solely maintained by the cloud consumer or a trusted key management provider?		X	
			Do you store encryption keys in the cloud?		X	
			Do you have separate key management and key usage duties?		X	

		in accordance with the organization-defined requirements for key generation, distribution, storage, access, and destruction. Platform and data appropriate encryption (e.g., AES-256 or higher) in open/validated formats and standard algorithms shall be required. Keys shall not be stored in the cloud (i.e. at the cloud provider in question), but maintained by the cloud consumer or trusted key management provider. Key management and key usage shall be separated duties.				
Data Security & Information Lifecycle Management *Nonproduction Data*	SA-11	Production data shall not be replicated or used in non-production environments. Any use of customer data in non-production environments requires explicit, documented approval from all customers whose data is affected, and must comply with all legal and regulatory requirements for scrubbing of sensitive data elements.	Do you have procedures in place to ensure production data shall not be replicated or used in non-production environments?	X		
Governance - Portability Requirements						
Interoperability & Portability *APIs*	CHFS - 1	The provider shall use open and published APIs to ensure support for interoperability between components and to facilitate migrating applications.	Do you publish a list of all APIs available in the service and indicate which are standard and which are customized?		X	
Interoperability & Portability *Data Request*	CHFS - 2	All structured and unstructured data shall be available to the customer and provided to them upon request in an industry-standard format (e.g., .doc, .xls, .pdf, logs, and flat files).	Is customer data (Structured & Unstructured) available on request in an industry-standard format (e.g., .doc, .xls, or .pdf)?	X		
Interoperability & Portability *Policy & Legal*	CHFS - 3	Policies, procedures, and mutually-agreed upon provisions	Do you provide policies and procedures (i.e. service level agreements) governing the use of APIs for interoperability between your service and third-party applications?		X	

	CHFS - 4	and/or terms shall be established to satisfy customer (tenant) requirements for service-to-service application (API) and information processing interoperability, and portability for application development and information exchange, usage, and integrity persistence.	Do you provide policies and procedures (i.e. service level agreements) governing the migration of application data to and from your service?		X	
Interoperability & Portability *Standardized Network Protocols*	CHFS - 5	The provider shall use secure (e.g., non-clear text and authenticated) standardized network protocols for the import and export of data and to manage the service, and shall make available a document to consumers (tenants) detailing the relevant interoperability and portability standards that are involved.	Can data import, data export and service management be conducted over secure (e.g., non-clear text and authenticated), industry accepted standardized network protocols?	X		
	CHFS - 6		Do you provide consumers (tenants) with documentation detailing the relevant interoperability and portability network protocol standards that are involved?		X	
Interoperability & Portability *Virtualization*	CHFS - 7	The provider shall use an industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability, and shall have documented custom changes made to any hypervisor in use, and all solution-specific virtualization hooks, available for customer review.	Do you use an industry-recognized virtualization platform and standard virtualization formats (e.g.., OVF) to help ensure interoperability?			X
	CHFS - 8		Do you have documented custom changes made to any hypervisor in use, and all solution-specific virtualization hooks available for customer review?			X
Security Framework - Organizational Security Framework	CHFS - 9	Design, acquisition, implementation, configuration, modification, and management of infrastructure and software are consistent with defined processing integrity and related security policies.	What Security Framework do you follow (.i.e. NIST, , ISO/IEC 27001, etc…,)?		X	
Security Assessment Framework and Methodology - Vulnerability Assessment and Penetration Test Security	CHFS - 10	Design, acquisition, implementation, configuration, modification, and management of infrastructure and software are consistent with defined processing	What Security Framework and Methodology do you follow for security assessment and penetration testing (.i.e. OSSTMM, OWASP, etc…,)?		X	

Framework and Methodology		integrity and related security policies.				