The global provider
of secure financial messaging services

SWIFT Customer Security Controls (CSC) Framework Introductory training

SWIFT Customer Security Controls (CSC) Framework

مقدمه

شبکه ی جهانی پیام‌رسانی مالی یا سوییفت (SWIFT) یک شبکه ی بین بانکی بین‌المللی برای نقل و انتقالات مالی جهانی می باشد که الزامات امنیتی را برای سازمان‌ها و بانک‌هایی که به این شبکه متصل هستند قرارداده است.

کنترل‌های امنیت اطلاعات مشتری سوییفت شامل الزامات اجباری (mandatory) و مصلحتی (advisory) می‌باشد.

الزامات اجباری یک سطح حداقلی لازم را برای تمامی اعضای شبکه به اجبار می‌گذارد که می‌بایست توسط تمامی اعضا به روی زیرساخت شبکه ی SWIFT داخل سازمانشان پیاده‌سازی شوند. SWIFT با اولویت بندی این کنترل‌های امنیتی سعی کرده است رویکردی واقع گرایانه را در پیاده سازی این کنترل ها بر مبنای کاهش ریسک‌های امنیتی در پیش بگیرد.

کنترل‌های مصلحتی براساس تجربه‌های پیشین به اعضا توصیه شده است. در طول زمان براساس تغییرات تهدیدهای موجود کنترل‌ها دستخوش تغییر خواهند شد. با ظهور تکنولوژی های جدید نیازمند به تغییر کنترل‌های امنیتی خواهند بود تا سطح امنیتی شبکه را در حد قابل قبولی حفظ نمایند. بنابراین برخی از کنترل‌های مصلحتی در طول زمان اجباری می‌شوند.

تمامی کنترل‌ها حول محوریت سه موضوع مهم تعریف شده اند:

1 - امنیت محیط
2 - شناسایی و محدود نمودن دسترسی
3 - کشف و پاسخ

در نهایت کنترل‌های تعریف شده همسو با استانداردهای امنیتی موجود تعریف شده اند.

درباره ی IT House

شـــرکت راهکار نوآوران فرتاک از ســـال ۲۰۱۱ میلادی به منظور ارایه خدمات مشـاوره‌ای و آموزشـی اسـتانداردهای مدیریت فناوری اطلاعات، پا به عرصـه ی ظهور گذاشـــت. این شـــرکت ابتدا با نام تجاری NIS ICT اولین و تنها موسسه آموزشی ایرانی تحت اعتبار مرجع اعتباردهی بین المللی، APMG انگلستان است که با دارا بودن شبکه ای گسترده از شرکای بین المللی، سبد محصولات منحصر به فرد، تائیدیه های ملی و بین المللی، اساتید و کارشناسان مجرب ایرانی و خارجی، مجموعه ای تقریباً کامل از جمله دوره های آموزشـی، آزمون های بین المللی و خدمات پژوهشی، فنی و مهندسی را به مخاطبان خود ارائه می دهد. خدمات آموزشیIT House بسته بـه موضـوع، با همکاری انحصـاری مؤسـسـاتی از جمله Quint (هلند)، AXELOS ، تحت اعتبار مراجع جهانی همچون مؤسـسـه مدیریت پروژه آمریکا (PMI) با بـالاترین امتیـاز (PDU) ممکن برگزار می گردد. در کنـار آموزش هـا، IT Houseامجوز/ امکـان برگزاری طیف گسـترده ای از آزمون هـای مختلف مراجع بین المللی IRCA (انگلسـتان)، APMG، (انگلسـتان)، Exin (هلند) و ISACA (آمریکا) را نیز فراهم نموده است.

این شـرکت اولین مجموعه‌ی ایرانی بوده اسـت که کلیه خـدمات اسـتانداردهای خانواده‌ی PCI را در ایران تحت اعتبار QSA های معتبر ارایه نموده است. این شرکت شریک تجاری انحصاری Advantio اولین QSA اروپا در ایران می باشد.

تماس با IT House

آدرس:
تهران، سـهروردی شـمالی، خیابان تهمتن پلاک ۶ واحد۱
تلفن: + ۹۸ (۰) ۲۱ ۹۱۰۷۱۴۶۶
فکس: + ۹۸ (۰) ۲۱ ۸۶۰۳۱۴۴۷
وبسایت: www.it-house.me
ایمیل: info@it-house.me

اهداف دوره

۱- آشنایی با عملکرد کلی شبکه SWIFT
۲- انواع معماری‌های شبکه ی SWIFT
۳- کارکرد برنامه ی امنیت CSC
۴- آشنایی با کنترل‌های امنیتی SWIFT

مخاطبان دوره

- تمامی متخصـصـان و علاقه مندان در حوزه امنیت اطلاعات
- مدیران پروژه های مرتبط
- کارشناسان امنیت اطلاعات
- کارشناسان پرداخت، سوییچ، ترمینال‌ها و ...
- برنامه‌نویسان پرداخت و بانک
- ممیزان و مشـاوران سـیسـتم های مدیریت امنیت اطلاعات
- مدیران و واحدهای امنیت اطلاعات شبکه بانکی

مدت زمان دوره

۲ روز (۱۶ ساعت) حضوری
۱۲ ساعت آنلاین

سرفصل های دوره

Day 1:
- Overview of SWIFT
  - Core messaging services
  - Connectivity types
  - FIN and ISO 20022 messaging standards
- SWIFT's Customer Security Programme (CSP) Introductory
  - Risk and threats
  - Architecture types
  - Framework objectives and principles
  - CSP evolution and overview of changes
  - Risk management and compliance report
  - Incident response
- Security Essentials
  - Technical introduction to risk and security controls
  - Application and interface hardening
  - Security parameters settings
- SWIFT Customer Security Programme
  - Customer Security Controls Framework (CSCF)
  - Independent Assessment Framework (IAF)
  - Compliance reporting options

Day 2:
- Scope of security controls
- Architecture types
- Security controls structure and compliance
- SWIFT CSP controls overview
  - SWIFT Customer Security Controls Framework v2021
  - 1. Restrict Internet Access & Protect Critical Systems from General IT Environment v2021
  - 2. Reduce Attack Surface and Vulnerabilities v2021
  - 3. Physically Secure the Environment v2021
  - 4. Prevent Compromise of Credentials v2021
  - 5. Manage Identities and Segregate Privileges v2021
  - 6. Detect Anomalous Activity to Systems and Transaction Records v2021
  - 7. Plan for Incident Response and Information Sharing v2021
- Shared responsibilities in cloud-based environments
- Best practices and recommendations

پیش نیازهای دوره

آشـــنایی اولیـه بـا مفـاهیم امنیـت اطلاعـات برای شرکت کنندگان در این دوره ی آموزشی پیشنهاد می گردد.

تعداد شرکت کنندگان

۱۵ الی ۲۲ نفر

درباره ی مدرک

مدارک این دوره ی آموزشـی تحت اعتبار شـرکت IT House می باشد

درباره ی آزمون

آزمون پایانی ندارد.

زبان

در صورت استفاده از اساتید بین المللی ، دوره به زبان انگلیسـی ارائه می گردد که امکان اسـتفاده از سـیسـتم ترجمه همزمان در صـورت درخواسـت متقاضیان مقدور می باشد. در دوره های آموزشی که توسط اساتید ایرانی این موسسه ارائه می گردد زبان مبنا فارسی می باشد.

محتوای آموزشی

محتوای مورد اسـتفاده در این دوره ی آموزشـی، تحت اعتبار QSA های اروپایی می باشد.