RESILIA Foundation
Cyber Resillience Best Practice

مقدمه

RESILIA مجموعه ای جامع از ابزارها و آموزش ها برای کمک به سازمان در دستیابی به بهترین عملکرد در حوزه ی امنیت سایبری است. این چارچوب کمک می کند تا سازمان بتواند از طریق استفاده از فرآیندها و استانداردهای موجود، انعطاف پذیری سایبری خود را ارتقا داده و بدون در نظر گرفتن نقش یا مسئولیت افراد از طریق بکار گیری بهترین مهارت ها و رفتارها در حوزه ی امنیت سایبری در سراسر سازمان فراتر از امنیت سایبری موثر و دستیابی به قابلیت انعطاف پذیری سایتی در سازمان اقدامات لازم مورد انجام قرار گیرد. RESILIA توسط انجمن جهانی Axelos مبتنی بر راهنمای Cyber Resilience Best Practice مودر توسعه قرار گرفته است. استفاده از چرخه حیات خدمات Service Life Cycle مورد اشاره در RESILIA و ITIL توانایی سازمان در شناسایی، ارائه پاسخ و بهبودی ناشی از حملات سایبری را ارتقا می دهد. بر این اساس می توان گفت RESILIA به معنای تجهیز کارکنان با دانش و مهارت های لازم و ایجاد آگاهی، شفافیت و اطمینان از نحوه ی واکنش و بازیابی شرایط برای بهبود توانایی سازمان در تشخیص و مبارزه با تهدیدات امنیت سایبری در افراد سازمان از طریق موارد ذیل می باشد:

- خسارات ناشی از نقص امنیت سایتی را کاهش می دهد
- بهینه سازی بازیابی ناشی از نقض های امنیت سایبری
- اسان سازی پذیرش مفهوم Cyber resilience در فرآیندهای موجود سازمان
- پشتیبانی از بهترین روشهای طراحی استراتژی انعطاف پذیری سایبری در داخل سازمان
- ایجاد یک زبان مشترک برای پذیرش انعطاف پذیری سایبری در سراسر سازمان
- پشتیبانی موثر از هزینه ها با ایجاد امنیت در پروژه ها و برنامه های سازمان
- محافظت در برابر تعهدیدات با حصول اطمینان از راه حل های مناسب مناسب طراحی شده سازگار با استراتژی

RESILIA Foundation
CYBER RESILLIENCE

درباره ی IT HOUSE

مؤسسه فناوری اطلاعات راهکار نوآوران فرتاک پس از ۷ سال همکاری موفق و مستمر شرکت NIS CERT کانادا با سازمان های ایرانی، در سال ۲۰۱۱ میلادی به عنوان یکی از واحدهای کسب و کار استراتژیک (SBU) این شرکت، با نام تجاری NISICT پا به عرصه ی ظهور گذاشت. این مجموعه در طی ۸ سال پس از همکاری موفق با بیش از ۲۰۰ سازمان بر تر ایرانی، از ابتدای سال 2019 میلادی با توجه به راه اندازی مراکز تخصصی پیشرفته با همکاری شبکه ی گسترده ای از شرکای معتبر داخلی و بین المللی در طیف وسیعی از بهروش ها و استاندارد های بین المللی با هدف ارائه راهکار های جامع مدیریتی در حوزه ی فناوری اطلاعات، ماهیت تجاری خود (برند) را تغییر داده و از نشان تجاری IT HOUSE در حوزه ی محصولات و خدمات خود استفاده خواهد نمود. IT HOUSE با همکاری انحصاری مؤسساتی از جمله Quint (هلند)، NTT (ایرلند)، ACT POWER (مراکش) تحت اعتبار مراجع جهانی همچون انجمن جهانی tmforum آمریکا، PCI Council آمریکا، ISACA آمریکا، AXELOS انگلستان قادر به ارائه خدمات در تزار استاندارد های بین المللی به سازمان های ایرانی می باشد

انجام عملیات تشخیص و محافظت در مقابل حملات سایبری بر عهده سازمان نیست بلکه افراد سازمان هستند که مجری چنین فعالیتهایی خواهند بود. تجهیز افراد به نحوه کنش و واکنش در فضای سایبری امری الزامی جهت حفظ ارزشهای سازمان در داخل سازمان است

اهداف دوره

1. Understand the purpose, benefits and key terms of cyber resilience
2. Understand the purpose of risk management and the key activities needed to address risks and opportunities
3. Understand the purpose of a management system and how best practices and standards can contribute
4. Understand the purpose of cyber resilience strategy, the associated control objectives and their interactions with ITSM activities
5. Understand the purpose of cyber resilience design, the associated control objectives and their interactions with ITSM activities
6. Understand the purpose of cyber resilience transition, the associated control objectives and their interactions with ITSM activities
7. Understand the purpose of cyber resilience operation, the associated control objectives and their interactions with ITSM activities
8. Understand the purpose of cyber resilience continual improvement, the associated control objectives and their interactions with ITSM activities
9. Understand the purpose and benefits of segregation of duties and dual controls

مخاطبان دوره

- مدیران امنیت اطلاعات
- مدیریان امنیت سایبری
- مدیران ریسک
- مدیران فناوری اطلاعات
- مدیران سیستم های و روش ها
- تحلیل گران کسب و کار

مدت زمان دوره

۳/۵ روز– حضوری (۲۸ ساعت)
۲۱ ساعت – آنلاین تعاملی

سرفصل های دوره

1 Introduction

1.1 Intended audience
1.2 Making cyber resilience real through the use of examples
1.3 Aligning cyber resilience with business outcomes
1.4 What is cyber resilience?
1.5 Some important characteristics of cyber resilience
1.6 Wider benefits of cyber resilience – building trust
1.7 How to achieve a sufficient level of cyber resilience
1.8 Scope of this publication
1.9 Introduction questions

2 Risk management

2.1 Management of Risk
2.2 Assets, threats, vulnerabilities and risks
2.3 Actions to address risks and opportunities
2.4 Risk management questions

3 Managing cyber resilience

3.1 The need for a single management system
3.2 The ITIL service lifecycle
3.3 Managing cyber resilience questions

4 Cyber resilience strategy

4.1 Control objectives and controls for a cyber resilience strategy
4.2 Aligning cyber resilience strategy with IT service strategy
4.3 Strategy scenarios
4.4 Cyber resilience strategy questions

iT House
Enabling Your Enterprise IT

RESILIA™
LICENSED AFFILIATE
ON BEHALF OF AXELOS

5 Cyber resilience design

5.1 Control objectives and controls for cyber resilience design
5.2 Aligning cyber resilience design with IT service design
5.3 Design scenarios
5.4 Cyber resilience design questions

6 Cyber resilience transition

6.1 Control objectives and controls for cyber resilience transition
6.2 Aligning cyber resilience transition with IT service transition
6.3 Transition scenarios
6.4 Cyber resilience transition questions

7 Cyber resilience operation

7.1 Control objectives and controls for cyber resilience operation
7.2 Aligning cyber resilience operation with IT service operation
7.3 Operation scenarios
7.4 Cyber resilience operation questions

8 Cyber resilience continual improvement

8.1 Control objectives and controls for cyber resilience continual improvement
8.2 Aligning cyber resilience continual improvement with IT continual service improvement
8.3 Using the ITIL CSI approach to plan cyber resilience improvements
8.4 Using MSP to plan and manage cyber resilience improvements
8.5 Maturity models
8.6 Continual improvement scenarios
8.7 Cyber resilience continual improvement Questions

9 Cyber resilience roles and responsibilities

9.1 Roles and responsibilities across the organization
9.2 Segregation of duties and dual controls
9.3 Cyber resilience roles and responsibilities questions

پیش نیازهای دوره

تسلط بر مفاهیم RISK، امنیت و مدیریت و حاکمیت خدمات ضروری است

تعداد شرکت کنندگان

۶ الی ۱۸ نفر

درباره ی مدرک

به شرکت کنندگان در این دوره ی آموزشی گواهی حضور از سوی شرکت IT HOUSE (NISICT) تحت اعتبار شرکت PECB کانادا اعطا خواهد شد.

درباره ی آزمون

آزمون ندارد

زبان

در صورت استفاده از اساتید بین المللی، دوره به زبان انگلیسی ارائه می گردد که امکان استفاده از سیستم ترجمه همزمان در صورت درخواست متقاضیان مقدور می باشد. در دوره های آموزشی که توسط اساتید ایرانی این موسسه ارائه می گردد زبان مبنا پارسی می باشد.

محتوای آموزشی

محتوای مورد استفاده در این دوره ی آموزشی آخرین ویرایش از الگوها و استانداردهای ارائه شده توسط Axelos می باشد

تماس با IT House

آدرس:
تهران، سهروردی شمالی، کوچه تهمتن، پلاک ۶ واحد ۱
تلفن: + ۹۸ (۰) ۲۱ 88731466
فکس: + ۹۸ (۰) ۲۱ 86031447
وبسایت: www.it-house.me
ایمیل: crm@it-house.me

iT House
Enabling Your Enterprise IT

RESILIA™
LICENSED AFFILIATE
ON BEHALF OF AXELOS