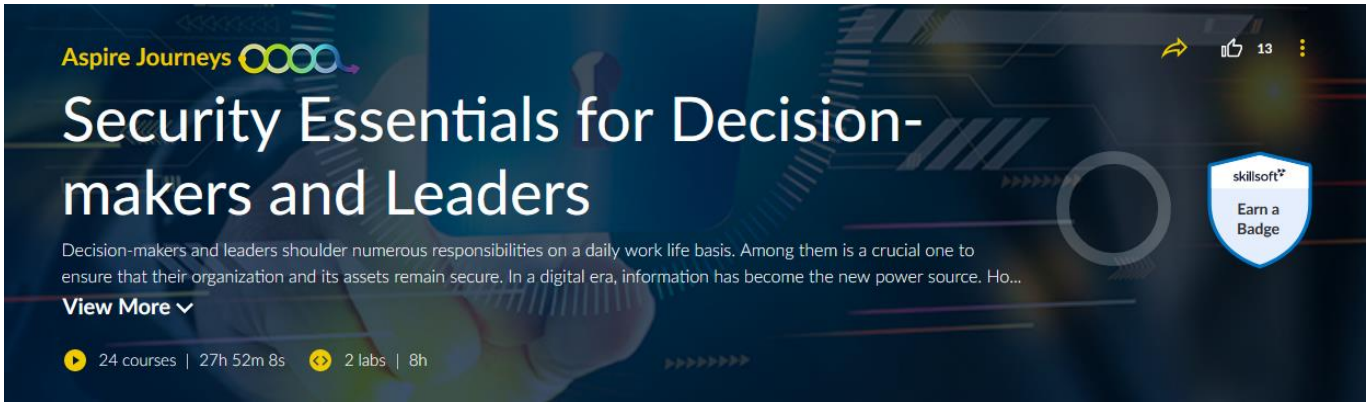
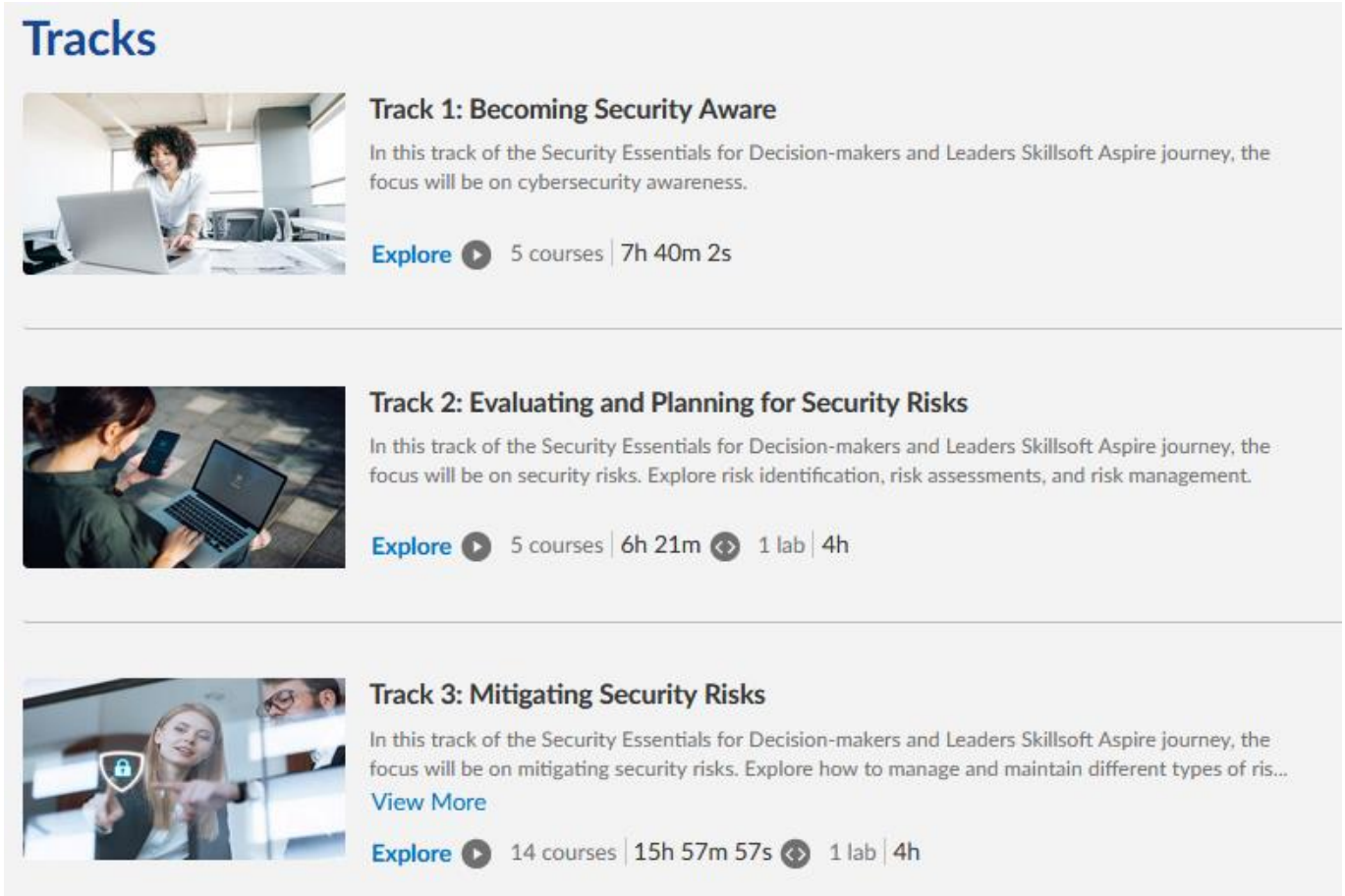
Security Essentials for Decision-makers and Leaders

SKILLSOFT ASPIRE JOURNEY

skillsoft

Decision-makers and leaders shoulder numerous responsibilities on a daily work life basis. Among them is a crucial one to ensure that their organization and its assets remain secure.
In a digital era, information has become the new power source. However, for decision-makers and leaders across the globe, protecting the organization's information from abuse, misuse, or unauthorized access can be challenging. New security threats emerge every day and decision-makers and leaders need to be armed with the right skills to make well-informed security decisions.
In this Skillsoft Aspire journey, you will begin by becoming aware of common security threats, exposure to them, and their impact on businesses and assets. You will continue your discovery of what you need to do by learning how to identify, evaluate, and plan for security risks. Finally, you will learn how to adopt best practices and guidelines to mitigate security risks.





PREREQUISITES

In order to fully profit from the potential of this Aspire Journey, we recommend the following prerequisite skills:

- Familiar with Cybersecurity
- Knowledge of security threats

Cybersecurity Awareness: Getting Started with Security Foundations

Objectives

- outline the core foundational concepts of information security and recognize why it is important to an organization
- describe the standard information security roles within an organization
- list the responsibilities of various information security roles within an organization
- classify the expectations of users and organizations in relation to security, IT systems, permissions, and usage
- recognize that security is everyone's responsibility in a professional environment and outline how to use the Responsible-Accountable-Consulted-Informed (RACI) chart to see different responsibilities are distributed
- recognize the importance of strategic planning and decision-making when it comes to information security
- recognize the importance of effective communication for fostering proper information security
- define the concept of security governance in relation to information security
- list the standard security governance activities that relate to information security
- describe how proper information security can support the organization's overall business objectives

Cybersecurity Awareness: Information Security Fundamentals

Objectives

- recall what is meant by information security, what it protects, and how it protects it
- use case studies and examples to illustrate what can happen when information is not protected
- list the domains into which various types of information security can be categorized
- describe the purpose and importance of cybersecurity and outline the cybersecurity framework
- describe the various types of approaches to cybersecurity
- describe the CIA triad and its importance and outline some cybersecurity confidentiality concepts
- describe the integrity concepts of the CIA Triad
- describe the availability concepts of the CIA Triad
- discuss the CIA impacts and methods
- define the function of security architecture and name related frameworks
- define the purpose of security controls and name security control methods
- classify and describe different types of security controls
- describe examples of risks that can occur to anyone in any situation as well as those that expose organization's to security risks
- define the role of humans in protecting the security of information

Cybersecurity Awareness: Key Security Terms & Concepts

Objectives

- describe key concepts of cybersecurity assets and risks
- describe the key terms associated with cybersecurity threats
- recognize the key concepts of cybersecurity vulnerability and countermeasures
- list the types of threat actors and their motives
- list the types of attack targets
- define what is meant by security exposure and a security threat or risk
- list types of cybersecurity threats
- describe what comprises mobile technology threats
- define what is meant by cloud threats and list types of such threats
- define advanced persistent threats (APTs)
- give an example of an APT
- describe how an insider threat in an organization would manifest
- describe what malware is and list standard types of malware
- list the steps performed in a cyberattack on security
- define what is meant by uncertainty in cybersecurity

Cybersecurity Awareness: Exposure to Security Risks

Objectives

- list and describe the critical information security issues -confidentiality, integrity, availability, authentication, non-repudiation, privacy, and trust
- recognize the standard security threats to an organization
- differentiate using examples what exposure, threat or risk, security attack, exploits or breach of security, and impact/severity mean
- illustrate using examples common actions from daily work-life that expose people to security risks
- recognize the importance of threat identification and describe the concepts of threat modeling and threat identification sources and methods
- define the STRIDE model in the context of threat identification
- define the PASTA threat modeling method and its stages
- identify why and how security is everyone's responsibility
- list different methods to reduce security risks

Final Exam: Becoming Security Aware

Objectives

- define the concept of security governance in relation to information security
- describe key concepts of cybersecurity assets and risks
- describe the availability concepts of the CIA Triad
- describe the CIA triad and its importance and outline some cybersecurity confidentiality concepts
- describe the integrity concepts of the CIA Triad
- describe what comprises mobile technology threats
- describe what malware is and list standard types of malware
- differentiate using examples what exposure, threat or risk, security attack, exploits or breach of security, and impact/severity mean
- list and describe the critical information security issues -confidentiality, integrity, availability, authentication, non-repudiation, privacy, and trust
- list different methods to reduce security risks
- list the responsibilities of various information security roles within an organization
- list the steps performed in a cyberattack on security
- list the types of threat actors and their motives
- outline the core foundational concepts of information security and recognize why it is important to an organization
- recognize the standard security threats to an organization

Security Risks: Key Risk Terms & Concepts

Objectives

- outline how risks are related to assets
- identify the similarities and differences between likelihood and probability assessment
- recognize the role of vulnerabilities in risks and the correlation between risk and threat
- outline risk probability, the impact generated by it, and how to measure it using a risk score
- describe risk severity and identify various risk security levels
- identify potential risks that may exist within an organization and differentiate between risk appetite and risk tolerance
- define the concept and advantages of a risk management process
- recognize the importance of a risk management plan and identify its components
- describe the role of a risk register in managing risk and outline the elements of risks listed within it
- describe the features of different risk treatment methods
- recognize the importance of managing risk and implementing a risk-based approach
- outline the elements of the COBIT 5 framework and describe the ISO 31000 standard for risk management
- list the three key stages of a risk management process: risk identification, risk assessment, and risk management
- illustrate the importance of security risk assessment in preempting and preparing for risks, prioritizing risks, and identifying assets to be protected

Security Risks: Performing Security Risk Identification

Objectives

- identify the differences between threat and risk
- recognize the purpose and importance of risk identification
- outline the risk identification process and recognize organizational components impacted by risk
- distinguish between different methods used for risk identification
- list the best practices used for risk identification and identify the benefits of the process
- recognize the characteristics and functions of a risk register
- demonstrate the method to create a risk register in Microsoft Excel

Security Risks: Performing Security Risk Assessments

Objectives

- define the concept, advantages, and activities of risk assessment
- list different types of risk assessment
- describe the characteristics of qualitative risk assessment along with its advantages and disadvantages
- describe the characteristics of quantitative risk assessment along with its advantages and disadvantages
- identify vulnerability assessment and penetration testing as security assessment methods
- demonstrate security vulnerability assessment
- outline risk categorization using the four-quadrant risk classification
- illustrate how to update a risk register in Microsoft Excel
- recognize the importance of prioritizing risks
- outline the role of probability-impact matrix in prioritizing risks
- demonstrate how to prioritize risks in a security risk register using a probability-impact matrix

Security Risks: Planning for Security Risk Management

Objectives

- describe the purpose of risk management and list the best practices
- outline the stages and activities in a risk management process
- identify the components of a risk management plan and recognize different risk categories
- list the elements of a risk management plan and the steps involved in creating one
- describe the features of a risk mitigation plan and its role in risk management
- create a risk mitigation plan in Microsoft Word
- outline the factors that influence risk tolerance and risk appetite and the differences between them
- examine the concept of risk monitoring and control measures and list their outcomes in risk management planning
- recognize the importance of treating risks and list different risk strategy methods
- describe the role of decision making in managing risks

Evaluating and Planning for Security Risks

Objectives

- Practice evaluating and planning for security risks by creating a risk register and identifying risks, applying a probability matrix to identify high risks, performing a vulnerability assessment and creating a risk mitigation plan.

Final Exam: Evaluating and Planning for Security Risks

Objectives

- define risk assessment
- demonstrate vulnerability assessment
- describe risk management process for security (with a key focus on standards such as ISO 31000)
- describe risk strategies taking security-related work examples
- describe the details of a risk management plan
- describe the risk identification process
- describe vulnerability assessment and penetration testing as security assessment methods
- differentiate between risk appetite and risk tolerance
- identify the need to prioritize risks
- list risk treatment methods (Risk acceptance, avoidance, reduction, transfer)
- list the activities in a risk management process
- list the methods used for risk identification
- recognize how increasing risk tolerance and risk appetite can be an effective risk management strategy
- recognize security threat as a risk
- recognize the need for risk identification

Mitigating Security Risks: Managing Network & Infrastructure Security Risks

Objectives

- describe the network vulnerabilities that can turn into threats
- describe commonly used network vulnerability prevention methods
- illustrate using examples how a vulnerable network exposes the organization to cyber, data, cloud, and information security risks
- define network security
- list basic network zones and compare them in relation to security
- describe the role of monitoring, detection, and logging
- list the tools that can be used for network security, keeping capabilities for monitoring, detection, and logging in mind
- recognize the characteristics of a secure network design for protecting networks and systems
- list the guidelines and best practices for network security

Mitigating Security Risks: Managing Physical Security Risks

Objectives

- list several physical security risks
- describe what is meant by tailgating
- describe physical security and its importance
- outline the layers of physical security that can prevent a physical security risk
- list the key physical security risk countermeasures
- outline how security principles can be applied to the design of your facility and site
- recognize how to implement security controls to tighten facility and site security
- recognize how to implement internal and perimeter security controls
- list various physical security standards

Mitigating Security Risks: Cyber Security Risks

Objectives

- define what is meant by a security risk in relation to information technology
- list potential information and data security risks
- list potentional cloud security risks
- describe common sources of cybercrimes, their targets, and how to use these to identify effective prevention methods
- recognize common cyberattacks and crimes using examples
- list the best practices to manage threats from worms, viruses, logic bombs, trojans, and rootkits
- describe ways to thwart various attacks, including DoS
- describe methods to handle backdoor attacks
- describe the role of zero-day exploits in exploiting vulnerabilities
- list examples of zero-day attacks
- describe methods to handle zero-day vulnerabilities

Mitigating Security Risks: Managing Social Engineering Risks

Objectives

- describe what is meant by social engineering and give examples
- describe the key intent of social engineering
- list the principles of social engineering attacks (authority, intimidation, consensus, scarcity, urgency, familiarity, and trust)
- describe using examples how social engineering is used as a medium to launch cyber attacks
- list some types of social engineering attacks
- list some types of spoofing attacks
- identify the possible targets in social engineering
- describe the best practices for protecting against social engineering

Mitigating Security Risks: Information, Cloud, & Data Security Risk Considerations

Objectives

- describe commonly used methods to compromise information security
- list three fundamental information security principles
- describe some threats to information security principles
- recognize through examples how the human factor is a key source of data theft
- state some key technologies to secure data and information
- identify the key worldwide information security regulations and governance frameworks
- describe the need for cloud security
- describe the benefits of cloud security
- outline the ISO 27017 cloud security principles that should be considered when formulating a cloud security risk management plan

Mitigating Security Risks: Managing Information, Cloud, & Data Security Risks

Objectives

- describe the role of security controls in managing risks
- describe the security control categories and types
- define what's meant by the information security approach, Defense in Depth
- list and categorize key countermeasures for managing risks
- outline the guidelines and best practices for ensuring information is secure
- outline the guidelines and best practices for implementing security measures against common cloud security risks
- describe the role of access control in securing data and list some common types of access control
- list the best practices and guidelines to adopt for making sure data is managed securely
- describe the role of digital signatures in securing information
- define what's meant by data backup and list some backup types
- describe why data backup is needed
- list the best practices and guidelines for backing up data
- outline how unintentional data exposure happens and name some keys reasons why it happens
- outline best practices for protecting data and information using common security risk scenarios
- recognize how to use data science and AI to detect emerging security threats

Mitigating Security Risks: Handling Natural Threats

Objectives

- recognize the need for securing assets against natural disasters
- list the key considerations to be kept in mind when planning natural disaster risk mitigation
- define an emergency action plan and lists its minimum requirements
- explain how an effective emergency action plan is vital to managing natural disaster risk
- illustrate using an example how to draft an emergency action plan

Mitigating Security Risks: Managing Risks from Internal Stakeholders

Objectives

- define the role of internal stakeholders in the context of security
- identify the security risks that can come from decisions taken by stakeholders
- describe the role of effective communication and stakeholder engagement in managing security risks from internal stakeholders
- describe the methods used in effective reporting of security health
- illustrate through a security-related work example scenario how effective stakeholder communication and engagement can result in a more secure workplace

Mitigating Security Risks: Managing Security in a Hybrid Workplace

Objectives

- describe what is meant by a hybrid workplace
- recognize the security concerns for an organization when its employees work in a hybrid workplace
- describe the key security decisions to be made when adopting a hybrid workplace
- define the 'work from home' method of working
- illustrate using examples the security concerns for an organization when its employees work from home
- compare and contrast the security risks of WFH and hybrid workplaces
- distinguish the responsibilities of employees and organizations in a work from home scenario
- describe practical tips and guidelines for a secure WFH culture that security leaders should communicate to their employees

Mitigating Security Risks: Information Security Governance

Objectives

- define information security governance
- describe why security governance is needed
- list the benefits of security governance
- outline the relationship between security governance and the CIA Triad
- list the desired outcomes of security governance
- compare security governance and security management
- list the elements of security governance
- define the role and importance of security policies, procedures, standards, and guidelines
- list the types of IT governance frameworks
- describe the role of senior management in security governance
- describe methods to create and deliver governance
- describe the senior management roles and responsibilities in security governance
- list methods to review governance
- describe the signs of security governance
- outline some examples of missing governance
- list the reasons for ineffective security governance
- list some security governance best practices and outline the method to implement security governance
- list and describe the components of the security governance structure

Mitigating Security Risks: Managing the Incidents

Objectives

- define what's meant by an incident in the context of a security breach
- outline the incident management process
- describe the key terms used in the incident management process
- list the objectives of the incident management process and use them to recognize why this process is needed
- list the benefits of the incident management process
- list the steps involved in the incident management process
- describe the relationship incident management has with other processes
- list the roles and responsibilities involved in the incident management process
- illustrate the use of incident handling forms
- outline some incident prevention measures
- identify the security incident signs an employee should be aware of and escalate when found

Mitigating Security Risks: Maintaining Business Continuity

Objectives

- describe what's meant by business continuity planning (BCP) in the context of managing threats
- outline what comprises disaster recovery planning and list some types of disaster recovery plans
- compare business continuity planning and disaster recovery planning
- outline how business continuity planning helps reduce the impact of a disaster
- list the steps in the business continuity planning lifecycle that help define an effective business continuity plan
- define the role of the risk management plan as the first step in business continuity planning (BCP)
- define the role of business impact analysis as the second step in business continuity planning (BCP)
- define the role of the incident response plan as the third step in in business continuity planning (BCP)
- define the role of recovery time objectives in business continuity planning (BCP)
- define the role of recovery point objectives in business continuity planning (BCP)
- define the role of the disaster recovery plan as the fourth step in business continuity planning (BCP)
- compare and contrast a business continuity plan with an emergency action plan
- recognize the role of the organization in community post-disaster recovery planning
- outline the steps to building an organization’s business resiliency in the face of a disaster
- describe using COVID-19 as an example the guidelines and best practices for dealing with and pursuing business excellence during a pandemic

Mitigating Security Risks: Maintaining a Secure Workplace

Objectives

- describe the components and characteristics of a secure workplace and why a workplace needs to be secure
- list the best practices for establishing a secure workplace
- outline what a security policy is and the guidelines and best practices for establishing one
- describe the guidelines for conducting effective security training and security awareness-building activities for employees
- outline the guidelines for cultivating a security mindset
- outline guidelines for encouraging employees to actively participate in maintaining security
- define the Cyber Maturity Model certification (CMMC) and describe how it helps to ensure a secure organization

Mitigating Security Risks

Objectives

- Mitigate security risks by identifying a phishing email, creating and sending a phishing email and subscribing to the Microsoft Security Notification Service. Then, calculate the vulnerability score for a given vulnerability.

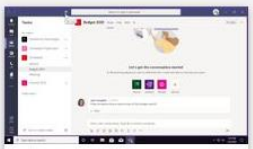
Final Exam: Mitigating Security Risks

Objectives

- compare and contrast the security risk of WFH and hybrid workplace
- Compare Business Continuity and Disaster Recovery
- define an emergency action plan
- define an incident
- define a secure workplace
- define Incident Response Plan as the third step in BCP
- describe defense-in-depth
- describe the guidelines for conducting effective security training and security awareness building activities for employees
- describe the guidelines to encourage employees to actively participate in maintaining the security
- describe the ISO 27017 Cloud security principles to consider when formulating a Cloud security risk management plan
- describe the layers of physical security that can prevent a physical security risk
- describe the methods to handle backdoor attacks
- describe the methods to handle zero-day vulnerabilities
- describe the methods used in effective reporting of security health
- describe the network vulnerabilities that can turn into threats
- describe the role of access control in securing data
- describe the role of effective communication and stakeholder engagement in managing security risks from internal stakeholders
- describe the signs of security governance
- describe the threats to information security principles
- illustrate using an example how to draft an Emergency Action plan
- implement the internal and perimeter security controls
- list the benefits of security governance
- list the best practices and guidelines to adopt for secure data management
- list the principles of social engineering attacks (Authority, Intimidation, Consensus, Scarcity, Urgency, Familiarity, Trust)
- list the steps in Business Continuity Planning
- list the steps in the incident management process
- list the tools that can be used for network security keeping monitoring, detection, and logging in context
- list the Types of IT Governance Frameworks
- list the types of social engineering attacks
- recognize the security concerns for an organization when its employees work in a hybrid workplace

Productivity Tools for Decision-makers and Leaders

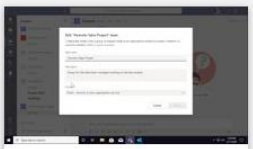
Optional



COURSE

Getting to know the application

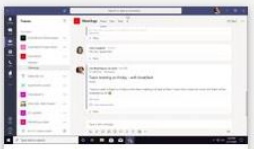
998



COURSE

Using Teams & Channels

743



COURSE

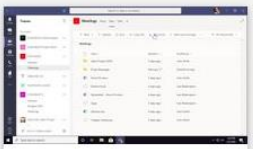
Communicating via the App

719

COURSE

Formatting, Illustrating & Reacting to Messages

537



COURSE

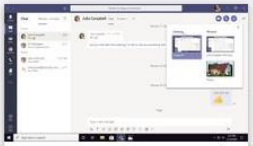
Creating, Finding & Organizing Files

531

COURSE

Working with Apps, Tabs & Wiki

461



COURSE

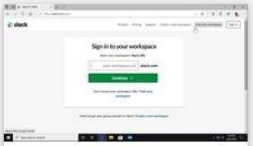
Making calls, Organizing Contacts & Using Voicemail

449

COURSE

Creating, Joining & Managing Meetings

459



COURSE

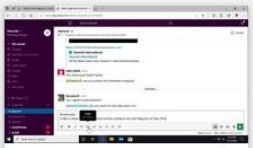
Signing in & Setting Up Slack

26

COURSE

Using Channels in Slack

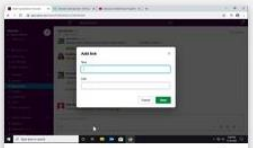
12



COURSE

Using Private Messaging & Communication Tools in...

14



COURSE

Creating, Finding & Sharing Information in Slack

7

COURSE

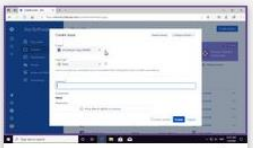
Configuring Slack

6

COURSE

Creating & Setting Up Projects in Jira Cloud

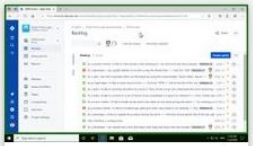
150



COURSE

Configuring & Managing Boards in Jira Cloud

97



COURSE

Planning & Working on a Software Project in Jira...

75

COURSE

Reporting in Jira Software

73

COURSE

Signing in & Navigating within Spaces

39

COURSE

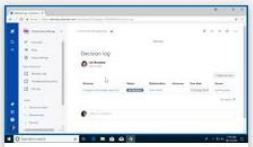
Setting Up & Managing Spaces

33

COURSE

Working with Space

27



COURSE

Working with Team Members

75

COURSE

Configuring Spaces

19

Bookshelf

Optional

BOOK

The Cybersecurity Playbook: How Every Leader and...

BOOK

Security Fundamentals

2

BOOK

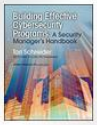
Cybersecurity Essentials

15

BOOK

Information Technology Security Fundamentals

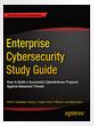
17



BOOK

Building Effective Cybersecurity Programs: A...

4



BOOK

Enterprise Cybersecurity Study Guide: How to Build ...

3

BOOK

Financial Cybersecurity Risk Management: Leadership...

BOOK

Cybersecurity Program Development for Business:...

2

BOOK

Cybersecurity for Dummies

24

BOOK

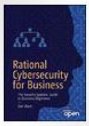
Cybersecurity: A Self-Teaching Introduction

10

BOOK

Building an Effective Cybersecurity Program, 2n...

3



BOOK

Rational Cybersecurity for Business: The Security...

1

BOOK

How to Measure Anything in Cybersecurity Risk

19

BOOK

The Complete Guide to Cybersecurity Risks and...

43

BOOK

Enterprise Security Risk Management: Concepts an...

4

BOOK

Information Security Risk Management for ISO 2700...

9

BOOK

The Manager's Guide to Enterprise Security Risk...

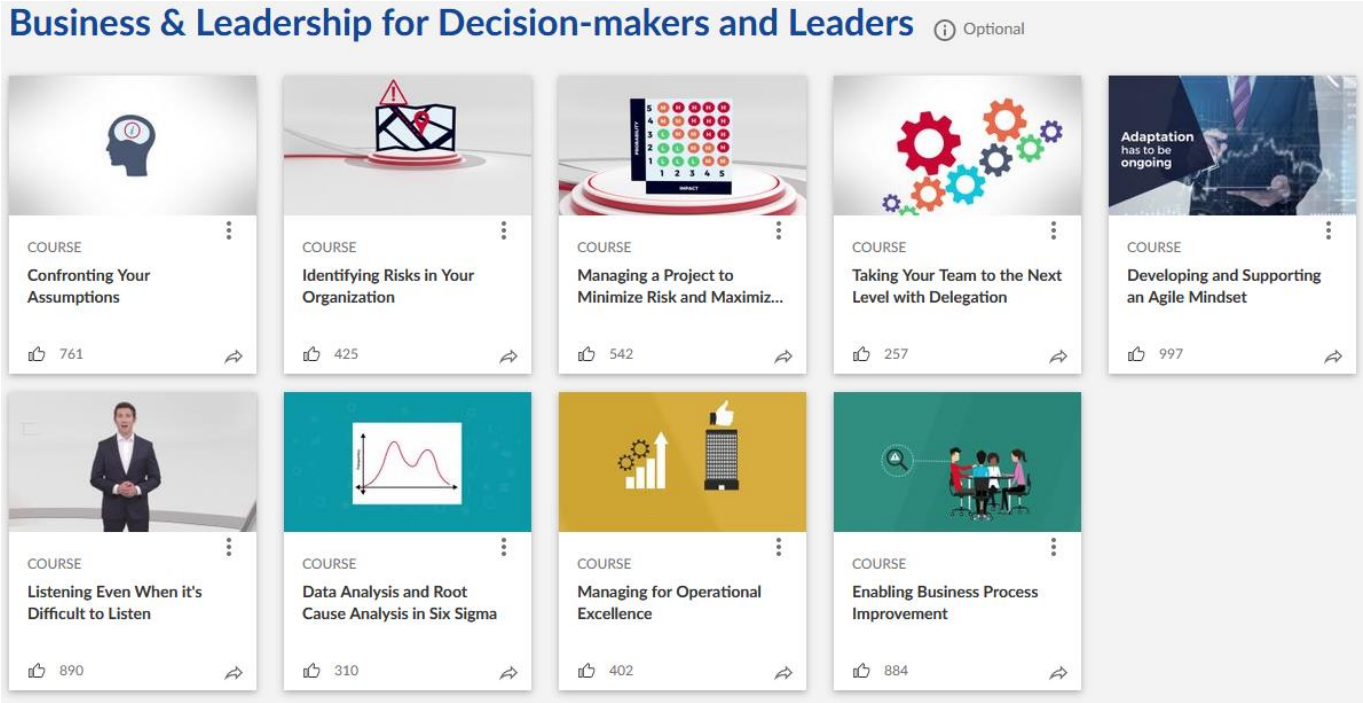
BOOK

IT Security Risk Control Management: An Audit...

3

BOOK

Cybersecurity and Decision Makers: Data Security and...



FOLLOW US ON:

www.skilltech.pl

email: biuro@skilltech.pl

tel. +48 22 44 88 827

SkillTech
Technology hired for excellence