Based on ENISA’s European Cybersecurity Skills Framework (ECSF), this calendar will feature a different skill each month. ECSO aims to spread awareness of key aspects of cybersecurity and showcase ECSO Members and cybersecurity community’s solutions and services.

The monthly themes for 2023 are planned as follows:

January – Chief Information Security Officer
February – Cyber incident Responder
March – Cyber Legal, Policy and Compliance Officer
April – Cyber Threat Intelligence Specialist
May – Cybersecurity Architect
June – Cybersecurity Auditor
July – Cybersecurity Educator
August – Cybersecurity Implementer
September – Cybersecurity Researcher
October – Cybersecurity Risk Manager
November – Digital Forensics Investigator
December – Penetration Tester
Did you know?

1. A Cybersecurity Risk Manager handles the organisation's cybersecurity-related risks aligned to the organisation's strategy. They also develop, maintain and communicate the risk management processes and reports. More [HERE](#).
3. Depending on the interest of the Cybersecurity Risk Manager ECSO has two Working Groups where they may contribute within their field to European cybersecurity as a whole. The first Working Group is dedicated to research and new technologies. This working group has a goal to define the cyber security EU R&I roadmap and vision, establish priorities through a Strategic Research and Innovation Agenda (SRIA) for the H2020 Work Programme and the future Horizon Europe and Digital Europe Programme. Very often, coordinating cybersecurity activities and pilots projects includes working side by side with Cybersecurity Risk Managers who participate on different levels. Together, they assist in the development of innovative cybersecurity-related solutions and contribute towards cutting-edge cybersecurity business ideas, services and solutions through ECSO. More [on this Working Group](#) HERE.
4. The second ECSO Working Group of interest for a Cybersecurity Risk Manager is dedicated to cyber resilience of economy, infrastructures and services. In its vision to have a trusted environment for practitioners and end-users in cybersecurity to share information, lessons learned and best practices to increase cyber resilience of European companies and organisations, it is essential to receive input from Cybersecurity Risk Managers. In this working Group, they may engage with ECSO’s CISO Community, the SOC/CTI Task Force, and experts within the NIS2 Directive. More [HERE](#).
Resources from our Members
Cybersecurity Risk Manager

Today's risks are complex and interconnected, with new risks emerging rapidly. Volatility is increasing, along with regulatory pressure. We have seen major disruptions to business cycles over the last three decades, including the dot-com crash, the global financial crisis and the recent Covid-19 pandemic. Volatility seems likely to increase, along with threats from known and unknown places. Regulation is unlikely to become less complex or less demanding. In this environment, every organisation needs to improve its risk management capabilities.

We work with Chief Finance Officers, Chief Risk Officers and other senior risk and compliance executives to help them manage their risk agenda across five key areas: Cyber Risk, Operational Risk & Resilience, Fraud & Financial Crime, Regulatory & Compliance and Financial Risk.

|| Interesting finding: Cyber transformers are six times more likely than the rest to apply leading risk management practices (65% vs. 11%) read more here and on our State of Cybersecurity Resilience 2023 report.

- Compliance Risk Study - 2022 | Accenture
- Call for change: Managing ICT governance and risk – UNIQA Case Study
- The Cyber-Resilient CEO (accenture.com)
In today's digital world, managing cyber risks has become increasingly crucial, and the energy sector is particularly vulnerable to cyber-attacks. These attacks can have severe consequences for both energy supply and public safety. Operators managing critical infrastructures in the energy sector must remain vigilant and protect against cyber threats. To help EPES (Electrical Power and Energy Systems) operators with this task, the CyberSEAS research project develops a risk assessment tool. The tool follows the guidelines set by the ISO31000 standard and includes several steps. It identifies assets using MITRE ATT&CK mapping, it assesses asset vulnerabilities using the Common Vulnerability Scoring System and a Cyber Maturity Model questionnaire. It also calculates probability and financial impacts, identifies risk profiles to prioritise, and identifies countermeasures based on cost-benefit analysis. This tool can help energy operators understand the potential risks and impacts of cyber-attacks and provide a systematic approach to managing and mitigating them.

I am interested in learning more HERE.
Learn new skills and what it’s like to be a Cybersecurity Risk Manager! (FOR FREE!)

The Cybersecurity Career Path is part of the Cybersecurity Learning Hub which is an initiative designed to tackle the global cybersecurity skills shortage. Hosted on Trailhead, Salesforce’s learning platform, it provides over 70 free courses with career oriented information, expert interviews and training modules. Take the Cybersecurity Risk Manager Trailmix to learn how and what it’s like to manage risks associated with digital business assets. You can also check out other cybersecurity roles and learn vital skills for free whilst you’re there!
CGRC Certification - The CGRC certification is a proven way to demonstrate your knowledge and skills to integrate governance, performance management, risk management and regulatory compliance within your organisation. Learn how to utilise frameworks to integrate security and privacy within organisational objectives, better enabling stakeholders to make informed decisions regarding data security, compliance, supply chain risk management and more.

Risk Manager Practitioner Certificates - The ISC2 risk management certificates provide an understanding of how to assess and analyse risk, and take a deeper dive into standards and risk methods to ensure cybersecurity practitioners are ready for success. There are three risk manager practitioner certificates available.

Governance Risk and Compliance Skill Builders - ISC2 offers 11 skill builders on cybersecurity risk management that are created by industry experts and available now on demand. Earn CPE Credits with these short-format learning courses.
Resources from the Community
In today’s hyper-connected world, where technology fuels every aspect of our lives, the need for robust cybersecurity measures has never been more critical. Businesses, governments, and individuals are increasingly reliant on digital infrastructures, making them susceptible to a myriad of cyber threats. In this context, the role of a cybersecurity risk manager emerges as a keystone, ensuring the security and resilience of organisations against evolving threats. More HERE.

The Role of a Cybersecurity Risk Manager in the Modern Digital Landscape

We define cybersecurity strategies, consulting and regulatory alignment to security frameworks. Also, we implement methodologies and execute services of analysis and risks management, DRP, BCP, BIA/RIA. We rely on our Insside Security Suite platform (ISS), Risk Management Module. Learn more HERE.

Governance, Risk & Management

We define cybersecurity strategies, consulting and regulatory alignment to security frameworks. Also, we implement methodologies and execute services of analysis and risks management, DRP, BCP, BIA/RIA. We rely on our Insside Security Suite platform (ISS), Risk Management Module. Learn more HERE.
Cybersecurity Risk Managers play a crucial role in ensuring organizational safety amidst digital chaos. One indispensable tool in their arsenal is Digital Forensics and Incident Response (DFIR). DFIR isn't just a theoretical concept; it involves diving hands-on, quite literally, into the digital realm. By gaining in-depth knowledge of DFIR, Cybersecurity Risk Managers transform into digital detectives, comprehending the nuances of cyberattacks and mastering the techniques to combat them. itrainsec offers online training that equips teams and individuals with this essential knowledge. More HERE.

BLINDSPOT: Game-changing Risk Intelligence at Your Fingerprints

BLINDSPOT is a next-generation risk intelligence platform, created with the goal of providing users with a holistic assessment of any organization's cyber risk level. In the growing landscape of sophisticated supply chain attacks, we understood the need to oversee the interconnected systems between organizations and their suppliers, vendors, and third and fourth parties. The platform monitors contemporary incidents and predicts subsequent adversarial activities - therefore preventing software and physical supply-chain attacks and detrimental breaches worldwide. See more HERE.
Thank you for your time!

The Cybersecurity Awareness Calendar is an initiative launched by:
European Cyber Security Organisation (ECSO)
Avenue des Arts 46
1000, Brussels

@ecso_eu
cCompany/ecso-cyber-security
www.ecs-org.eu
secretariat@ecs-org.eu