Bạn sẽ tìm hiểu về các khuôn khổ và biện pháp kiểm soát bảo mật được sử dụng để giảm thiểu rủi ro cho tổ chức. Bạn sẽ đề cập đến các nguyên tắc của bộ ba CIA và các khuôn khổ khác nhau của Viện Tiêu chuẩn và Công nghệ Quốc gia (NIST). Ngoài ra, bạn sẽ khám phá đạo đức bảo mật.

# **Mục tiêu học tập**

* Xác định khung bảo mật và kiểm soát
* Xác định bộ ba CIA và NIST CSF
* Thảo luận cách sử dụng bộ ba CIA và NIST CSF để phát triển các thủ tục và quy trình nhằm giải quyết các mối đe dọa, rủi ro và lỗ hổng bảo mật
* Giải thích đạo đức bảo mật

# **Frameworks và kiểm soát**

## **Chào mừng đến với mô-đun 3**

|  |
| --- |
| **Welcome to module 3**  Hi there, glad to have you back! You're halfway done with the first course, so you're making great progress. |

Chào mừng đến với mô-đun 3

Xin chào, rất vui vì bạn đã trở lại!Bạn đã hoàn thành được một nửa khóa học đầu tiên, vì vậy bạn đang tiến bộ rất nhiều.

|  |
| --- |
| In this section, we'll discuss how organizations protect themselves from threats, risks, and vulnerabilities by covering key principles such as: frameworks, controls, and ethics. To help you better understand how this relates to the role of a security analyst, we'll use an analogy. |

Trong phần này,chúng ta sẽ thảo luận về cách các tổ chức tự bảo vệ mình khỏi các mối đe dọa, rủi ro vàcác lỗ hổng bằng cách đề cập đến các nguyên tắc chính như: khuôn khổ, biện pháp kiểm soát và đạo đức.Để giúp bạn hiểu rõ hơn điều này liên quan như thế nào đến vai trò của nhà phân tích bảo mật,chúng ta sẽ sử dụng một sự tương tự.

|  |
| --- |
| Imagine you want to plant a garden. You research, plan, prepare, and purchase materials while considering all the things that could potentially present a risk to your garden. You establish a plan to pull weeds, spray for bugs, and water your plants regularly to prevent issues or incidents. But as the days go by, unexpected problems arise. The weather has been unpredictable and pests have been aggressively trying to infiltrate your garden. |

Hãy tưởng tượng bạn muốn trồng một khu vườn. Bạn nghiên cứu, lập kế hoạch, chuẩn bị,và mua vật liệu trong khi xem xét tất cả những thứ có thểcó khả năng gây nguy hiểm cho khu vườn của bạn.Bạn lập kế hoạch nhổ cỏ, phun thuốc trừ sâu,và tưới nước cho cây thường xuyên để ngăn ngừa các vấn đề hoặc sự cố.Nhưng ngày tháng trôi qua, những vấn đề bất ngờ nảy sinh.Thời tiết diễn biến khó lường vàsâu bệnh đang tích cực cố gắng xâm nhập vào khu vườn của bạn.

|  |
| --- |
| You start implementing better ways to safeguard your garden by installing a surveillance camera, building a fence, and covering your plants with a canopy to keep your garden healthy and growing. Now that you have a better idea about the threats to your garden and how to keep your plants safe, you establish better policies and procedures to continuously monitor and safeguard your garden. |

Bạn bắt đầu thực hiện những cách tốt hơn để bảo vệ khu vườn của mình bằng cách lắp đặtcamera giám sát, xây hàng rào vàche phủ cây của bạn bằng một tán cây để giữ cho khu vườn của bạn khỏe mạnh và phát triển.Bây giờ bạn đã có ý tưởng tốt hơn về các mối đe dọa đối với khu vườn của bạn vàlàm thế nào để giữ cho cây trồng của bạn được an toàn,bạn thiết lập các chính sách và thủ tục tốt hơn để liên tục theo dõi vàbảo vệ khu vườn của bạn.

|  |
| --- |
| In this way, security resembles a garden. It's an evolving industry that will challenge you to make continuous improvements to policies and procedures that help protect your organization and the people it serves. |

Theo cách này, an ninh giống như một khu vườn.Đó là một ngành đang phát triển sẽ thách thức bạn thực hiện liên tụccải tiến các chính sách và thủ tục giúp bảo vệ tổ chức của bạn vànhững người mà nó phục vụ.

|  |
| --- |
| To that end, we'll introduce security frameworks and controls and explain why they're important. We'll also cover core components and specific examples of frameworks and controls, including the Confidentiality, Integrity, and Availability Triad, or CIA Triad. We'll end with the discussion about the ethics of security and share a few notable ethical concerns in the security field. |

Để đạt được mục đích đó, chúng tôi sẽ giới thiệu các khung bảo mật vàkiểm soát và giải thích tại sao chúng quan trọng.Chúng tôi cũng sẽ đề cập đến các thành phần cốt lõi và các ví dụ cụ thể về khung vàkiểm soát, bao gồm tính bảo mật, tính toàn vẹn vàBộ ba sẵn có hoặc Bộ ba CIA.Chúng ta sẽ kết thúc bằng cuộc thảo luận về đạo đức của an ninh vàchia sẻ một số mối quan tâm đạo đức đáng chú ý trong lĩnh vực bảo mật.

|  |
| --- |
| Evolving security practices may seem a little abstract, but many of us use them every day. For example, I use security keys, which are a type of security control, as a second form of authentication to access my accounts. The keys ensure that only I can access my accounts, even if a password has been compromised. By improving confidentiality, they also assure me that the integrity of my accounts is intact. |

Các biện pháp bảo mật ngày càng phát triển có vẻ hơi trừu tượng, nhưngnhiều người trong chúng ta sử dụng chúng hàng ngày.Ví dụ: tôi sử dụng khóa bảo mật, một loại kiểm soát bảo mật,như một hình thức xác thực thứ hai để truy cập vào tài khoản của tôi.Các khóa đảm bảo rằng chỉ tôi mới có thể truy cập vào tài khoản của mình,ngay cả khi mật khẩu đã bị xâm phạm.Bằng cách cải thiện tính bảo mật,họ cũng đảm bảo với tôi rằng tính toàn vẹn của tài khoản của tôi vẫn nguyên vẹn.

|  |
| --- |
| Having processes and procedures in place to organize security efforts and make informed decisions is important for any organization. I'm so excited to get started, and I hope you are too! |

Có sẵn các quy trình và thủ tục để tổ chức các nỗ lực bảo mật vàđưa ra quyết định sáng suốt là quan trọng đối với bất kỳ tổ chức nào.Tôi rất háo hức được bắt đầu và tôi hy vọng bạn cũng vậy!

## **Giới thiệu về khung bảo mật và kiểm soát**

|  |
| --- |
| **Introduction to security frameworks and controls**  Imagine you're working as a security analyst and receive multiple alerts about suspicious activity on the network. You realize that you'll need to implement additional security measures to keep these alerts from becoming serious incidents. But where do you start? |

**Giới thiệu về khung bảo mật và kiểm soát**

Hãy tưởng tượng bạn đang làm việc như một nhà phân tích chứng khoán và nhận đượcnhiều cảnh báo về hoạt động đáng ngờ trên mạng.Bạn nhận ra rằng bạn sẽ cần phải thực hiệncác biện pháp an ninh bổ sung để giữnhững cảnh báo này trở thànhsự cố nghiêm trọng. Nhưng bạn bắt đầu ở đâu?

|  |
| --- |
| As an analyst, you'll start by identifying your organization's critical assets and risks. Then you'll implement the necessary frameworks and controls. |

Là một nhà phân tích, bạn sẽ bắt đầu bằng việc xác địnhtài sản và rủi ro quan trọng của tổ chức bạn.Sau đó bạn sẽ thực hiệncác khuôn khổ và biện pháp kiểm soát cần thiết.

|  |
| --- |
| In this video, we'll discuss how security professionals use frameworks to continuously identify and manage risk. We'll also cover how to use security controls to manage or reduce specific risks. |

Trong video này, chúng ta sẽ thảo luận về cách các chuyên gia bảo mậtsử dụng các khuôn khổ để liên tục xác định và quản lý rủi ro.Chúng tôi cũng sẽ đề cập đến cách sử dụngkiểm soát an ninh để quản lý hoặc giảm thiểu rủi ro cụ thể.

|  |
| --- |
| Security frameworks are guidelines used for building plans to help mitigate risks and threats to data and privacy. Security frameworks provide a structured approach to implementing a security lifecycle. The security lifecycle is a constantly evolving set of policies and standards that define how an organization manages risks, follows established guidelines, and meets regulatory compliance, or laws. |

Khung bảo mật là hướng dẫnđược sử dụng để xây dựng kế hoạchđể giúp giảm thiểu rủi ro và mối đe dọa đối với dữ liệu và quyền riêng tư.Khung bảo mật cung cấp một cách tiếp cận có cấu trúcđể thực hiện vòng đời bảo mật.Vòng đời bảo mật làmột loạt các chính sách không ngừng phát triểnvà các tiêu chuẩn xác địnhcách tổ chức quản lý rủi ro,tuân theo các hướng dẫn đã được thiết lập,và đáp ứng sự tuân thủ quy định hoặc pháp luật.

|  |
| --- |
| There are several security frameworks that may be used to manage different types of organizational and regulatory compliance risks. The purpose of security frameworks include protecting personally identifiable information, known as PII, securing financial information, identifying security weaknesses, managing organizational risks, and aligning security with business goals. |

Có một số khung bảo mậtcó thể được sử dụng để quản lýcác loại hình tổ chức khác nhauvà rủi ro tuân thủ quy định.Mục đích của khung bảo mật bao gồm việc bảo vệthông tin nhận dạng cá nhân, được gọi là PII,đảm bảo thông tin tài chính,xác định điểm yếu về bảo mật,quản lý rủi ro tổ chức,và điều chỉnh bảo mật với mục tiêu kinh doanh.

|  |
| --- |
| Frameworks have four core components and understanding them will allow you to better manage potential risks. The first core component is identifying and documenting security goals. For example, an organization may have a goal to align with the E.U.'s General Data Protection Regulation, also known as GDPR. GDPR is a data protection law established to grant European citizens more control over their personal data. A security analyst may be asked to identify and document areas where an organization is out of compliance with GDPR. |

Các khung có bốn thành phần cốt lõi vàhiểu chúng sẽ cho phép bạnquản lý tốt hơn các rủi ro tiềm ẩn.Thành phần cốt lõi đầu tiên làxác định và ghi lại các mục tiêu bảo mật.Ví dụ: một tổ chức có thể có mục tiêu làphù hợp với Quy định bảo vệ dữ liệu chung của EU,còn được gọi là GDPR.GDPR là luật bảo vệ dữ liệu được thiết lập đểtrao cho công dân châu Âu nhiều quyền kiểm soát hơntrên dữ liệu cá nhân của họ.Một nhà phân tích bảo mật có thể được yêu cầu xác định và ghi lạilĩnh vực mà một tổ chứckhông tuân thủ GDPR.

|  |
| --- |
| The second core component is setting guidelines to achieve security goals. For example, when implementing guidelines to achieve GDPR compliance, your organization may need to develop new policies for how to handle data requests from individual users. |

Thành phần cốt lõi thứ hai là thiết lậphướng dẫn để đạt được mục tiêu an ninh.Chẳng hạn, khi triển khaihướng dẫn để đạt được sự tuân thủ GDPR,tổ chức của bạn có thể cần phát triểnchính sách mới về cách xử lýyêu cầu dữ liệu từ người dùng cá nhân.

|  |
| --- |
| The third core component of security frameworks is implementing strong security processes. In the case of GDPR, a security analyst working for a social media company may help design procedures to ensure the organization complies with verified user data requests. An example of this type of request is when a user attempts to update or delete their profile information. |

Thành phần cốt lõi thứ ba của khung bảo mật làthực hiện các quy trình bảo mật mạnh mẽ.Trong trường hợp GDPR,một nhà phân tích bảo mật làm việc chomột công ty truyền thông xã hội có thể giúp thiết kếcác thủ tục để đảm bảo tổ chứctuân thủ các yêu cầu dữ liệu người dùng đã được xác minh.Một ví dụ về loại yêu cầu này là khi người dùngcố gắng cập nhật hoặc xóa thông tin hồ sơ của họ.

|  |
| --- |
| The last core component of security frameworks is monitoring and communicating results. As an example, you may monitor your organization's internal network and report a potential security issue affecting GDPR to your manager or regulatory compliance officer. |

Thành phần cốt lõi cuối cùng củakhuôn khổ bảo mật làtheo dõi và thông báo kết quả.Ví dụ, bạn có thể theo dõimạng nội bộ của tổ chức bạn và báo cáomột vấn đề bảo mật tiềm ẩn ảnh hưởng đếnGDPR cho người quản lý hoặc nhân viên tuân thủ quy định của bạn.

|  |
| --- |
| Now that we've introduced the four core components of security frameworks, let's tie them all together. Frameworks allow analysts to work alongside other members of the security team to document, implement, and use the policies and procedures that have been created. It's essential for an entry-level analyst to understand this process because it directly affects the work they do and how they collaborate with others. Next, we'll discuss security controls. |

Bây giờ chúng tôi đã giới thiệubốn thành phần cốt lõi của khung bảo mật,chúng ta hãy buộc tất cả chúng lại với nhau.Các khung cho phép các nhà phân tích làm việc cùng vớicác thành viên khác của đội an ninh để ghi lại,thực hiện và sử dụng các chính sáchvà các thủ tục đã được tạo ra.Điều cần thiết đối với một nhà phân tích cấp đầu vào là phải hiểuQuá trình này vì nó ảnh hưởng trực tiếpcông việc họ làm và cách họ cộng tác với người khác.Tiếp theo, chúng ta sẽ thảo luận về các biện pháp kiểm soát bảo mật.

|  |
| --- |
| Security controls are safeguards designed to reduce specific security risks. For example, your company may have a guideline that requires all employees to complete a privacy training to reduce the risk of data breaches. As a security analyst, you may use a software tool to automatically assign and track which employees have completed this training. |

Kiểm soát an ninh là biện pháp bảo vệđược thiết kế để giảm thiểu rủi ro bảo mật cụ thể.Ví dụ: công ty của bạncó thể có một hướng dẫn yêu cầutất cả nhân viên phải hoàn thànhđào tạo về quyền riêng tư để giảm nguy cơ vi phạm dữ liệu.Là một nhà phân tích chứng khoán,bạn có thể sử dụng một công cụ phần mềm để tự độngchỉ định và theo dõi cái nàonhân viên đã hoàn thành khóa đào tạo này.

|  |
| --- |
| Security frameworks and controls are vital to managing security for all types of organizations and ensuring that everyone is doing their part to maintain a low level of risk. |

Các khuôn khổ và biện pháp kiểm soát bảo mật đượcquan trọng để quản lý an ninh cho tất cả các loạitổ chức và đảm bảo rằng mọi người đềuthực hiện phần việc của mình để duy trì mức độ rủi ro thấp.

|  |
| --- |
| Understanding their purpose and how they are used allows analysts to support an organization's security goals and protect the people it serves. |

Hiểu mục đích của họ và làm thế nàochúng được sử dụng cho phép các nhà phân tíchhỗ trợ các mục tiêu bảo mật của tổ chứcvà bảo vệ những người mà nó phục vụ.

|  |
| --- |
| In the following videos, we'll discuss some well-known frameworks and principles that analysts need to be aware of to minimize risk and protect data and users. |

Trong các video tiếp theo,chúng ta sẽ thảo luận về một số framework nổi tiếngvà những nguyên tắc mà nhà phân tích cần phảilưu ý để giảm thiểu rủi ro và bảo vệ dữ liệu và người dùng.

## **Thiết kế an toàn**

|  |
| --- |
| **Secure design**  Hi, welcome back! Previously, we discussed frameworks and controls in general. In this video, you'll learn about specific frameworks and controls that organizations can voluntarily use to minimize risks to their data and to protect users. Let's get started! |

**Thiết kế an toàn**

Xin chào, chào mừng trở lại!Trước đây, chúng ta đã thảo luận về các khuôn khổvà điều khiển nói chung.Trong video này, bạn sẽ tìm hiểu vềcác khuôn khổ và biện pháp kiểm soát cụ thể mà các tổ chứccó thể tự nguyện sử dụng để giảm thiểurủi ro đối với dữ liệu của họ và để bảo vệ người dùng.Bắt đầu nào!

|  |
| --- |
| The CIA triad is a foundational model that helps inform how organizations consider risk when setting up systems and security policies. CIA stands for confidentiality, integrity, and availability. |

Bộ ba CIA là một mô hình nền tảnggiúp thông báo cách các tổ chức xem xétrủi ro khi thiết lập hệ thống và chính sách bảo mật.CIA là viết tắt của bí mật,tính toàn vẹn và tính sẵn sàng.

|  |
| --- |
| Confidentiality means that only authorized users can access specific assets or data. For example, strict access controls that define who should and should not have access to data, must be put in place to ensure confidential data remains safe. |

Tính bí mật có nghĩa là chỉ những người dùng được ủy quyền mớicó thể truy cập vào tài sản hoặc dữ liệu cụ thể.Ví dụ: kiểm soát truy cập nghiêm ngặtxác định ai nên và không nên có quyền truy cập vào dữ liệu,phải được đặt ra để đảm bảodữ liệu bí mật vẫn được an toàn.

|  |
| --- |
| Integrity means the data is correct, authentic, and reliable. To maintain integrity, security professionals can use a form of data protection like encryption to safeguard data from being tampered with. |

Tính toàn vẹn có nghĩa là dữ liệu đượcchính xác, xác thực và đáng tin cậy.Để duy trì tính toàn vẹn,các chuyên gia bảo mật có thể sử dụng một hình thứcbảo vệ dữ liệu như mã hóađể bảo vệ dữ liệu khỏi bị giả mạo.

|  |
| --- |
| Availability means data is accessible to those who are authorized to access it. Let's define a term that came up during our discussion of the CIA triad: |

Tính sẵn sàng có nghĩa là dữ liệu đượccó thể truy cập được đối với những người được phép truy cập nó.Hãy định nghĩa một thuật ngữ xuất hiện trongcuộc thảo luận của chúng tôi về bộ ba CIA:

|  |
| --- |
| asset. |

tài sản.

|  |
| --- |
| An asset is an item perceived as having value to an organization. |

Tài sản là một vật phẩm được coi là có giá trị đối với một tổ chức.

|  |
| --- |
| And value is determined by the cost associated with the asset in question. |

Và giá trị được xác định bởi chi phíliên quan đến tài sản được đề cập.

|  |
| --- |
| For example, an application that stores sensitive data, such as social security numbers or bank accounts, is a valuable asset to an organization. It carries more risk and therefore requires tighter security controls in comparison to a website that shares publicly available news content. As you may remember, earlier in the course, we discussed frameworks and controls in general. Now, we'll discuss a specific framework developed by the U.S.-based National Institute of Standards and Technology: the Cybersecurity Framework, also referred to as the NIST CSF. The NIST Cybersecurity Framework is a voluntary framework that consists of standards, guidelines, and best practices to manage cybersecurity risk. |

Ví dụ: một ứng dụng lưu trữ dữ liệu nhạy cảm,chẳng hạn như số an sinh xã hội hoặc tài khoản ngân hàng,là tài sản có giá trị đối với một tổ chức.Nó mang lại nhiều rủi ro hơn và do đó đòi hỏiso sánh kiểm soát an ninh chặt chẽ hơnđến một trang web chia sẻ nội dung tin tức có sẵn công khai.Như bạn có thể nhớ,trước đó trong khóa học,chúng tôi đã thảo luận về các khuôn khổ và biện pháp kiểm soát nói chung.Bây giờ, chúng ta sẽ thảo luận về một framework cụ thể được phát triển bởiNational có trụ sở tại Hoa KỳViện Tiêu chuẩn và Công nghệ:Khung An ninh mạng, cũngđược gọi là NIST CSF.Khung an ninh mạng NIST làmột khuôn khổ tự nguyện bao gồm các tiêu chuẩn,hướng dẫn và thực tiễn tốt nhấtđể quản lý rủi ro an ninh mạng.

|  |
| --- |
| It's important to become familiar with this framework because security teams use it as |

Điều quan trọng là phải làm quen với khuôn khổ nàybởi vì đội an ninh sử dụng nó như

|  |
| --- |
| a baseline to manage short and long-term risk. Managing and mitigating risks and protecting an organization's assets from threat actors are key goals for security professionals. Understanding the different motives a threat actor may have, alongside identifying your organization's most valuable assets is important. Some of the most dangerous threat actors to consider are disgruntled employees. They are the most dangerous because they often have access to sensitive information and know where to find it. In order to reduce this type of risk, security professionals would use the principle of availability, as well as organizational guidelines based on frameworks to ensure staff members can only access the data they need to perform their jobs. |

cơ sở để quản lý rủi ro ngắn hạn và dài hạn.Quản lý và giảm thiểu rủi ro và bảo vệtài sản của một tổ chức từCác tác nhân đe dọa là mục tiêu chính của các chuyên gia bảo mật.Hiểu các động cơ khác nhaumột kẻ đe dọa có thể có,cùng với việc xác định tổ chức của bạntài sản có giá trị nhất là quan trọng.Một số tác nhân đe dọa nguy hiểm nhấtcần xem xét là những nhân viên bất mãn.Chúng nguy hiểm nhất vì chúng thường cótruy cập thông tin nhạy cảmvà biết tìm nó ở đâu.Để hạn chế loại rủi ro này,các chuyên gia bảo mật sẽ sử dụngnguyên tắc sẵn có,cũng như các hướng dẫn tổ chứcdựa trên các khuôn khổ để đảm bảonhân viên chỉ có thể truy cậpdữ liệu họ cần để thực hiện công việc của mình.

|  |
| --- |
| Threat actors originate from all across the globe, and a diverse workforce of security professionals helps organizations identify attackers' intentions. A variety of perspectives can assist organizations in understanding and mitigating the impact of malicious activity. That concludes our introduction to the CIA triad and NIST CSF framework, which are used to develop processes to secure organizations and the people they serve. You may be asked in an interview if you know about security frameworks and principles. Or you may be asked to explain how they're used to secure organizational assets. In either case, throughout this program, you'll have multiple opportunities to learn more about them and apply what we've discussed to real-world situations. Coming up, we'll discuss the ethics of security. See you soon! |

Các tác nhân đe dọa có nguồn gốc từ khắp nơi trên thế giới,và lực lượng lao động đa dạng gồm các chuyên gia bảo mậtgiúp các tổ chức xác định ý định của kẻ tấn công.Nhiều quan điểm khác nhau có thể hỗ trợ các tổ chức tronghiểu biết và giảm nhẹtác động của hoạt động độc hại.Điều đó kết thúc phần giới thiệu của chúng tôi vềbộ ba CIA và khuôn khổ NIST CSF,được sử dụng để phát triển các quy trình nhằmđảm bảo an toàn cho các tổ chức và những người mà họ phục vụ.Bạn có thể được hỏi trong một cuộc phỏng vấn nếu bạnbiết về các khuôn khổ và nguyên tắc bảo mật.Hoặc bạn có thể được yêu cầu giải thích chúng như thế nàođược sử dụng để bảo đảm tài sản của tổ chức.Trong cả hai trường hợp, trong suốt chương trình này,bạn sẽ có nhiều cơ hộiđể tìm hiểu thêm về họvà áp dụng những gì chúng ta đã thảo luận vào các tình huống thực tế.Sắp tới chúng ta sẽ thảo luậnđạo đức của an ninh. Hẹn sớm gặp lại!

## **Kiểm soát, khuôn khổ và tuân thủ**

|  |
| --- |
| **Controls, frameworks, and compliance**  Previously, you were introduced to security frameworks and how they provide a structured approach to implementing a security lifecycle. As a reminder, a security lifecycle is a constantly evolving set of policies and standards. In this reading, you will learn more about how security frameworks, controls, and compliance regulations—or laws—are used together to manage security and make sure everyone does their part to minimize risk. |

**Kiểm soát, khuôn khổ và tuân thủ**

Trước đây, bạn đã được giới thiệu về các khung bảo mật và cách chúng cung cấp cách tiếp cận có cấu trúc để triển khai vòng đời bảo mật. Xin nhắc lại, vòng đời bảo mật là một tập hợp các chính sách và tiêu chuẩn không ngừng phát triển. Trong bài đọc này, bạn sẽ tìm hiểu thêm về cách các khung bảo mật, biện pháp kiểm soát và quy định tuân thủ—hoặc luật—được sử dụng cùng nhau để quản lý bảo mật và đảm bảo mọi người thực hiện phần việc của mình để giảm thiểu rủi ro.

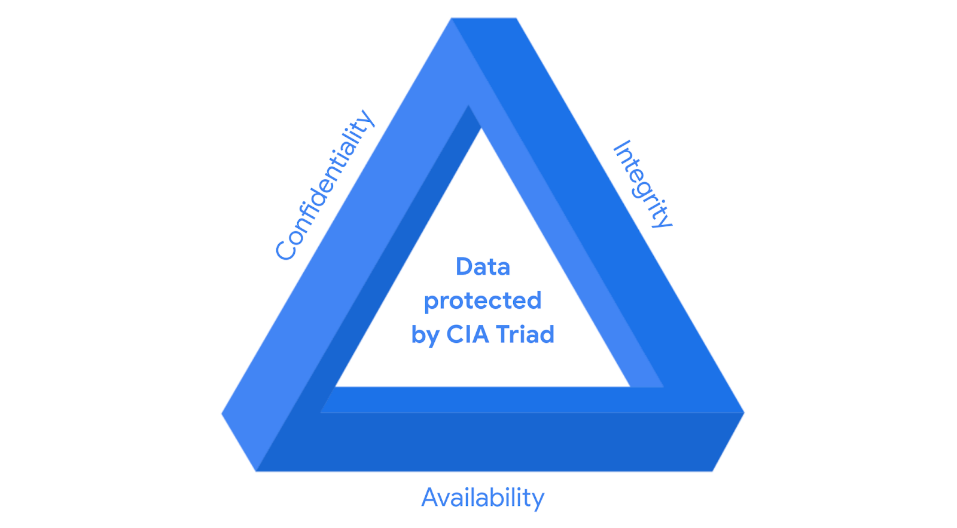
|  |
| --- |
| **How controls, frameworks, and compliance are related**  The **confidentiality, integrity, and availability (CIA) triad** is a model that helps inform how organizations consider risk when setting up systems and security policies.  CIA are the three foundational principles used by cybersecurity professionals to establish appropriate controls that mitigate threats, risks, and vulnerabilities.  As you may recall, security controls are safeguards designed to reduce specific security risks. So they are used alongside frameworks to ensure that security goals and processes are implemented correctly and that organizations meet regulatory compliance requirements. |

**Các biện pháp kiểm soát, khuôn khổ và sự tuân thủ có liên quan như thế nào**

Bộ ba bảo **mật, toàn vẹn và sẵn sàng (CIA)** là mô hình giúp thông báo cách các tổ chức xem xét rủi ro khi thiết lập hệ thống và chính sách bảo mật.

CIA là ba nguyên tắc cơ bản được các chuyên gia an ninh mạng sử dụng để thiết lập các biện pháp kiểm soát thích hợp nhằm giảm thiểu các mối đe dọa, rủi ro và lỗ hổng.

Như bạn có thể nhớ lại, kiểm soát bảo mật là các biện pháp bảo vệ được thiết kế để giảm các rủi ro bảo mật cụ thể. Vì vậy, chúng được sử dụng cùng với các khuôn khổ để đảm bảo rằng các mục tiêu và quy trình bảo mật được triển khai chính xác và các tổ chức đáp ứng các yêu cầu tuân thủ quy định.



|  |
| --- |
| **Security frameworks** are guidelines used for building plans to help mitigate risks and threats to data and privacy. They have four core components:   1. Identifying and documenting security goals 2. Setting guidelines to achieve security goals 3. Implementing strong security processes 4. Monitoring and communicating results   **Compliance** is the process of adhering to internal standards and external regulations. |

**Khung bảo mật** là các nguyên tắc được sử dụng để xây dựng kế hoạch nhằm giúp giảm thiểu rủi ro và mối đe dọa đối với dữ liệu và quyền riêng tư. Chúng có bốn thành phần cốt lõi:

1. Xác định và ghi lại các mục tiêu bảo mật
2. Thiết lập các nguyên tắc để đạt được mục tiêu bảo mật
3. Thực hiện các quy trình bảo mật mạnh mẽ
4. Giám sát và truyền đạt kết quả

**Tuân thủ** là quá trình tuân thủ các tiêu chuẩn nội bộ và các quy định bên ngoài.

|  |
| --- |
| **Specific controls, frameworks, and compliance**  The National Institute of Standards and Technology (NIST) is a U.S.-based agency that develops multiple voluntary compliance frameworks that organizations worldwide can use to help manage risk. The more aligned an organization is with compliance, the lower the risk.  Examples of frameworks include the NIST Cybersecurity Framework (CSF) and the NIST Risk Management Framework (RMF).  **Note:** Specifications and guidelines can change depending on the type of organization you work for.  In addition to the [NIST CSF](https://www.nist.gov/cyberframework) and [NIST RMF](https://csrc.nist.gov/projects/risk-management/about-rmf), there are several other controls, frameworks, and compliance standards that are important for security professionals to be familiar with to help keep organizations and the people they serve safe. |

**Các biện pháp kiểm soát, khuôn khổ và tuân thủ cụ thể**

Viện Tiêu chuẩn và Công nghệ Quốc gia (NIST) là cơ quan có trụ sở tại Hoa Kỳ, phát triển nhiều khuôn khổ tuân thủ tự nguyện mà các tổ chức trên toàn thế giới có thể sử dụng để giúp quản lý rủi ro. Tổ chức càng tuân thủ chặt chẽ thì rủi ro càng thấp.

Ví dụ về các khung bao gồm Khung bảo mật không gian mạng NIST (CSF) và Khung quản lý rủi ro NIST (RMF).

**Lưu ý:** Các thông số kỹ thuật và nguyên tắc có thể thay đổi tùy thuộc vào loại tổ chức mà bạn làm việc.

Ngoài việc[NIST CSF](https://www.nist.gov/cyberframework)Và[NIST RMF](https://csrc.nist.gov/projects/risk-management/about-rmf), có một số biện pháp kiểm soát, khuôn khổ và tiêu chuẩn tuân thủ khác rất quan trọng mà các chuyên gia bảo mật cần phải làm quen để giúp giữ an toàn cho các tổ chức và những người mà họ phục vụ.

|  |
| --- |
| **The Federal Energy Regulatory Commission - North American Electric Reliability Corporation (FERC-NERC)**  FERC-NERC is a regulation that applies to organizations that work with electricity or that are involved with the U.S. and North American power grid. These types of organizations have an obligation to prepare for, mitigate, and report any potential security incident that can negatively affect the power grid. They are also legally required to adhere to the Critical Infrastructure Protection (CIP) Reliability Standards defined by the FERC. |

**Ủy ban Điều tiết Năng lượng Liên bang - Tập đoàn Độ tin cậy Điện Bắc Mỹ (FERC-NERC)**

FERC-NERC là quy định áp dụng cho các tổ chức làm việc trong lĩnh vực điện lực hoặc có liên quan đến lưới điện Hoa Kỳ và Bắc Mỹ. Những loại tổ chức này có nghĩa vụ chuẩn bị, giảm thiểu và báo cáo mọi sự cố an ninh tiềm ẩn có thể ảnh hưởng tiêu cực đến lưới điện. Về mặt pháp lý, họ cũng được yêu cầu phải tuân thủ các Tiêu chuẩn về độ tin cậy của Bảo vệ cơ sở hạ tầng quan trọng (CIP) do FERC xác định.

|  |
| --- |
| **The Federal Risk and Authorization Management Program (FedRAMP®)**  FedRAMP is a U.S. federal government program that standardizes security assessment, authorization, monitoring, and handling of cloud services and product offerings. Its purpose is to provide consistency across the government sector and third-party cloud providers. |

**Chương trình quản lý rủi ro và ủy quyền liên bang (FedRAMP®)**

FedRAMP là chương trình của chính phủ liên bang Hoa Kỳ nhằm tiêu chuẩn hóa việc đánh giá, ủy quyền, giám sát và xử lý các dịch vụ đám mây và sản phẩm. Mục đích của nó là cung cấp sự nhất quán trong toàn bộ khu vực chính phủ và các nhà cung cấp đám mây bên thứ ba.

|  |
| --- |
| **Center for Internet Security (CIS®)**  CIS is a nonprofit with multiple areas of emphasis. It provides a set of controls that can be used to safeguard systems and networks against attacks. Its purpose is to help organizations establish a better plan of defense. CIS also provides actionable controls that security professionals may follow if a security incident occurs. |

**Trung tâm An ninh Internet (CIS®)**

CIS là một tổ chức phi lợi nhuận tập trung vào nhiều lĩnh vực. Nó cung cấp một bộ điều khiển có thể được sử dụng để bảo vệ hệ thống và mạng khỏi các cuộc tấn công. Mục đích của nó là giúp các tổ chức thiết lập một kế hoạch phòng thủ tốt hơn. CIS cũng cung cấp các biện pháp kiểm soát hữu ích mà các chuyên gia bảo mật có thể tuân theo nếu xảy ra sự cố bảo mật.

|  |
| --- |
| **General Data Protection Regulation (GDPR)**  GDPR is a European Union (E.U.) general data regulation that protects the processing of E.U. residents’ data and their right to privacy in and out of E.U. territory. For example, if an organization is not being transparent about the data they are holding about an E.U. citizen and why they are holding that data, this is an infringement that can result in a fine to the organization. Additionally, if a breach occurs and an E.U. citizen’s data is compromised, they must be informed. The affected organization has 72 hours to notify the E.U. citizen about the breach. |

**Quy định chung về bảo vệ dữ liệu (GDPR)**

GDPR là quy định dữ liệu chung của Liên minh Châu Âu (EU) nhằm bảo vệ việc xử lý dữ liệu của cư dân EU và quyền riêng tư của họ trong và ngoài lãnh thổ EU. Ví dụ: nếu một tổ chức không minh bạch về dữ liệu họ đang nắm giữ về một công dân EU và lý do họ nắm giữ dữ liệu đó, thì đây là hành vi vi phạm có thể dẫn đến phạt tiền đối với tổ chức. Ngoài ra, nếu xảy ra vi phạm và dữ liệu của công dân EU bị xâm phạm, họ phải được thông báo. Tổ chức bị ảnh hưởng có 72 giờ để thông báo cho công dân EU về hành vi vi phạm.

|  |
| --- |
| **Payment Card Industry Data Security Standard (PCI DSS)**  PCI DSS is an international security standard meant to ensure that organizations storing, accepting, processing, and transmitting credit card information do so in a secure environment. The objective of this compliance standard is to reduce credit card fraud. |

**Tiêu chuẩn bảo mật dữ liệu ngành thẻ thanh toán (PCI DSS)**

PCI DSS là một tiêu chuẩn bảo mật quốc tế nhằm đảm bảo rằng các tổ chức lưu trữ, chấp nhận, xử lý và truyền thông tin thẻ tín dụng thực hiện trong một môi trường an toàn. Mục tiêu của tiêu chuẩn tuân thủ này là giảm gian lận thẻ tín dụng.

|  |
| --- |
| **The Health Insurance Portability and Accountability Act (HIPAA)**  HIPAA is a U.S. federal law established in 1996 to protect patients' health information. This law prohibits patient information from being shared without their consent. It is governed by three rules:   1. Privacy 2. Security 3. Breach notification   Organizations that store patient data have a legal obligation to inform patients of a breach because if patients' **Protected Health Information** (PHI) is exposed, it can lead to identity theft and insurance fraud. PHI relates to the past, present, or future physical or mental health or condition of an individual, whether it’s a plan of care or payments for care. Along with understanding HIPAA as a law, security professionals also need to be familiar with the Health Information Trust Alliance (HITRUST®), which is a security framework and assurance program that helps institutions meet HIPAA compliance. |

**Đạo luật về trách nhiệm giải trình và cung cấp bảo hiểm y tế (HIPAA)**

HIPAA là luật liên bang Hoa Kỳ được thành lập năm 1996 để bảo vệ thông tin sức khỏe của bệnh nhân. Luật này cấm chia sẻ thông tin của bệnh nhân mà không có sự đồng ý của họ. Nó được điều chỉnh bởi ba quy tắc:

1. Sự riêng tư
2. Bảo vệ
3. Thông báo vi phạm

Các tổ chức lưu trữ dữ liệu bệnh nhân có nghĩa vụ pháp lý phải thông báo cho bệnh nhân về hành vi vi phạm vì nếu **Thông tin sức khỏe được bảo vệ** (PHI) của bệnh nhân bị lộ, điều đó có thể dẫn đến hành vi trộm cắp danh tính và gian lận bảo hiểm. PHI liên quan đến sức khỏe hoặc tình trạng thể chất hoặc tinh thần trong quá khứ, hiện tại hoặc tương lai của một cá nhân, cho dù đó là kế hoạch chăm sóc hay thanh toán cho việc chăm sóc. Cùng với việc hiểu HIPAA như một luật, các chuyên gia bảo mật cũng cần phải làm quen với Liên minh tin cậy thông tin y tế (HITRUST®), đây là một khuôn khổ bảo mật và chương trình đảm bảo giúp các tổ chức đáp ứng tuân thủ HIPAA.

|  |
| --- |
| **International Organization for Standardization (ISO)**  ISO was created to establish international standards related to technology, manufacturing, and management across borders. It helps organizations improve their processes and procedures for staff retention, planning, waste, and services. |

**Tổ chức Tiêu chuẩn hóa Quốc tế (ISO)**

ISO được tạo ra để thiết lập các tiêu chuẩn quốc tế liên quan đến công nghệ, sản xuất và quản lý xuyên biên giới. Nó giúp các tổ chức cải thiện quy trình và thủ tục của họ trong việc giữ chân nhân viên, lập kế hoạch, lãng phí và dịch vụ.

|  |
| --- |
| **System and Organizations Controls (SOC type 1, SOC type 2)**  The American Institute of Certified Public Accountants® (AICPA) auditing standards board developed this standard. The SOC1 and SOC2 are a series of reports that focus on an organization's user access policies at different organizational levels such as:   * Associate * Supervisor * Manager * Executive * Vendor * Others   They are used to assess an organization’s financial compliance and levels of risk. They also cover confidentiality, privacy, integrity, availability, security, and overall data safety. Control failures in these areas can lead to fraud. |

**Kiểm soát hệ thống và tổ chức (SOC loại 1, SOC loại 2)**

Hội đồng tiêu chuẩn kiểm toán của Viện Kế toán Công chứng® Hoa Kỳ (AICPA) đã phát triển tiêu chuẩn này. SOC1 và SOC2 là một loạt báo cáo tập trung vào chính sách truy cập người dùng của tổ chức ở các cấp tổ chức khác nhau, chẳng hạn như:

* Kết hợp
* Người giám sát
* Giám đốc
* Điều hành
* Người bán
* Người khác

Chúng được sử dụng để đánh giá mức độ tuân thủ tài chính và mức độ rủi ro của tổ chức. Chúng cũng bao gồm tính bảo mật, quyền riêng tư, tính toàn vẹn, tính khả dụng, bảo mật và an toàn dữ liệu tổng thể. Kiểm soát thất bại trong các lĩnh vực này có thể dẫn đến gian lận.

|  |
| --- |
| **Pro tip**: There are a number of regulations that are frequently revised. You are encouraged to keep up-to-date with changes and explore more frameworks, controls, and compliance. Two suggestions to research: the Gramm-Leach-Bliley Act and the Sarbanes-Oxley Act. |

**Mẹo chuyên nghiệp** : Có một số quy định thường xuyên được sửa đổi. Bạn được khuyến khích cập nhật các thay đổi và khám phá thêm các khuôn khổ, biện pháp kiểm soát và tuân thủ. Hai gợi ý nghiên cứu: Đạo luật Gramm-Leach-Bliley và Đạo luật Sarbanes-Oxley.

|  |
| --- |
| **United States Presidential Executive Order 14028**  On May 12, 2021, President Joe Biden released an executive order related to improving the nation’s cybersecurity to remediate the increase in threat actor activity. Remediation efforts are directed toward federal agencies and third parties with ties to U.S. [critical infrastructure](https://csrc.nist.gov/glossary/term/critical_infrastructure#:~:text=Definition(s)%3A,any%20combination%20of%20those%20matters.). For additional information, review the [Executive Order on Improving the Nation’s Cybersecurity](https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/). |

**Sắc lệnh hành pháp của Tổng thống Hoa Kỳ 14028**

Vào ngày 12 tháng 5 năm 2021, Tổng thống Joe Biden đã ban hành lệnh hành pháp liên quan đến việc cải thiện an ninh mạng của quốc gia nhằm khắc phục sự gia tăng hoạt động của các tác nhân đe dọa. Các nỗ lực khắc phục được hướng tới các cơ quan liên bang và các bên thứ ba có quan hệ với Hoa Kỳ[cơ sở hạ tầng quan trọng](https://csrc.nist.gov/glossary/term/critical_infrastructure#:~:text=Definition(s)%3A,any%20combination%20of%20those%20matters.). Để biết thêm thông tin, hãy xem lại[Sắc lệnh hành pháp về cải thiện an ninh mạng quốc gia](https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/).

|  |
| --- |
| **Key takeaways**  In this reading you learned more about controls, frameworks, and compliance. You also learned how they work together to help organizations maintain a low level of risk.  As a security analyst, it’s important to stay up-to-date on common frameworks, controls, and compliance regulations and be aware of changes to the cybersecurity landscape to help ensure the safety of both organizations and people. |

**Bài học chính**

Trong bài đọc này, bạn đã tìm hiểu thêm về các biện pháp kiểm soát, khuôn khổ và sự tuân thủ. Bạn cũng đã học được cách họ làm việc cùng nhau để giúp các tổ chức duy trì mức độ rủi ro thấp.

Là một nhà phân tích bảo mật, điều quan trọng là phải luôn cập nhật các khuôn khổ, biện pháp kiểm soát và quy định tuân thủ chung cũng như nhận thức được những thay đổi trong bối cảnh an ninh mạng để giúp đảm bảo an toàn cho cả tổ chức và con người.

## **Heather: Bảo vệ dữ liệu và thông tin nhạy cảm**

|  |
| --- |
| **Heather: Protect sensitive data and information**  Hello, my name is Heather and I'm the Vice President of Security Engineering at Google. PII has been an important topic on the internet since the beginning of the internet. And we have been talking about increasingly sophisticated ways to protect that data over time. When we think about collecting PII on behalf of another person, we should make sure we're very deliberate about how it's handled and where it's stored, and that we understand where it's stored all the time. Depending on what kind of role you're in, you might also need to protect that data to comply with regulation or law. And so, it's important to understand how the data relates to some of those obligations. If an organization fails to meet their obligations, a number of things might happen. First, you might see a government regulator become more interested in understanding the practices around how a company is handling data. Secondly, consumers, customers, businesses may actually begin to directly inquire of the company how they're handling data. And this may become part of the customer relationship and increasingly important if that data is very sensitive. And third, the last consequence is legal action. And it's not uncommon for us to see victims of cybersecurity incidents now suing companies for mishandling their data. You can keep up to date with compliance, regulation and laws around PII by consulting the relevant website in the jurisdiction that you have a question for. Many government websites now post the laws, regulations, and compliance requirements for data that's being handled. The regulations and laws that govern how PII can be handled are very complex, all over the world, countries, states, counties are regulating it at different levels. It's important to understand and to be aware that these laws exist. However, if you need to ask a question about a specific law, it's important to seek advice from legal counsel for that particular jurisdiction. It may be very different than the jurisdiction that you're in. |

**Heather: Bảo vệ dữ liệu và thông tin nhạy cảm**

## Xin chào, tên tôi là Heather vàTôi là Phó Chủ tịch Kỹ thuật Bảo mật tại Google.PII đã là một chủ đề quan trọng trên internetkể từ khi có Internet.Và chúng ta đã nói về những cách ngày càng phức tạp để bảo vệdữ liệu đó theo thời gian.Khi chúng tôi nghĩ đến việc thu thập PII thay mặt cho người khác,chúng ta nên đảm bảo rằng chúng ta rất cân nhắc về cách xử lý vànơi nó được lưu trữ và chúng tôi luôn biết nó được lưu trữ ở đâu.Tùy thuộc vào vai trò của bạn,bạn cũng có thể cần bảo vệ dữ liệu đó để tuân thủ quy định hoặc pháp luật.Và vì vậy, điều quan trọng là phải hiểu dữ liệu liên quan như thế nào đến một số trong số đónghĩa vụ.Nếu tổ chức không thực hiện được nghĩa vụ của mình,một số điều có thể xảy ra.Đầu tiên, bạn có thể thấy cơ quan quản lý của chính phủ quan tâm nhiều hơn đếnhiểu các thực tiễn xung quanh cách một công ty xử lý dữ liệu.Thứ hai, người tiêu dùng, khách hàng, doanh nghiệp có thể thực sự bắt đầuđể trực tiếp hỏi công ty cách họ xử lý dữ liệu.Và điều này có thể trở thành một phần của mối quan hệ khách hàng vàngày càng quan trọng nếu dữ liệu đó rất nhạy cảm.Và thứ ba, hậu quả cuối cùng là hành động pháp lý.Và không có gì lạ khi chúng ta chứng kiến ​​những nạn nhân của an ninh mạngsự cố hiện đang kiện các công ty vì xử lý sai dữ liệu của họ.Bạn có thể cập nhật các quy định, tuân thủ và luật pháp xung quanh PIIbằng cách tham khảo trang web có liên quan trong khu vực pháp lý mà bạn có thắc mắc.Nhiều trang web của chính phủ hiện nay đăng các luật, quy định vàyêu cầu tuân thủ đối với dữ liệu đang được xử lý.Các quy định và luật chi phối cách xử lý PII rất phức tạp,trên toàn thế giới, các quốc gia, tiểu bang,các quận đang điều chỉnh nó ở các cấp độ khác nhau.Điều quan trọng là phải hiểu và nhận thức được rằng những luật này tồn tại.Tuy nhiên, nếu bạn cần đặt câu hỏi về một luật cụ thể,điều quan trọng là tìm kiếm lời khuyên từ cố vấn pháp lý cho khu vực pháp lý cụ thể đó.Nó có thể rất khác so với khu vực pháp lý mà bạn đang ở.

## **Kiểm tra kiến thức của bạn: Khung và điều khiển**

# **Đạo đức trong an ninh mạng**

## **Đạo đức trong an ninh mạng**

|  |
| --- |
| **Ethics in cybersecurity**  In security, new technologies present new challenges. For every new security incident or risk, the right or wrong decision isn't always clear. |

**Đạo đức trong an ninh mạng**

Trong lĩnh vực bảo mật, các công nghệ mới đặt ra những thách thức mới.Đối với mọi sự cố hoặc rủi ro an ninh mới, quyền hoặcquyết định sai lầm không phải lúc nào cũng rõ ràng.

|  |
| --- |
| For example, imagine that you're working as an entry-level security analyst and you have received a high risk alert. You investigate the alert and discover data has been transferred without authorization. |

Ví dụ: hãy tưởng tượng bạn đang làm việc với tư cách là nhà phân tích bảo mật cấp thấp vàbạn đã nhận được cảnh báo rủi ro cao.Bạn điều tra cảnh báo vàphát hiện dữ liệu đã được chuyển giao mà không được phép.

|  |
| --- |
| You work diligently to identify who made the transfer and discover it is one of your friends from work. What do you do? |

Bạn làm việc chăm chỉ để xác định ai đã thực hiện chuyển khoản vàphát hiện ra đó là một trong những người bạn ở nơi làm việc của bạn.Bạn làm nghề gì?

|  |
| --- |
| Ethically, as a security professional, your job is to remain unbiased and maintain security and confidentiality. |

Về mặt đạo đức, với tư cách là một chuyên gia bảo mật, công việc của bạn là luôn không thiên vị vàduy trì an ninh và bảo mật.

|  |
| --- |
| While it's normal to want to protect a friend, regardless of who the user in question may be, your responsibility and obligation is to adhere to the policies and protocols you've been trained to follow. In many cases, security teams are entrusted with greater access to data and information than other employees. Security professionals must respect that privilege and act ethically at all times. |

Mặc dù việc muốn bảo vệ một người bạn là điều bình thường,bất kể người dùng được đề cập là ai, trách nhiệm và nghĩa vụ của bạnlà tuân thủ các chính sách và giao thức mà bạn đã được đào tạo để tuân theo.Trong nhiều trường hợp, các nhóm bảo mật được giao quyền truy cập nhiều hơn vào dữ liệu vàthông tin hơn những nhân viên khác.Các chuyên gia bảo mật phải tôn trọng đặc quyền đó và luôn hành động có đạo đức.

|  |
| --- |
| Security ethics are guidelines for making appropriate decisions as a security professional. As another example, if you as an analyst have the ability to grant yourself access to payroll data and can give yourself a raise, just because you have access to do so, does that mean you should? The answer is no. You should never abuse the access you've been granted and entrusted with. |

Đạo đức bảo mật là hướng dẫn chođưa ra quyết định phù hợp với tư cách là một chuyên gia bảo mật.Một ví dụ khác, nếu bạn với tư cách là nhà phân tích có khả năng cấp cho mình quyền truy cậpvào dữ liệu bảng lương và có thể tự tăng lương chỉ vì bạn có quyền truy cập để làmvậy điều đó có nghĩa là bạn nên làm vậy?Câu trả lời là không.Bạn không bao giờ nên lạm dụng quyền truy cập mà bạn đã được cấp và giao phó.

|  |
| --- |
| Let's discuss ethical principles that may raise questions as you navigate solutions for mitigating risks. These are confidentiality, privacy protections, and laws. |

Hãy thảo luận về các nguyên tắc đạo đức có thể đặt ra câu hỏi khi bạn định hướnggiải pháp giảm thiểu rủi ro.Đó là tính bảo mật, bảo vệ quyền riêng tư và luật pháp.

|  |
| --- |
| Let's begin with the first ethical principle, confidentiality. Earlier we discussed confidentiality as part of the CIA triad. Now let's discuss how confidentiality can be applied to ethics. As a security professional, you'll encounter proprietary or private information, such as PII. It's your ethical duty to keep that information confidential and safe. For example, you may want to help out a coworker by providing computer system access outside of properly documented channels. However, this ethical violation can result in serious consequences, including reprimands, the loss of your professional reputation, and legal repercussions for both you and your friend. |

Hãy bắt đầu với nguyên tắc đạo đức đầu tiên, tính bảo mật.Trước đó chúng ta đã thảo luận về vấn đề bảo mật như một phần của bộ ba CIA.Bây giờ hãy thảo luận về cách áp dụng tính bảo mật vào đạo đức.Là một chuyên gia bảo mật, bạn sẽ gặp phải vấn đề độc quyềnhoặc thông tin cá nhân, chẳng hạn như PII.Nghĩa vụ đạo đức của bạn là giữ thông tin đó bí mật và an toàn.Ví dụ: bạn có thể muốn giúp đỡ đồng nghiệp bằng cách cung cấp máy tínhtruy cập hệ thống bên ngoài các kênh được ghi chép phù hợp.Tuy nhiên, hành vi vi phạm đạo đức này có thể gây ra những hậu quả nghiêm trọng,bao gồm khiển trách, mất danh tiếng nghề nghiệp của bạn vàhậu quả pháp lý cho cả bạn và bạn của bạn.

|  |
| --- |
| The second ethical principle to consider is privacy protections. Privacy protection means safeguarding personal information from unauthorized use. For example, imagine you receive a personal email after hours from your manager requesting a colleague's home phone number. Your manager explains that they can't access the employee database at the moment, but they need to discuss an urgent matter with that person. |

Nguyên tắc đạo đức thứ hai cần xem xét là bảo vệ quyền riêng tư.Bảo vệ quyền riêng tư có nghĩa là bảo vệ thông tin cá nhân khỏisử dụng trái phép.Ví dụ: hãy tưởng tượng bạn nhận được email cá nhân saugiờ kể từ khi người quản lý của bạn yêu cầu số điện thoại nhà của đồng nghiệp.Người quản lý của bạn giải thích rằng họ không thể truy cập cơ sở dữ liệu nhân viên vào lúc này,nhưng họ cần thảo luận một vấn đề khẩn cấp với người đó.

|  |
| --- |
| As a security analyst, your role is to follow the policies and procedures of your company, which in this example, state that employee information is stored in a secure database and should never be accessed or shared in any other format. So, accessing and sharing the employee's personal information would be unethical. In situations like this, it can be difficult to know what to do. So, the best response is to adhere to the policies and procedures set by your organization. |

Là nhà phân tích bảo mật, vai trò của bạn là tuân theo các chính sách và thủ tục của công ty bạn,trong ví dụ này nêu rõ rằng thông tin nhân viên được lưu trữtrong cơ sở dữ liệu an toàn và không bao giờ được truy cập hoặc chia sẻ ở bất kỳ định dạng nào khác.Vì vậy, việc truy cập và chia sẻ thông tin cá nhân của nhân viên sẽ là phi đạo đức.Trong những tình huống như thế này, thật khó để biết phải làm gì.Vì vậy, cách ứng phó tốt nhất là tuân thủ các chính sách và thủ tụcdo tổ chức của bạn đặt ra.

|  |
| --- |
| A third important ethical principle we must discuss is the law. Laws are rules that are recognized by a community and enforced by a governing entity. |

Nguyên tắc đạo đức quan trọng thứ ba mà chúng ta phải thảo luận là luật pháp.Pháp luật là những quy định được cộng đồng thừa nhận vàđược thực thi bởi một cơ quan quản lý.

|  |
| --- |
| For example, consider a staff member at a hospital who has been trained to handle PII, and SPII for compliance. The staff member has files with confidential data that should never be left unsupervised, but the staff member is late for a meeting. Instead of locking the files in a designated area, the files are left on the staff member's desk, unsupervised. Upon the employee's return, the files are missing. The staff member has just violated multiple compliance regulations, and their actions were unethical and illegal, since their negligence has likely resulted in the loss of private patient and hospital data. |

Ví dụ, hãy xem xét một nhân viên tại bệnh viện đã được đào tạođể xử lý PII và SPII để tuân thủ.Nhân viên có các tập tin chứa dữ liệu bí mật không bao giờ được để lạikhông được giám sát, nhưng nhân viên đó lại đến trễ cuộc họp.Thay vì khóa các tập tin trong một khu vực được chỉ định,các tập tin được để trên bàn của nhân viên, không được giám sát.Khi nhân viên trở lại, các tập tin bị thiếu.Nhân viên vừa vi phạm nhiều quy định tuân thủ vàhành động của họ là phi đạo đức và bất hợp pháp, vì sự sơ suất của họ có thể dẫn đếntrong việc mất dữ liệu bệnh nhân và bệnh viện tư nhân.

|  |
| --- |
| As you enter the security field, remember that technology is constantly evolving, and so are attackers' tactics and techniques. Because of this, security professionals must continue to think critically about how to respond to attacks. |

Khi bạn bước vào lĩnh vực bảo mật, hãy nhớ rằng công nghệ không ngừng phát triển,và chiến thuật và kỹ thuật của kẻ tấn công cũng vậy.Vì điều này, các chuyên gia bảo mật phải tiếp tục suy nghĩ chín chắn vềlàm thế nào để đáp ứng với các cuộc tấn công.

|  |
| --- |
| Having a strong sense of ethics can guide your decisions to ensure that the proper processes and procedures are followed to mitigate these continually evolving risks. |

Có ý thức đạo đức tốt có thể hướng dẫn các quyết định của bạn để đảm bảo rằng các quyết định đúng đắnquy trình và thủ tụcđược tuân thủ để giảm thiểu những rủi ro liên tục phát triển này.

## **Các khái niệm đạo đức hướng dẫn các quyết định về an ninh mạng**

|  |
| --- |
| **Ethical concepts that guide cybersecurity decisions**  Previously, you were introduced to the concept of security ethics. **Security** **ethics** are guidelines for making appropriate decisions as a security professional. Being ethical requires that security professionals remain unbiased and maintain the security and confidentiality of private data. Having a strong sense of ethics can help you navigate your decisions as a cybersecurity professional so you’re able to mitigate threats posed by threat actors’ constantly evolving tactics and techniques. In this reading, you’ll learn about more ethical concepts that are essential to know so you can make appropriate decisions about how to legally and ethically respond to attacks in a way that protects organizations and people alike. |

**Các khái niệm đạo đức hướng dẫn các quyết định về an ninh mạng**

Trước đây, bạn đã được giới thiệu khái niệm về đạo đức bảo mật. **Đạo đức bảo mật** là những hướng dẫn để đưa ra quyết định phù hợp với tư cách là một chuyên gia bảo mật. Có đạo đức đòi hỏi các chuyên gia bảo mật phải không thiên vị và duy trì tính bảo mật và bảo mật của dữ liệu riêng tư. Việc có ý thức đạo đức cao có thể giúp bạn định hướng các quyết định của mình với tư cách là một chuyên gia an ninh mạng để bạn có thể giảm thiểu các mối đe dọa do các chiến thuật và kỹ thuật không ngừng phát triển của các tác nhân đe dọa gây ra. Trong bài đọc này, bạn sẽ tìm hiểu thêm về các khái niệm đạo đức cần biết để có thể đưa ra quyết định phù hợp về cách ứng phó hợp pháp và có đạo đức trước các cuộc tấn công theo cách bảo vệ các tổ chức cũng như mọi người.

|  |
| --- |
| **Ethical concerns and laws related to counterattacks**  **United States standpoint on counterattacks**  In the U.S., deploying a counterattack on a threat actor is illegal because of laws like the Computer Fraud and Abuse Act of 1986 and the Cybersecurity Information Sharing Act of 2015, among others. You can only defend. The act of counterattacking in the U.S. is perceived as an act of vigilantism. Avigilante is a person who is not a member of law enforcement who decides to stop a crime on their own. And because threat actors are criminals, counterattacks can lead to further escalation of the attack, which can cause even more damage and harm. Lastly, if the threat actor in question is a state-sponsored hacktivist, a counterattack can lead to serious international implications. A **hacktivist** is a person who uses hacking to achieve a political goal. The political goal may be to promote social change or civil disobedience.  For these reasons, the only individuals in the U.S. who are allowed to counterattack are approved employees of the federal government or military personnel. |

**Những lo ngại về đạo đức và luật pháp liên quan đến phản công**

**Quan điểm của Hoa Kỳ về các cuộc phản công**

Tại Hoa Kỳ, việc triển khai một cuộc phản công nhằm vào tác nhân đe dọa là bất hợp pháp vì các luật như Đạo luật Lừa đảo và Lạm dụng Máy tính năm 1986 và Đạo luật Chia sẻ Thông tin An ninh Mạng năm 2015, cùng nhiều luật khác. Bạn chỉ có thể phòng thủ. Hành động phản công ở Mỹ được coi là hành động cảnh giác. Người cảnh giác là người không phải là thành viên của cơ quan thực thi pháp luật và quyết định tự mình ngăn chặn tội phạm. Và bởi vì những kẻ đe dọa là tội phạm, các cuộc phản công có thể dẫn đến sự leo thang hơn nữa của cuộc tấn công, có thể gây ra nhiều thiệt hại và tổn hại hơn. Cuối cùng, nếu tác nhân đe dọa được đề cập là một kẻ tấn công được nhà nước bảo trợ, thì một cuộc phản công có thể dẫn đến những tác động quốc tế nghiêm trọng. Hacktivist là người sử dụng hack để đạt được mục tiêu chính trị **.** Mục tiêu chính trị có thể là thúc đẩy sự thay đổi xã hội hoặc sự bất tuân dân sự. 

Vì những lý do này, những cá nhân duy nhất ở Hoa Kỳ được phép phản công là nhân viên chính phủ liên bang hoặc quân nhân được phê duyệt.

|  |
| --- |
| **International standpoint on counterattacks**  The International Court of Justice (ICJ), which updates its guidance regularly, states that a person or group can counterattack if:   * The counterattack will only affect the party that attacked first. * The counterattack is a direct communication asking the initial attacker to stop. * The counterattack does not escalate the situation. * The counterattack effects can be reversed.   Organizations typically do not counterattack because the above scenarios and parameters are hard to measure. There is a lot of uncertainty dictating what is and is not lawful, and at times negative outcomes are very difficult to control. Counterattack actions generally lead to a worse outcome, especially when you are not an experienced professional in the field.  To learn more about specific scenarios and ethical concerns from an international perspective, review updates provided in the [Tallinn Manual online](https://ccdcoe.org/research/tallinn-manual/). |

**Quan điểm quốc tế về phản công**

Tòa án Công lý Quốc tế (ICJ), nơi thường xuyên cập nhật hướng dẫn của mình, tuyên bố rằng một người hoặc một nhóm có thể phản công nếu:

* Cuộc phản công sẽ chỉ ảnh hưởng đến bên tấn công trước.
* Cuộc phản công là một cuộc giao tiếp trực tiếp yêu cầu kẻ tấn công ban đầu dừng lại.
* Cuộc phản công không làm tình hình leo thang.
* Hiệu ứng phản công có thể bị đảo ngược.

Các tổ chức thường không phản công vì các kịch bản và thông số trên rất khó đo lường. Có rất nhiều điều không chắc chắn về việc điều gì là hợp pháp và điều gì không hợp pháp, và đôi khi rất khó kiểm soát những kết quả tiêu cực. Các hành động phản công thường dẫn đến kết quả tồi tệ hơn, đặc biệt khi bạn không phải là chuyên gia giàu kinh nghiệm trong lĩnh vực này.

Để tìm hiểu thêm về các tình huống cụ thể và các mối lo ngại về đạo đức từ góc độ quốc tế, hãy xem lại các thông tin cập nhật được cung cấp trong[Hướng dẫn sử dụng Tallinn trực tuyến](https://ccdcoe.org/research/tallinn-manual/).

|  |
| --- |
| **Ethical principles and methodologies**  Because counterattacks are generally disapproved of or illegal, the security realm has created frameworks and controls—such as the confidentiality, integrity, and availability (CIA) triad and others discussed earlier in the program—to address issues of confidentiality, privacy protections, and laws. To better understand the relationship between these issues and the ethical obligations of cybersecurity professionals, review the following key concepts as they relate to using ethics to protect organizations and the people they serve. |

**Các nguyên tắc và phương pháp đạo đức**

Bởi vì các cuộc phản công thường bị phản đối hoặc bất hợp pháp, lĩnh vực bảo mật đã tạo ra các khuôn khổ và biện pháp kiểm soát—chẳng hạn như bộ ba bí mật, tính toàn vẹn và tính khả dụng (CIA) và những vấn đề khác đã được thảo luận trước đó trong chương trình—để giải quyết các vấn đề về bảo mật, bảo vệ quyền riêng tư và luật pháp . Để hiểu rõ hơn mối quan hệ giữa những vấn đề này và nghĩa vụ đạo đức của các chuyên gia an ninh mạng, hãy xem lại các khái niệm chính sau đây vì chúng liên quan đến việc sử dụng đạo đức để bảo vệ các tổ chức và những người mà họ phục vụ.

|  |
| --- |
| **Confidentiality** means that only authorized users can access specific assets or data. Confidentiality as it relates to professional ethics means that there needs to be a high level of respect for privacy to safeguard private assets and data. |

**Tính bảo mật** có nghĩa là chỉ những người dùng được ủy quyền mới có thể truy cập vào các tài sản hoặc dữ liệu cụ thể. Tính bảo mật liên quan đến đạo đức nghề nghiệp có nghĩa là cần phải có sự tôn trọng cao đối với quyền riêng tư để bảo vệ tài sản và dữ liệu riêng tư.

|  |
| --- |
| **Privacy protection** means safeguarding personal information from unauthorized use. Personally identifiable information (PII) and sensitive personally identifiable information (SPII)are types of personal data that can cause people harm if they are stolen. **PII** data is any information used to infer an individual's identity, like their name and phone number. **SPII** data is a specific type of PII that falls under stricter handling guidelines, including social security numbers and credit card numbers. To effectively safeguard PII and SPIIdata, security professionals hold an ethical obligation to secure private information, identify security vulnerabilities, manage organizational risks, and align security with business goals. |

**Bảo vệ quyền riêng tư** có nghĩa là bảo vệ thông tin cá nhân khỏi việc sử dụng trái phép. Thông tin nhận dạng cá nhân (PII) và thông tin nhận dạng cá nhân nhạy cảm (SPII) là các loại dữ liệu cá nhân có thể gây hại cho mọi người nếu chúng bị đánh cắp. **Dữ liệu PII** là bất kỳ thông tin nào được sử dụng để suy ra danh tính của một cá nhân, như tên và số điện thoại của họ. **Dữ liệu SPII** là một loại PII cụ thể tuân theo các nguyên tắc xử lý chặt chẽ hơn, bao gồm số an sinh xã hội và số thẻ tín dụng. Để bảo vệ hiệu quả dữ liệu PII và SPII , các chuyên gia bảo mật có nghĩa vụ đạo đức trong việc bảo mật thông tin cá nhân, xác định các lỗ hổng bảo mật, quản lý rủi ro tổ chức và điều chỉnh bảo mật cho phù hợp với mục tiêu kinh doanh.

|  |
| --- |
| **Laws** are rules that are recognized by a community and enforced by a governing entity. As a security professional, you will have an ethical obligation to protect your organization, its internal infrastructure, and the people involved with the organization. To do this:   * You must remain unbiased and conduct your work honestly, responsibly, and with the highest respect for the law. * Be transparent and just, and rely on evidence. * Ensure that you are consistently invested in the work you are doing, so you can appropriately and ethically address issues that arise. * Stay informed and strive to advance your skills, so you can contribute to the betterment of the cyber landscape.    As an example, consider the **Health Insurance Portability and Accountability Act (HIPAA)**, which is a U.S. federal law established to protect patients' health information, also known as PHI, or protected health information. This law prohibits patient information from being shared without their consent. So, as a security professional, you might help ensure that the organization you work for adheres to both its legal and ethical obligation to inform patients of a breach if their health care data is exposed. |

**Luật pháp** là những quy tắc được cộng đồng thừa nhận và được thực thi bởi một cơ quan quản lý. Là một chuyên gia bảo mật, bạn sẽ có nghĩa vụ đạo đức để bảo vệ tổ chức của mình, cơ sở hạ tầng nội bộ và những người có liên quan đến tổ chức. Để làm điều này:

* Bạn phải không thiên vị và thực hiện công việc của mình một cách trung thực, có trách nhiệm và với sự tôn trọng cao nhất đối với pháp luật.
* Hãy minh bạch và công bằng, và dựa vào bằng chứng.
* Đảm bảo rằng bạn luôn đầu tư vào công việc mình đang làm để có thể giải quyết các vấn đề phát sinh một cách phù hợp và có đạo đức.
* Luôn cập nhật thông tin và cố gắng nâng cao kỹ năng của mình để có thể đóng góp vào việc cải thiện bối cảnh mạng.

 Ví dụ: hãy xem xét **Đạo luật về trách nhiệm giải trình và cung cấp thông tin bảo hiểm y tế (HIPAA)** , là luật liên bang của Hoa Kỳ được thiết lập để bảo vệ thông tin sức khỏe của bệnh nhân, còn được gọi là PHI hoặc thông tin sức khỏe được bảo vệ. Luật này cấm chia sẻ thông tin của bệnh nhân mà không có sự đồng ý của họ. Vì vậy, với tư cách là một chuyên gia bảo mật, bạn có thể giúp đảm bảo rằng tổ chức mà bạn làm việc tuân thủ cả nghĩa vụ pháp lý và đạo đức trong việc thông báo cho bệnh nhân về hành vi vi phạm nếu dữ liệu chăm sóc sức khỏe của họ bị lộ.

|  |
| --- |
| **Key takeaways**  As a future security professional, ethics will play a large role in your daily work. Understanding ethics and laws will help you make the correct choices if and when you encounter a security threat or an incident that results in a breach. |

**Bài học chính**

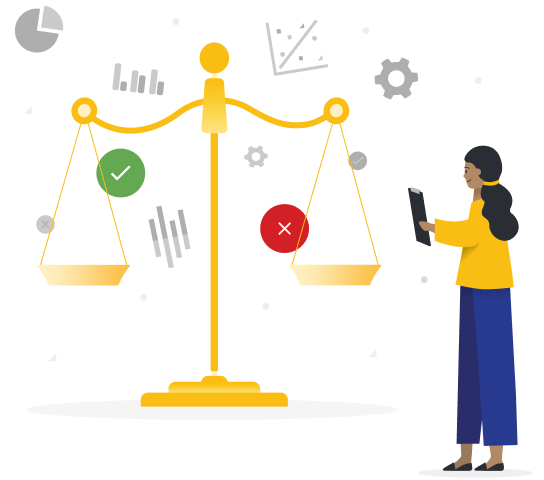
Là một chuyên gia bảo mật trong tương lai, đạo đức sẽ đóng một vai trò lớn trong công việc hàng ngày của bạn. Hiểu rõ đạo đức và luật pháp sẽ giúp bạn đưa ra những lựa chọn đúng đắn nếu và khi bạn gặp phải mối đe dọa an ninh hoặc sự cố dẫn đến vi phạm.

## **Thực hành: Đạo đức dành cho chuyên gia an ninh mạng**

|  |
| --- |
| **Practice: Ethics for cybersecurity professionals**  Explore a number of scenarios that you might encounter as a security analyst, and consider how you would respond to security incidents based on your understanding of security ethics. |

**Thực hành: Đạo đức dành cho chuyên gia an ninh mạng**

Khám phá một số tình huống mà bạn có thể gặp phải với tư cách là nhà phân tích bảo mật và xem xét cách bạn sẽ ứng phó với các sự cố bảo mật dựa trên hiểu biết của bạn về đạo đức bảo mật.



|  |  |
| --- | --- |
| Scenario | Response |
| You work for a hospital as a security analyst.  One day, you log into your work computer and see a ransom note displayed on your screen. Access to files and applications is locked.  You realize this is a ransomware attack. | ~~Initiate a counter- attack~~  ~~Use a self-developed decryptor tool to stop the attack~~  Immediately contact your supervisor  ~~Contact government agencies for assistance~~ |
| A doctor you work with claims to have laptop performance issues, so you try to identify the problem.  As you’re working, you notice the doctor’s laptop has unsecured patient files visible on-screen instead of within the medical practice’s secure software. | Immediately secure the patient files  ~~Submit a formal complaint to Health and Human Services~~  ~~Publicly shame the doctor for not following proper procedures~~  ~~Assume the doctor knows about the issue and do nothing~~ |
| You work for a medical device company as an entry-level security analyst.  Your supervisor has asked you to securely dispose of old developer laptops, and tells you they may contain PII (personally identifiable information). | Take the laptops home and perform a factory reset  Dispose of the laptops without properly erasing the data  Store the laptops in an area designated for old equipment  Remove the laptop hard drives and irreversibly erase all data |
| You work as an entry-level analyst for a pharmaceutical company.  You receive SIEM tool alerts about unusual employee activity.  You check their account activity and observe them copying confidential files to an external folder linked to an unknown destination. | Confront the user directly regarding non-compliance with internal ethical standards  Tell your supervisor and take no other action  Follow provided procedures to address the issue.  Report the incident to the company's security personnel |

|  |  |
| --- | --- |
| Tình huống |  |
| Bạn làm việc cho một bệnh viện với tư cách là nhà phân tích bảo mật.  Một ngày nọ, bạn đăng nhập vào máy tính ở cơ quan và thấy thông báo đòi tiền chuộc hiển thị trên màn hình. Quyền truy cập vào các tập tin và ứng dụng bị khóa.  Bạn nhận ra đây là một cuộc tấn công ransomware. | ~~Bắt đầu phản công~~  ~~Sử dụng công cụ giải mã tự phát triển để ngăn chặn cuộc tấn công~~  Hãy liên hệ ngay với người giám sát của bạn  ~~Liên hệ với các cơ quan chính phủ để được hỗ trợ~~ |
| Một bác sĩ làm việc cùng bạn tuyên bố rằng máy tính xách tay có vấn đề về hiệu suất, vì vậy bạn cố gắng xác định vấn đề.  Khi đang làm việc, bạn nhận thấy máy tính xách tay của bác sĩ có các tệp bệnh nhân không bảo mật hiển thị trên màn hình thay vì trong phần mềm bảo mật của phòng khám y tế. | Bảo mật ngay lập tức hồ sơ bệnh nhân  ~~Gửi khiếu nại chính thức tới Bộ Y tế và Dịch vụ Nhân sinh~~  ~~Công khai xấu hổ vì bác sĩ không tuân thủ đúng quy trình~~  ~~Giả sử bác sĩ biết về vấn đề này và không làm gì cả~~ |
| Bạn làm việc cho một công ty thiết bị y tế với vai trò là nhà phân tích bảo mật cấp độ đầu vào.  Người giám sát của bạn đã yêu cầu bạn tiêu hủy an toàn các máy tính xách tay cũ của nhà phát triển và cho bạn biết rằng chúng có thể chứa PII (thông tin nhận dạng cá nhân). | ~~Mang máy tính xách tay về nhà và thực hiện khôi phục cài đặt gốc~~  ~~Vứt bỏ máy tính xách tay mà không xóa dữ liệu đúng cách~~  ~~Cất giữ máy tính xách tay ở khu vực dành riêng cho thiết bị cũ~~  Tháo ổ cứng máy tính xách tay và xóa tất cả dữ liệu không thể phục hồi |
| Bạn làm việc như một nhà phân tích cấp đầu vào cho một công ty dược phẩm.  Bạn nhận được thông báo từ công cụ SIEM về hoạt động bất thường của nhân viên.  Bạn kiểm tra hoạt động tài khoản của họ và quan sát thấy họ sao chép các tệp bí mật vào một thư mục bên ngoài được liên kết đến một đích đến không xác định. | ~~Đối đầu trực tiếp với người dùng về việc không tuân thủ các tiêu chuẩn đạo đức nội bộ~~  ~~Hãy nói với người giám sát của bạn và không thực hiện hành động nào khác~~  Thực hiện theo các thủ tục được cung cấp để giải quyết vấn đề. |

## **Holly: Tầm quan trọng của đạo đức với tư cách là một chuyên gia an ninh mạng**

|  |
| --- |
| **Holly: The importance of ethics as a cybersecurity professional**  Hi, I'm Holly and I'm a Cloud Security Architect with Google Cloud. At the beginning of my adult career, I sold hosiery while I was going to school. That led me into an opportunity to work in banking, which then led me into an opportunity to work in telecommunications. From there I managed to get myself into a security vendor and learn security. Part of the way that I was able to change from my original half of my tech career being a database administrator to getting into cybersecurity was through getting certificates like you're doing today. Those really helped me gain credibility with potential employers when I didn't have the experience in this particular field yet. Ethics are really the crux of cybersecurity, you need to be able to be ethical in all of your actions in order to be a cybersecurity professional. Examples of unethical behavior are usually honestly just slight laziness, people taking shortcuts and not really thinking about the consequences of their actions. So, certainly when people share passwords to systems or give out private information, or look into systems for their own personal information or purposes about people they know or about celebrities. One of the most difficult situations that I ever faced in my technology career related to ethics was shortly after 9/11, my boss's boss's boss came to me with a bunch of keywords that were clearly related to the attack in New York and asked me to query the database that I administered that had everybody's text messages in it for the entire telecommunications company without anything in writing and without a court order. I was in a very uncomfortable position to tell someone that much senior than me that I wasn't comfortable doing that. I suggested that he bring something in writing to me to do that and he found someone else who did it for him. When you're faced with one of these difficult decisions, it's good to think about what would be the consequences of your decision. My encouragement to those of you out here taking this program is that the rewards that you get from helping to protect your company or your users or your organization from cyber criminals is really great. We get to be the good guys and help protect our industry and our customers from cyber attacks and cyber criminals. That's rewarding. |

**Holly: Tầm quan trọng của đạo đức với tư cách là một chuyên gia an ninh mạng**

Xin chào, tôi là Holly và tôi làKiến trúc sư bảo mật đám mây của Google Cloud.Khi bắt đầu sự nghiệp trưởng thành của tôi,Tôi đã bán hàng dệt kim khi còn đi học.Điều đó dẫn tôi đến cơ hội làm việc trong ngành ngân hàng,sau đó dẫn tôi vàocơ hội làm việc trong lĩnh vực viễn thông.Từ đó tôi đã có thể dấn thân vàomột nhà cung cấp bảo mật và tìm hiểu bảo mật.Một phần trong cách mà tôi có thểsự thay đổi so với nửa đầu sự nghiệp công nghệ của tôimột quản trị viên cơ sở dữ liệu để tham giaan ninh mạng là thông qua việc nhận được chứng chỉgiống như bạn đang làm ngày hôm nay.Những điều đó thực sự đã giúp tôi có được sự tín nhiệm vớinhững nhà tuyển dụng tiềm năng khi tôi khôngchưa có kinh nghiệm trong lĩnh vực cụ thể này.Đạo đức thực sự là mấu chốt của an ninh mạng,bạn cần có khả năng có đạo đức trong tất cảhành động của bạn để trở thành một chuyên gia an ninh mạng.Ví dụ về hành vi phi đạo đức lànói thật thì thường chỉ hơi lười biếng thôi,mọi người đi đường tắt và thực sự không phải vậysuy nghĩ về hậu quả của hành động của họ.Vì vậy, chắc chắn khi mọi người chia sẻ mật khẩu vớihệ thống hoặc cung cấp thông tin cá nhân,hoặc xem xét các hệ thống chothông tin cá nhân của riêng họhoặc mục đích về những người họ biết hoặc về những người nổi tiếng.Một trong những tình huống khó khăn nhất mà tôi từng gặp phảisự nghiệp công nghệ của tôi liên quanđến vấn đề đạo đức ngay sau ngày 11/9,sếp của sếp sếp của tôi đã đến gặp tôivới một loạt từ khóa rõ ràngliên quan đến vụ tấn công ởNew York và yêu cầu tôi truy vấn cơ sở dữ liệu mà tôiđược quản lý có tin nhắn văn bản của mọi người trong đótoàn bộ công ty viễn thôngmà không có bất cứ điều gì bằng văn bản và không có lệnh của tòa án.Tôi đang ở trong một tình thế rất khó chịu để nóimột người cao cấp hơn tôi nhiềurằng tôi không thấy thoải mái khi làm điều đó.Tôi đề nghị anh ấy mang thứ gì đó bằng văn bản tớitôi làm điều đó và anh ấyđã tìm được người khác làm việc đó cho anh ta.Khi bạn phải đối mặt với một trong những quyết định khó khăn này,thật tốt khi nghĩ về điều gì sẽ xảy rahậu quả của quyết định của bạn.Sự khuyến khích của tôi dành cho những người trong số các bạn ở đây đang tham giachương trình này là phần thưởng mà bạnnhận được từ việc giúp bảo vệ công ty hoặc người dùng của bạn hoặctổ chức của bạn khỏi tội phạm mạng thực sự tuyệt vời.Chúng ta trở thành người tốt và giúp đỡbảo vệ ngành công nghiệp của chúng tôi vàkhách hàng của chúng tôi khỏi các cuộc tấn công mạngvà tội phạm mạng. Đó là bổ ích.

## **Sử dụng đạo đức để đưa ra quyết định Lời nhắc thảo luận**

|  |
| --- |
| **Use ethics to make decisions**  You’ve been introduced to security ethics, including specific examples of how ethics are applied in the workplace. Now, it’s your turn to share a bit of your experience and exchange ideas with other learners in the course. |

**Sử dụng đạo đức để đưa ra quyết định**

Bạn đã được giới thiệu về đạo đức bảo mật, bao gồm các ví dụ cụ thể về cách áp dụng đạo đức tại nơi làm việc. Bây giờ, đến lượt bạn chia sẻ một chút kinh nghiệm của mình và trao đổi ý kiến ​​với những người học khác trong khóa học.

|  |
| --- |
| **Option 1:** Your example can be related to a work, academic, and/or volunteer setting and should focus on a time when you chose an ethical course of action.  For this discussion prompt, consider the following:   * What was the situation? * How did you use ethics to make a decision? * What was the impact and/or result of your decision? |

**Tùy chọn 1:** Ví dụ của bạn có thể liên quan đến môi trường làm việc, học tập và/hoặc tình nguyện và nên tập trung vào thời điểm bạn chọn một hành động có đạo đức.

Đối với lời nhắc thảo luận này, hãy xem xét những điều sau:

* Tình hình là gì?
* Bạn đã sử dụng đạo đức để đưa ra quyết định như thế nào?
* Tác động và/hoặc kết quả của quyết định của bạn là gì?

|  |
| --- |
| **Option 2:** Your example can be related to a work, academic, and/or volunteer setting and should focus on a time when someone else chose an ethical course of action.  For this discussion prompt, consider the following:   * What was the situation? * How did the person use ethics to make a decision? * What was the impact and/or result of the person’s decision?   Please write one to two paragraphs in response to one of the discussion options (150–250 words). Then, visit the [discussion forums](https://www.coursera.org/learn/foundations-of-cybersecurity/discussions) and, applying what you’ve learned, comment on at least two posts from other learners.  Participation is optional |

**Tùy chọn 2:** Ví dụ của bạn có thể liên quan đến môi trường làm việc, học tập và/hoặc tình nguyện và nên tập trung vào thời điểm người khác chọn một hành động có đạo đức.

Đối với lời nhắc thảo luận này, hãy xem xét những điều sau:

* Tình hình là gì?
* Người đó đã sử dụng đạo đức để đưa ra quyết định như thế nào?
* Tác động và/hoặc kết quả của quyết định của người đó là gì?

Vui lòng viết một đến hai đoạn văn để phản hồi một trong các phương án thảo luận (150–250 từ). Sau đó, hãy ghé thăm[diễn đàn thảo luận](https://www.coursera.org/learn/foundations-of-cybersecurity/discussions)và áp dụng những gì bạn đã học, bình luận về ít nhất hai bài đăng của những người học khác.

Việc tham gia là tùy chọn

## **Kiểm tra kiến thức của bạn: Đạo đức trong an ninh mạng**

# **Đánh giá: Bảo vệ khỏi các mối đe dọa, rủi ro và lỗ hỏng**

## **Gói lại**

|  |
| --- |
| **Wrap-up**  You are now better prepared to understand and help make decisions regarding assessing and managing risks. Let's review what we've covered. |

Bây giờ bạn đã chuẩn bị tốt hơn để hiểu và giúp đỡđưa ra quyết định liên quan đến việc đánh giá và quản lý rủi ro.Hãy xem lại những gì chúng tôi đã đề cập.

|  |
| --- |
| We discussed security frameworks and controls and how they're used to develop processes and procedures that protect organizations and the people they serve. We also discussed core components of frameworks, such as identifying security goals and establishing guidelines to achieve those goals. |

Chúng tôi đã thảo luận về các khuôn khổ bảo mật vàcác điều khiển và cách chúng được sử dụng để phát triểncác quy trình và thủ tục màbảo vệ các tổ chức và những người mà họ phục vụ.Chúng tôi cũng thảo luận về các thành phần cốt lõi của khung,chẳng hạn như xác định các mục tiêu bảo mật vàthiết lập các hướng dẫn để đạt được các mục tiêu đó.

|  |
| --- |
| Then, we introduced specific frameworks and controls, including the CIA triad and the NIST CSF, and how they are used to manage risk. |

Sau đó, chúng tôi đã giới thiệu các khuôn khổ và biện pháp kiểm soát cụ thể,bao gồm cả bộ ba CIA và NIST CSF,và cách chúng được sử dụng để quản lý rủi ro.

|  |
| --- |
| And finally, we discussed security ethics, including common ethical issues to consider, such as confidentiality, privacy protections, and laws. |

Và cuối cùng, chúng tôi đã thảo luận về đạo đức bảo mật,bao gồm các vấn đề đạo đức chung đểxem xét, chẳng hạn như tính bảo mật,bảo vệ quyền riêng tư và luật pháp.

|  |
| --- |
| You're almost there, only one more section to go in this course. Coming up, you'll learn about common tools and programming languages used by security analysts to protect organizational operations. Hope you're as excited as I am to keep going! |

Bạn gần như ở đó rồi, chỉ có một thôinhiều phần hơn để đi trong khóa học này.Tiếp theo, bạn sẽ tìm hiểu về các công cụ phổ biến vàngôn ngữ lập trình được sử dụng bởicác nhà phân tích bảo mật để bảo vệ hoạt động của tổ chức.Hy vọng bạn cũng hào hứng như tôi để tiếp tục!

## **Thuật ngữ trong trong module 3**

|  |
| --- |
| **Glossary terms from module 3**  **Terms and definitions from Course 1, Module 3** |

**Thuật ngữ trong học phần 3**

**Các thuật ngữ và định nghĩa trong Khóa 1, Học phần 3**

|  |
| --- |
| **Asset:** An item perceived as having value to an organization |

**Tài sản:** Một vật phẩm được coi là có giá trị đối với một tổ chức

|  |
| --- |
| **Availability:** The idea that data is accessible to those who are authorized to access it |

**Tính sẵn có:** Ý tưởng rằng dữ liệu có thể truy cập được đối với những người được phép truy cập nó

|  |
| --- |
| **Compliance:** The process of adhering to internal standards and external regulations |

**Tuân thủ:** Quá trình tuân thủ các tiêu chuẩn nội bộ và quy định bên ngoài

|  |
| --- |
| **Confidentiality:** The idea that only authorized users can access specific assets or data |

**Tính bảo mật:** Ý tưởng rằng chỉ những người dùng được ủy quyền mới có thể truy cập các tài sản hoặc dữ liệu cụ thể

|  |
| --- |
| **Confidentiality, integrity, availability (CIA) triad:** A model that helps inform how organizations consider risk when setting up systems and security policies |

**Bộ ba bí mật, toàn vẹn, sẵn có (CIA):** Một mô hình giúp thông báo cách các tổ chức xem xét rủi ro khi thiết lập hệ thống và chính sách bảo mật

|  |
| --- |
| **Hacktivist:** A person who uses hacking to achieve a political goal |

**Hacktivist:** Người sử dụng hack để đạt được mục tiêu chính trị

|  |
| --- |
| **Health Insurance Portability and Accountability Act (HIPAA):** A U.S. federal law established to protect patients' health information |

**Đạo luật về trách nhiệm giải trình và cung cấp thông tin bảo hiểm y tế (HIPAA):** Luật liên bang của Hoa Kỳ được thiết lập để bảo vệ thông tin sức khỏe của bệnh nhân

|  |
| --- |
| **Integrity:** The idea that the data is correct, authentic, and reliable |

**Tính toàn vẹn:** Ý tưởng rằng dữ liệu là chính xác, xác thực và đáng tin cậy

|  |
| --- |
| **National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF):** A voluntary framework that consists of standards, guidelines, and best practices to manage cybersecurity risk |

**Khung An ninh Mạng (CSF) của Viện Tiêu chuẩn và Công nghệ Quốc gia (NIST):** Một khung tự nguyện bao gồm các tiêu chuẩn, hướng dẫn và biện pháp thực hành tốt nhất để quản lý rủi ro an ninh mạng

|  |
| --- |
| **Privacy protection:** The act of safeguarding personal information from unauthorized use |

**Bảo vệ quyền riêng tư:** Hành động bảo vệ thông tin cá nhân khỏi việc sử dụng trái phép

|  |
| --- |
| **Protected health information (PHI):** Information that relates to the past, present, or future physical or mental health or condition of an individual |

**Thông tin sức khỏe được bảo vệ (PHI):** Thông tin liên quan đến sức khỏe hoặc tình trạng thể chất hoặc tinh thần trong quá khứ, hiện tại hoặc tương lai của một cá nhân

|  |
| --- |
| **Security architecture:** A type of security design composed of multiple components, such as tools and processes, that are used to protect an organization from risks and external threats |

**Kiến trúc bảo mật:** Một loại thiết kế bảo mật bao gồm nhiều thành phần, chẳng hạn như các công cụ và quy trình, được sử dụng để bảo vệ tổ chức khỏi các rủi ro và các mối đe dọa bên ngoài

|  |
| --- |
| **Security controls:** Safeguards designed to reduce specific security risks |

**Kiểm soát bảo mật:** Các biện pháp bảo vệ được thiết kế để giảm thiểu rủi ro bảo mật cụ thể

|  |
| --- |
| **Security ethics:** Guidelines for making appropriate decisions as a security professional |

**Đạo đức bảo mật:** Hướng dẫn đưa ra quyết định phù hợp với tư cách là chuyên gia bảo mật

|  |
| --- |
| **Security frameworks:** Guidelines used for building plans to help mitigate risk and threats to data and privacy |

**Khung bảo mật:** Nguyên tắc dùng để xây dựng kế hoạch giúp giảm thiểu rủi ro và các mối đe dọa đối với dữ liệu và quyền riêng tư

|  |
| --- |
| **Security governance:** Practices that help support, define, and direct security efforts of an organization |

**Quản trị bảo mật:** Các hoạt động giúp hỗ trợ, xác định và chỉ đạo các nỗ lực bảo mật của một tổ chức

|  |
| --- |
| **Sensitive personally identifiable information (SPII):** A specific type of PII that falls under stricter handling guidelines |

**Thông tin nhận dạng cá nhân nhạy cảm (SPII):** Một loại PII cụ thể nằm trong các hướng dẫn xử lý chặt chẽ hơn

## **Thử thách module 3**