NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST Cybersecurity Framework 2.0:
Cybersecurity, Enterprise Risk Management, and Workforce Management Quick-Start Guide

U.S. Department of Commerce
Howard Lutnick, Secretary of Commerce

National Institute of Standards and Technology
Craig Burkhardt, Acting Under Secretary of Commerce for Standards and Technology and Acting NIST Director

NIST Special Publication
NIST SP 1308
https://doi.org/10.6028/NIST.SP.1308
March 2026

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NISTサイバーセキュリティフレームワーク2.0：サイバーセキュリティ、事業体リスクマネジメント、および 人材マネジメント クイックスタートガイド

U.S. Department of Commerce
Howard Lutnick, Secretary of Commerce

National Institute of Standards and Technology
Craig Burkhardt, Acting Under Secretary of Commerce for Standards and Technology and Acting NIST Director

NIST Special Publication
NIST SP 1308
https://doi.org/10.6028/NIST.SP.1308
2026年3月

INTRODUCTION

Purpose of this Guide

This Quick-Start Guide (QSG) draws on concepts and practices from enterprise risk management, cybersecurity risk management, and workforce management **to help organizations improve communication about cybersecurity risks, plan workforce decisions, and implement risk-informed responses**. The scope of this QSG will vary depending on the user, but generally applies at the organization level, where cybersecurity risks of multiple systems are managed, and at the enterprise level, where senior leaders take on unique risk management responsibilities spanning multiple organizations (see NIST IR 8286 for a discussion of these levels). This QSG addresses the need for agile, continuous workforce adaptation to rapidly evolve for emerging threats and technologies. Organizations should iterate through this process regularly, with provisions for rapid response when significant threat landscape changes occur.

Cybersecurity Risk Management (CSRM)

Cybersecurity risks are one of many types of risk that all organizations should manage and integrate into their broader enterprise risk management (ERM) strategy. Potential negative impacts to organizations from cybersecurity risks include higher costs, data loss, operational disruptions, lost revenue, reputational damage, and reduced innovation. In addition to negative risks, positive risks—where an enterprise asset may constitute an opportunity to realize a benefit or positive impact—should also be considered. **The NIST Cybersecurity Framework (CSF) 2.0 provides guidance for managing cybersecurity risks** by helping organizations understand, assess, prioritize, and communicate consistently about cybersecurity efforts, including those related to the cybersecurity workforce.

Making ERM, CSRM, and Workforce Risk-Based Decisions

Gaps and opportunities related to the sufficiency and competency of an enterprise's cybersecurity workforce are one type of cybersecurity risk. This guide helps organizations make informed workforce and risk decisions based on the integration of ERM, CSRM, and workforce management strategy. For instance, based on the current organizational risk appetite and tolerance, cybersecurity strategy, mission objectives, budget, and existing cybersecurity workforce, an organization might decide they need to hire, upskill, reorganize, or change a risk treatment altogether to effectively address their current cybersecurity risks or to achieve their targeted cybersecurity outcomes. People, processes, and technology combine to achieve acceptable levels of enterprise and cybersecurity risk, and cybersecurity workforce assessment is often made more difficult by disconnects between technical and human resources teams. **The NICE Framework focuses on people**, **providing a common language for describing cybersecurity work, including the Work Roles an organization's cybersecurity staff must perform**.

Key Terms

- **Enterprise Risk Management:** An effective organization-wide approach to addressing the full spectrum of the organization's significant risks by understanding the combined impact of risks as an interrelated portfolio rather than addressing risks only within silos [NIST IR 8286r1].
- **Cybersecurity Risk Management:** The process of managing uncertainty on or within information and technology [NIST IR 8286D-upd1].
- **Cybersecurity Workforce Management:** Includes individuals and teams whose primary work responsibilities impact an organization's ability to protect its data, technology systems, and operations—both traditional IT security as well as related roles that apply cybersecurity skills and knowledge [NIST SP 800-181r1].

はじめに

本ガイドの目的

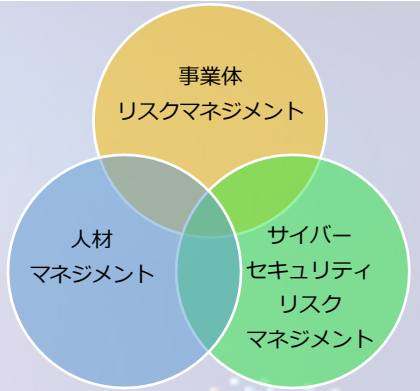
本クイックスタートガイド（QSG）は、事業体リスクマネジメント、サイバーセキュリティリスクマネジメント。および人材マネジメントの概念とプラクティスに基づき、**組織がサイバーセキュリティリスクに関するコミュニケーションを改善し、人材に関する意思決定を計画し、リスクを考慮した対応を実装できるよう支援するものである。** 本QSGの適用範囲はユーザーによって異なるが、一般的には、複数のシステムのサイバーセキュリティリスクを管理している組織レベル、および上級幹部が複数の組織にまたがる独自のリスク管理責任を担う企業レベルに適用される（これらのレベルに関する議論については、NIST IR 8286 を参照のこと）。本QSGは、新たな脅威や技術の急速な進化に対応するため、人材を機敏かつ継続的に適応させる必要性に対応するものである。組織は、脅威環境に重大な変化が生じた場合に迅速に対応できる体制を備えつつ、このプロセスを定期的に反復することが望ましい。

サイバーセキュリティリスクマネジメント（CSRM）

サイバーセキュリティリスクは、すべての組織が管理し、より広範な事業体リスクマネジメント（ERM）戦略に統合することが望ましい多くの種類のリスクの一つである。サイバーセキュリティリスクが組織にもたらす潜在的なインパクトには、コストの増加、データの損失、業務の中断、収益の損失、評判の毀損、イノベーションの阻害などが含まれる。ネガティブなリスクに加え、事業体の資産が利益またはプラスのインパクトをもたらす機会となり得る「ポジティブなリスク」についても考慮することが望ましい。 **NIST サイバーセキュリティフレームワーク（CSF）2.0は**、組織がサイバーセキュリティの取り組み（サイバーセキュリティ人材に関連する取り組みを含む）について理解し、アセスメントし、優先順位を付け、一貫して伝達できるよう支援することで、**サイバーセキュリティリスクを管理するためのガイダンスを提供する。**

ERM、CSRM、および人材に関するリスクベースの意思決定

事業体のサイバーセキュリティ人材の充足度や能力に関連するギャップと機会は、サイバーセキュリティリスクの一種である。本ガイドは、ERM、CSRM、および人材マネジメント戦略の統合に基づき、組織が情報に基づいた人材およびリスクに関する意思決定を行うのに役立つ。 例えば、組織の現在のリスク選好度とリスク許容度、サイバーセキュリティ戦略、ミッションの目的、予算、および既存のサイバーセキュリティ人材に基づき、組織は、現在のサイバーセキュリティリスクに効果的に対処したり、目標とするサイバーセキュリティ成果を達成したりするために、採用、スキルアップ、組織再編、あるいはリスク対応策の全面的な変更が必要であると判断する可能性がある。人、プロセス、テクノロジーが組み合わさって、事業体リスクおよびサイバーセキュリティリスクの受容可能なレベルが達成されるが、技術チームと人事チーム間の連携不足により、サイバーセキュリティ人材のアセスメントはしばしば困難になる。**NICEフレームワークは「人」に焦点を当て、組織のサイバーセキュリティ担当者が果たすべき職務上の役割を含め、サイバーセキュリティ業務を記述するための共通言語を提供している。**



主要用語

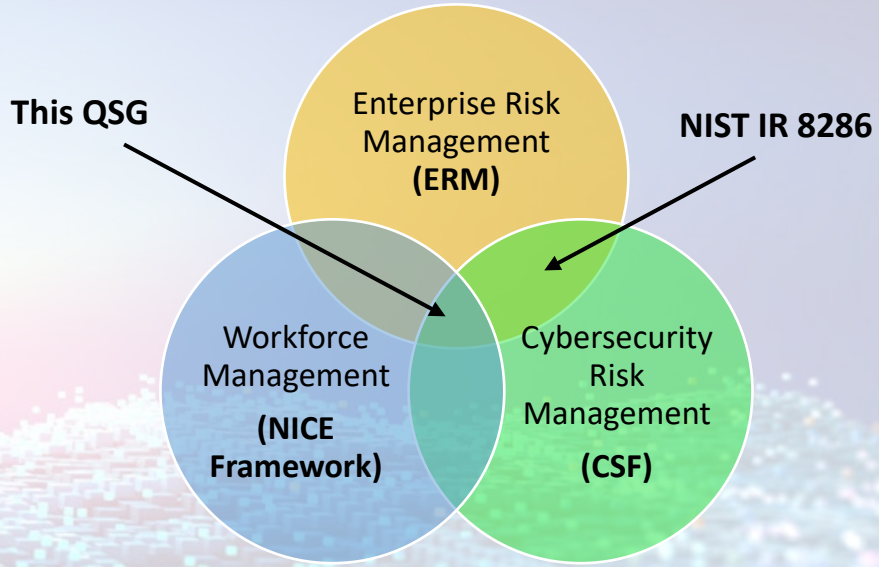
- **事業体リスクマネジメント：**各部門が個別にリスクに対処するのではなく、相互に関連するポートフォリオとしてその複合的なインパクトを理解することによって、組織の重大なリスクの全範囲に対処するための、組織全体にわたる効果的なアプローチ [NIST IR 8286r1]。
- **サイバーセキュリティリスクマネジメント：**情報および技術に関する、あるいはそれら内部における不確実性を管理するプロセス [NIST IR 8286D-upd1]。
- **サイバーセキュリティ人材マネジメント：**組織のデータ、技術システム、および業務を保護する能力にインパクトを与える主要な職責を負う個人およびチームを含む。これには、従来のITセキュリティに加え、サイバーセキュリティのスキルおよび知識を応用する関連職務も含まれる [NIST SP 800-181r1]。

RESOURCES TO ALIGN CYBERSECURITY, ERM, AND WORKFORCE MANAGEMENT

Three NIST resources enable users to align their cybersecurity, ERM, and workforce management practices in a streamlined process:

- The Cybersecurity Framework (CSF) 2.0 helps organizations—regardless of size, sector, or maturity—**understand and communicate their cybersecurity efforts**. At its most granular level, the CSF defines Categories and Subcategories of specific outcomes of cybersecurity risk management activities. Organizations use those outcomes to construct an Organizational Profile. Communities of interest can also use the CSF 2.0 outcome statements to create a Community Profile, which is a baseline of CSF outcomes that addresses shared interests and goals among a group of organizations.
- The NICE Framework helps organizations **improve cybersecurity capabilities, communicate work responsibilities, and develop training**. Once an organization's current or target cybersecurity posture in terms of CSF cybersecurity outcomes is identified, the NICE Framework can be used to identify how to support or reach that target goal. The most granular elements of the NICE Framework are Task, Knowledge, and Skill (TKS) statements. Work Roles are groups of TKS statements relevant to specific cybersecurity functions.
- The NIST IR 8286 series provides a suite of guidance documents and templates to support improved communication between cybersecurity professionals and organizational leadership and to **align cybersecurity risk management with broader ERM practices**.

Some units within an organization may already use individual resources described above; however, organizations will benefit from using all three together. This QSG connects the three resources and their respective stakeholder groups in a holistic, workforce-focused cybersecurity risk management process. Additional resources are listed on page 11.



Questions to Consider

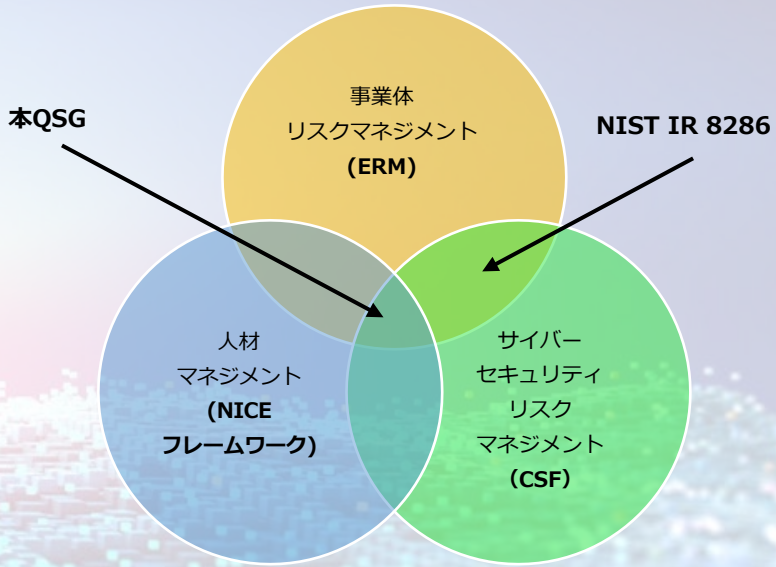
- **What** cybersecurity risks are likely to affect delivery of the organization's mission?
- **What** actions are necessary to mitigate identified cybersecurity risks?
- **How** is cybersecurity being incorporated into the broader ERM strategy?
- **How** are workforce capabilities of third parties and vendors assessed and monitored?
- **How** should information sharing and decision making among ERM, CSRM, and workforce teams take place?
- **Who** has the skills and knowledge necessary to achieve a given cybersecurity outcome?
- **What** contractual requirements exist for competencies and certifications of vendor staff?
- **Which** cybersecurity functions should be automated vs. requiring human judgment?

サイバーセキュリティ、事業体リスクマネジメント、および人材マネジメントを整合させるためのリソース

以下の3つのNISTリソースを活用することで、ユーザーはサイバーセキュリティ、事業体リスクマネジメント、および人材マネジメントの実践を、効率的なプロセスで整合させることができる：

- サイバーセキュリティフレームワーク（CSF）2.0は、規模、業種、成熟度にかかわらず、組織が**自組織のサイバーセキュリティの取り組みを理解し、伝達するの**を支援する。最も粒度の細かいレベルにおいて、CSFはサイバーセキュリティリスクマネジメント活動の具体的な成果に関するカテゴリとサブカテゴリを定義している。組織は、これらの成果を用いて組織プロファイルを構築する。共通の関心を持つコミュニティも、CSF2.0の成果記述を用いて「コミュニティプロファイル」を作成できる。これは、複数の組織間で共通の関心事および目標に対応した、CSFの成果のベースラインである。
- NICEフレームワークは、組織が**サイバーセキュリティ能力を向上させ、業務上の責任を明確に伝達し、トレーニングを開発する**のに役立つ。CSFのサイバーセキュリティ成果の観点から、組織の現状または目標とするサイバーセキュリティ態勢が識別されると、NICEフレームワークを用いて、その目標を達成または支援する方法を識別することができる。NICEフレームワークの最も粒度の細かい要素は、タスク（Task）、知識（Knowledge）、スキル（Skill）（TKS）ステートメントである。ワークロール（職務役割）とは、特定のサイバーセキュリティ機能に関連するTKSステートメントのグループを指す。
- NIST IR 8286シリーズは、サイバーセキュリティ専門家と組織の経営陣との間のコミュニケーションの向上を支援し、**サイバーセキュリティリスクマネジメントをより広範なERM（事業体リスクマネジメント）のプラクティスと整合させる**ための、一連のガイダンス文書およびテンプレートを提供している。

組織内の一部の部門では、すでに上記の個々のリソースを利用しているかもしれない。しかし、これら3つを併用することで、組織はより大きな効果を得ることができる。本QSGは、これら3つのリソースとそれぞれのステークホルダーグループを、包括的かつ人材に焦点を当てたサイバーセキュリティリスクマネジメントプロセスの中で結びつける。追加のリソースは、11ページに記載されている。



検討すべき質問

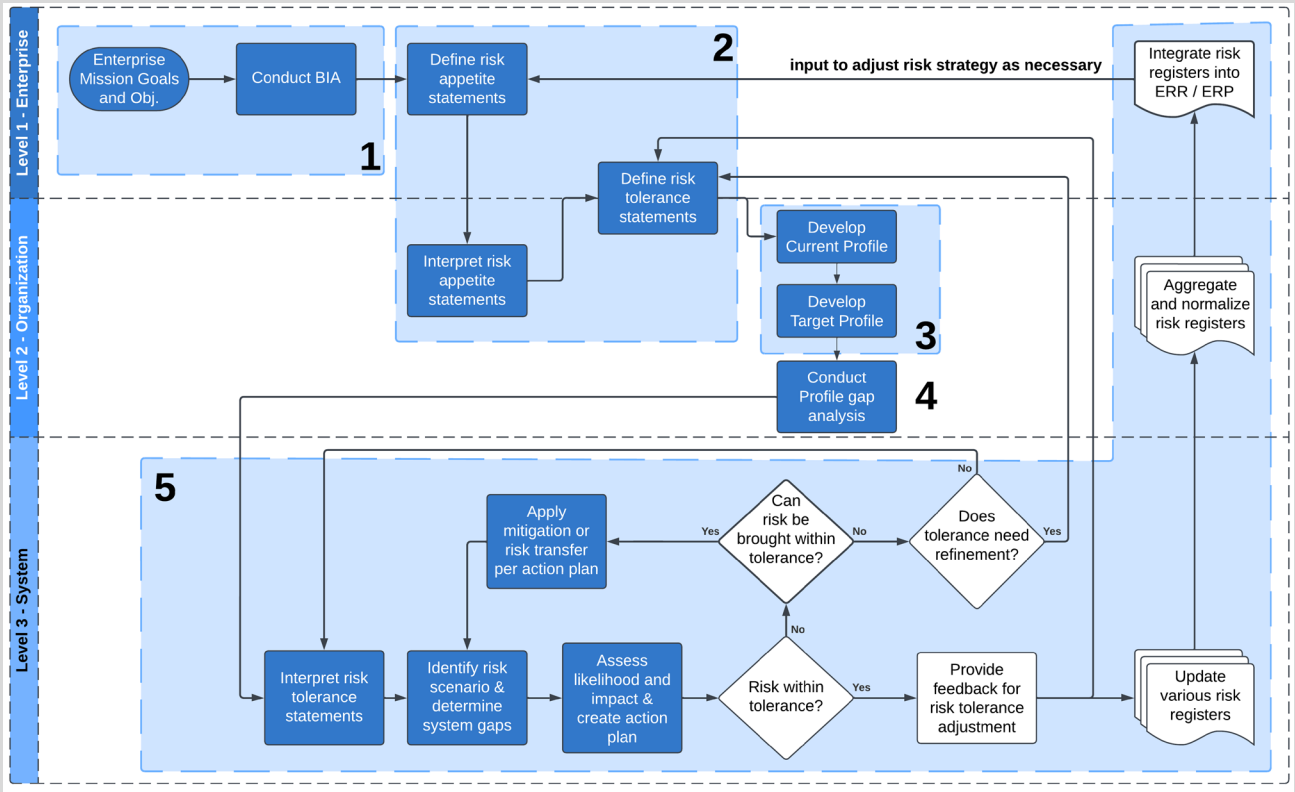
- 組織のミッションの遂行に影響を及ぼす可能性のあるサイバーセキュリティリスクは**何か**？
- 識別されたサイバーセキュリティリスクを軽減するために必要な措置は**何か**？
- サイバーセキュリティは、より広範なERM戦略に**どのように**組み込まれているか？
- サードパーティおよびベンダーの人材の能力は、**どのように**評価および監視されているか？
- ERM、CSRM、および人材チームの間の情報共有および意思決定は、**どのように**行われることが望ましいか？
- 特定のサイバーセキュリティ成果を達成するために必要なスキルおよび知識を持つのは**誰か**？
- ベンダーのスタッフの能力および資格に関する契約上の要件は**何か**？
- **どの**サイバーセキュリティ機能を自動化することが望ましいか、あるいは人間の判断を必要とすることが望ましいか？

NOTIONAL APPLICATION OF THE CSF

The remainder of this guide is organized into the five Cybersecurity Framework Profile implementation steps in alignment with CSRM/ERM integration and workforce management.

5 Steps for Creating and Using a CSF Organizational Profile

Five Cybersecurity Framework Profile implementation steps in alignment with CSRM/ERM integration (figure 7, NIST IR 8286Cr1)



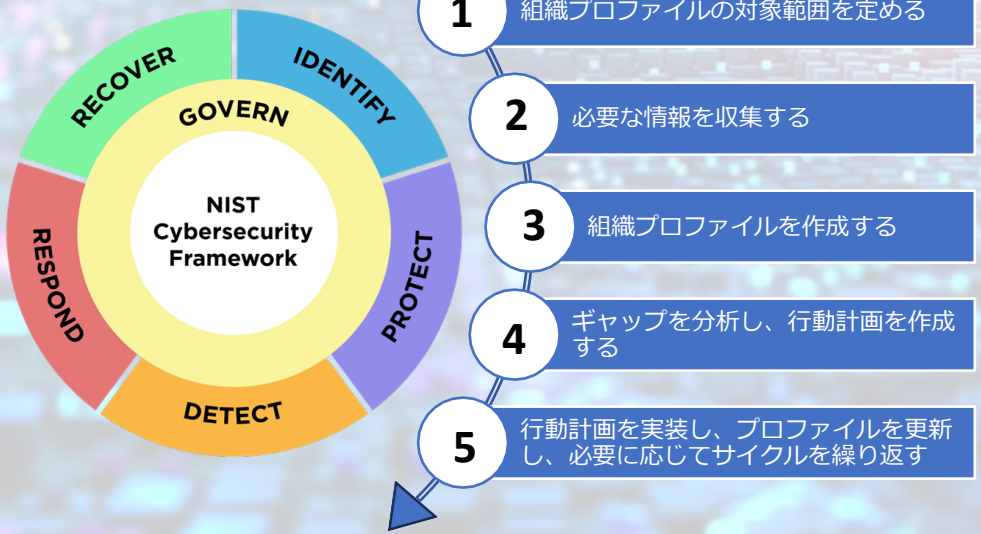
When used together, these steps enable users to align their cybersecurity, ERM, and workforce management practices to adequately address risks and inform continuous improvement of CSRM.

Note: the Business Impact Analysis in Step 1 provides a business process prioritization to inform risk direction (see NIST IR 8286Cr1).

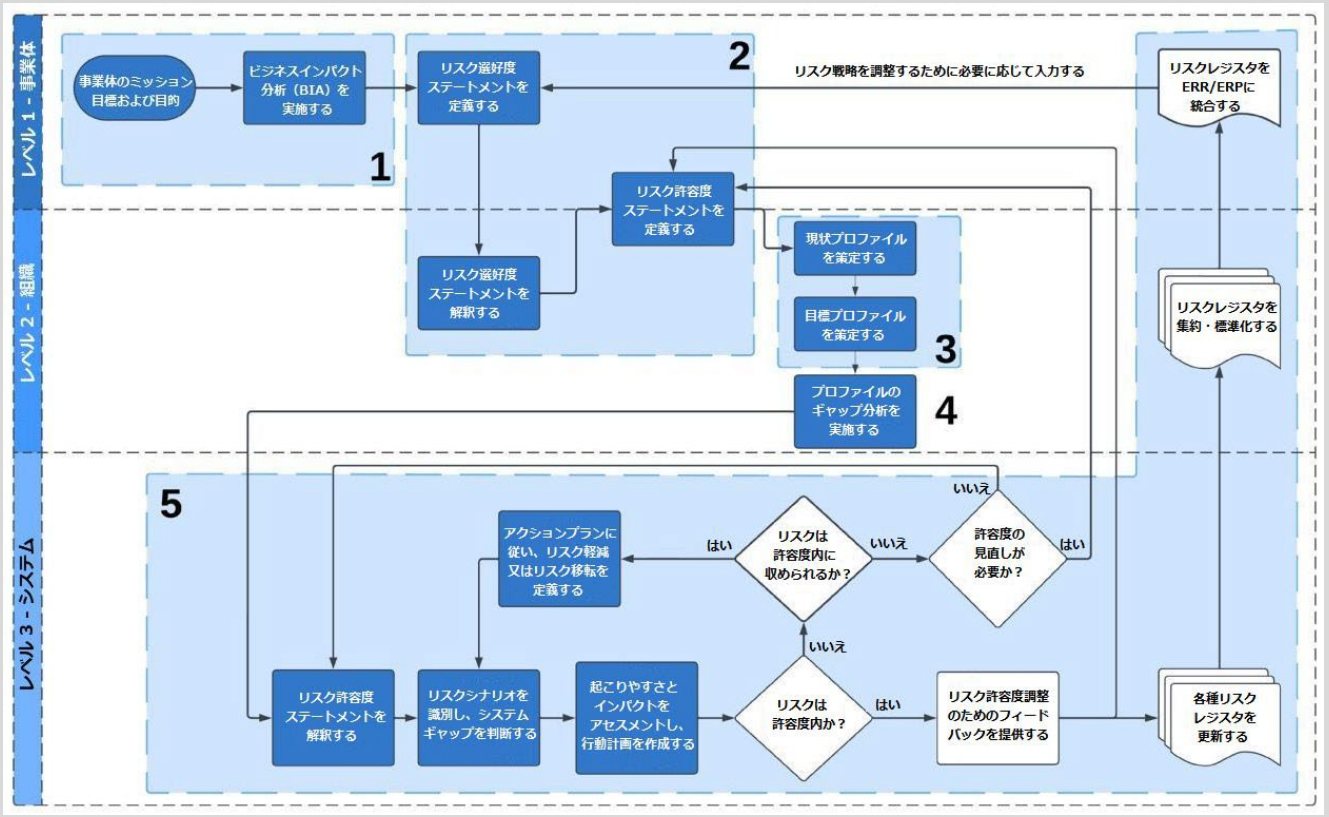
CSFの概念的な適用

本ガイドの残りの部分は、CSRM/ERMの統合および人材マネジメントと整合して、サイバーセキュリティフレームワークプロファイルの5つの実装ステップに沿って構成されている。

CSF組織プロファイルの作成と活用のための5つのステップ



CSRM／ERM統合と整合したサイバーセキュリティフレームワークプロファイルの5つの実装ステップ（図7、NIST IR 8286Cr1）



これらの手順を組み合わせて使用することで、ユーザーはサイバーセキュリティ、事業体リスクマネジメント、および人材マネジメントのプラクティスを整合させ、リスクに適切に対処し、CSRMの継続的な改善に役立てることができる。

注：ステップ1のBIA（ビジネスインパクト分析）は、リスク対応の方向性を決定するためのビジネスプロセスの優先順位付けを提供する（NIST IR 8286Cr1を参照）。

STEP 1: SCOPE THE ORGANIZATIONAL PROFILE

Overview: The scope defines the high-level facts, assumptions, and constraints on which the Profiles will be based. The first step is to convene stakeholders from across the enterprise with the perspective and authority to collect risk and workforce data, articulate needs, and execute identified risk responses. The purpose of the group will be to define the scope of the effort, align security risks to the enterprise mission, and make informed risk and workforce decisions based upon current and desired risk context, priorities, budget, etc.

Sample activities in this step:

1. Identify accountable leads from board-level, executive leadership, cybersecurity, enterprise risk management, and workforce management teams and establish an initial process timeline.
2. Review the organization's mission, goals, objectives and high-level priorities.
3. Conduct/review the business impact analysis (BIA), which includes identifying high value assets that are critical to achieving organizational objectives. This information is used to scope the CSF Organizational Profile. The BIA examines the potential impact associated with the loss or degradation of an enterprise's information assets based on a qualitative or quantitative assessment of the criticality and sensitivity of those assets. Learn more in NIST IR 8286D-upd1.
4. Establish change management protocols and executive sponsorship to ensure cross-functional collaboration among teams.
5. Identify third-party dependencies and include their workforce capabilities in scope.

Notes:

- An organization may use several Profiles. Each Profile can have a distinct scope (e.g., enterprise, system), which defines the high-level facts and assumptions on which the Profile is based.
- Stakeholder teams convened in this step may or may not have experience working closely together. Efforts should be made to obtain a shared understanding of each unit's roles, responsibilities, and internal processes and to create a high performing team.
- Organizations may find it beneficial to pilot the process described in this QSG by beginning with a subset of CSF outcomes.

Relevant CSF Core Category: Organizational Context (GV.OC)

The circumstances – mission, stakeholder expectations, dependencies, and legal, regulatory, and contractual requirements – surrounding the organization's cybersecurity risk management decisions are understood.

Key Term: High Value Asset

Information or an information system that is so critical to an organization that the loss or corruption of this information or loss of access to the system would have serious impacts on the organization's ability to perform its mission or conduct business [NIST SP 800-160 Vol. 2 Rev. 1].

ステップ1：組織プロファイルの対象範囲を定める

概要：対象範囲は、プロファイルの基礎となるハイレベルの事実、前提条件、および制約を定義するものである。最初のステップは、リスクおよび人材に関するデータを収集し、ニーズを明確にし、識別されたリスクへの対応を実行する視点と権限を持つステークホルダーを、事業体全体から招集することである。 このグループの目的は、取り組みの対象範囲を定義し、セキュリティリスクを事業体のミッションと整合させ、現状および目標とするリスク環境、優先順位、予算などに基づいて、情報に基づいたリスクおよび人材に関する意思決定を行うことである。

本ステップにおける活動例：

1. 取締役会レベル、経営陣、サイバーセキュリティ、事業体リスクマネジメント、および人材マネジメントの各チームから責任者を識別し、初期のプロセススケジュールを策定する。
2. 組織のミッション、目標、目的、およびハイレベルの優先順位を見直す。
3. ビジネスインパクト分析（BIA）を実施／レビューする。これには、組織の目標達成に不可欠な高価値資産の識別が含まれる。この情報は、CSF組織プロファイルの対象範囲を定めるために使用される。ビジネスインパクト分析（BIA）では、情報資産の重要度および機密性に関する定性的または定量的評価に基づき、事業体の情報資産の喪失または機能低下に伴う潜在的なインパクトを検証する。詳細は NIST IR 8286D-upd1を参照。
4. チーム間の部門横断的な連携を確保するため、変更管理の手順および経営陣の支援体制を確立する。
5. サードパーティへの依存関係を識別し、それらの人材能力を対象範囲に含める。

注記：

- 組織は複数のプロファイルを使用する場合がある。各プロファイルは独自の対象範囲（例えば、事業体、システム）を持つことができ、その対象範囲はプロファイルの基礎となるハイレベルの事実と仮定を定義する。
- 本ステップで招集されるステークホルダーチームは、これまで緊密に連携した経験がある場合もあれば、ない場合もある。各部門の役割、責任、内部プロセスについて共通認識を持ち、高いパフォーマンスを発揮するチームを構築するよう努めることが望ましい。
- 組織は、CSF成果の一部から着手することで、本QSGに記載されたプロセスを試験的に実施することが有益である場合がある。

関連するCSFコアのカテゴリ：
組織の状況（GV.OC）

組織のサイバーセキュリティリスク管理の意思決定を取り巻く状況（ミッション、ステークホルダーの期待、依存関係、および法的要求事項、規制上の要件、契約上の要求事項）が理解されている。

重要用語：高価値資産

組織にとって極めて重要な情報または情報システムであり、この情報の喪失もしくは破損、または当該システムへのアクセス喪失が、組織のミッション遂行能力または事業運営に深刻なインパクトを及ぼすもの [NIST SP 800-160 Vol. 2 Rev. 1]。

STEP 2: GATHER THE INFORMATION NEEDED TO PREPARE THE ORGANIZATIONAL PROFILE

Overview: Having a clear picture of the organization's current CSRM, ERM, and workforce context and risk environment helps leadership adequately address the most critical risks to an organization's mission.

ERM Information Source Considerations

- Risk appetite and risk tolerance statements, which are used to define parameters for determining acceptable levels of risk
- BIA registers
- Enterprise risk profiles
- Third-party risk assessments, including vendor workforce capabilities

CSRM Information Source Considerations

- A list of cybersecurity requirements, laws, rules, regulations, and standards followed by the organization
- Emerging and evolving risk factors that require new workforce capabilities
- Organizational policies
- Key Risk Indicators and Key Performance Indicators
- Cybersecurity risk registers

Workforce Information Source Considerations

- Workforce planning information, such as organizational charts or lists of filled and unfilled cybersecurity and risk management positions
- Inventory of existing skillsets within the organization (including professional certification data)
- Existing recruiting and training programs
- The NICE Framework to CSF 2.0 Crosswalk

Additional Information Source Considerations

- CSF Community Profiles, which can be used as the basis for an organization's own Target Profile
- NIST Guide to Creating Community Profiles

Relevant CSF Core Category and Subcategories: Risk Management Strategy (GV.RM)

The organization's priorities, constraints, risk tolerance and appetite statements, and assumptions are established, communicated, and used to support operational risk decisions.

- GV.RM-05: Lines of communication across the organization are established for cybersecurity risks, including risks from suppliers and other third parties.
- GV.RM-06: A standardized method for calculating, documenting, categorizing, and prioritizing cybersecurity risks is established and communicated.

Key Term: Business Impact Analysis (BIA) Register

A centralized registry of important asset management information, such as system ownership, contact information for key stakeholders, and characteristics of the physical devices (or services). Since asset management is an important element of cybersecurity risk management, this information is quite valuable for protecting the asset, detecting cyber events, responding quickly to potential issues, and recovering services when necessary. A BIA register is related to but separate from a risk register, which is a repository of risk information including the data understood about risks over time [NIST IR 8286D-upd1].

ステップ2：組織プロファイルを作成するために必要な情報を収集する

概要：組織の現在のCSRM、ERM、および人材状況やリスク環境を明確に把握することは、経営陣が組織のミッションにとって最も重大なリスクに適切に対処する上で役立つ。

ERMの情報源に関する考慮事項

- 受容可能なリスクのレベルを決定するためのパラメータを定義するために使用される、リスク選好度およびリスク許容度のステートメント
- BIA（ビジネスインパクト分析）レジスタ
- 企業のリスクプロファイル
- ベンダーの人材能力を含む、サードパーティのリスクアセスメント

CSRMの情報源に関する考慮事項

- 組織が遵守するサイバーセキュリティ要件、法律、規則、規制、および標準のリスト
- 新たな人材能力を必要とする、新たに発生・変化しているリスク要因
- 組織のポリシー
- 主要リスク指標と主要業績評価指標
- サイバーセキュリティリスクレジスタ

人材の情報源に関する考慮事項

- 組織図、またはサイバーセキュリティおよびリスクマネジメントのポジションにおける充足状況・未充足状況のリストなど、人材計画に関する情報
- 組織内の既存のスキルセットのリスト（専門資格データを含む）
- 既存の採用および研修プログラム
- NICEフレームワークとCSF 2.0の対応表

その他の情報源に関する考慮事項

- 組織独自のターゲットプロファイルの基礎として利用できるCSFコミュニティプロファイル
- NISTコミュニティプロファイル作成ガイド

関連するCSFコアのカテゴリおよびサブカテゴリ：
リスクマネジメント戦略（GV.RM）

運用リスクの意思決定を支援するために、組織の優先順位、制約条件、リスク許容度、リスク選好度の表明、及び前提条件が確立され、伝達され、使用されている。

- GV.RM-05：サプライヤ及びその他の第三者によるリスクを含む、サイバーセキュリティリスクに関する組織全体にわたるコミュニケーション系統が確立されている。
- GV.RM-06：サイバーセキュリティリスクの計算、文書化、分類、優先順位付けのための標準化された方法が確立され、伝達されている。

重要用語：ビジネスインパクト分析（BIA）レジスタ

システムの所有権、主要なステークホルダーの連絡先、物理的なデバイス（またはサービス）の特性など、重要な資産管理情報を一元的に管理する登録簿。資産管理はサイバーセキュリティリスクマネジメントの重要な要素であるため、この情報は、資産の保護、サイバーインシデントの検知、潜在的な問題への迅速な対応、および必要に応じたサービスの復旧において非常に価値がある。 BIAレジスタは、リスクレジスタとは関連しているものの、別個のものである。リスクレジスタとは、時間の経過とともに把握されたリスクに関するデータを含む、リスク情報の保管場所である [NIST IR 8286D-upd1]。

STEP 3: CREATE THE ORGANIZATIONAL PROFILE

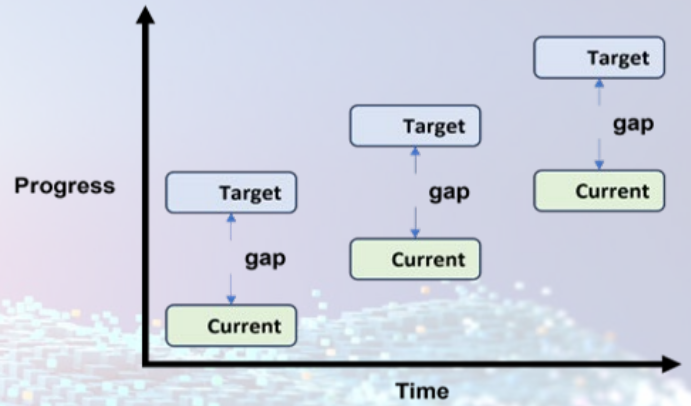
Overview: An Organizational Profile describes an organization's current and/or target cybersecurity posture in terms of cybersecurity outcomes from the Cybersecurity Framework (CSF) Core. Organizational Profiles are used to understand, tailor, assess, and prioritize cybersecurity outcomes based on an organization's mission objectives, stakeholder expectations, threat landscape, and requirements. Organizational Profiles can be categorized as:

- A **Current Profile** that specifies the CSF outcomes an organization currently achieves, and which characterizes how or to what extent each outcome is being achieved.
- A **Target Profile** specifies the desired CSF outcomes an organization has selected and prioritized for achieving its cybersecurity risk management objectives. It considers anticipated changes to the organization's cybersecurity posture, such as: new requirements, new technology adoption, and trends in threat intelligence.
- **Note:** These are viewed side-by-side as one artifact within the CSF Organizational Profile template to help organizations identify and analyze the risks presented within the gap between Current and Target.

Sample activities in this step:

1. Review the CSF Functions, Categories, and Subcategories to determine outcomes the organization currently achieves, and to what extent. This step provides an opportunity for enterprise stakeholders to review and analyze what is currently being done while considering enterprise risk context and risk strategy.
2. Review the CSF Functions, Categories, and Subcategories to determine target-state outcomes, with a clear understanding of organizational priorities and budget. This step provides an opportunity for cybersecurity risk managers, informed by an understanding of the risk implications defined in the current profile, to determine the desired set of processes and activities that will accomplish stakeholder expectations cost-effectively and efficiently.
3. Throughout each of the above activities, workforce managers, in conjunction with the CSRM and ERM teams, examine how workforce roles and skills contribute to risk management success, or could be improved to do so. Continuous profile updates reflect improvements and adjustments based on evolving risk conditions.

Drive Progress Over Time with CSF Profiles



Note: The gaps within this graphic are uniform to illustrate the general concept, but gaps between Current and Target state will vary.

Resources

- NIST provides a customizable CSF Organizational Profile template as a spreadsheet. You can download and use it to create Current and Target Profiles for your organization.
- View the CSF 2.0 Profiles page in the CSF 2.0 Resource Library.

CSF 2.0：サイバーセキュリティ、事業体リスクマネジメント、および人材マネジメント
クイックスタートガイド

ステップ3：組織プロファイルの作成

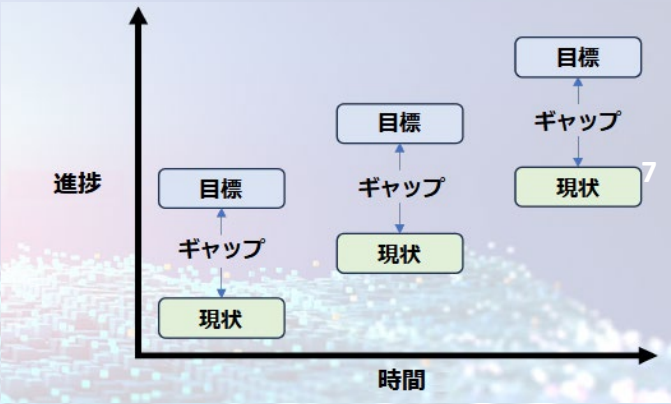
概要：組織プロファイルは、サイバーセキュリティフレームワーク（CSF）コアのサイバーセキュリティ成果の観点から、組織の現在および／または目標とするサイバーセキュリティ態勢を記述するものである。組織プロファイルは、組織のミッション目標、ステークホルダーの期待、脅威の状況、および要件に基づき、サイバーセキュリティの成果を理解、調整、アセスメント、優先順位を付けるために使用される。組織プロファイルは、次のように分類できる。

- 「**現状プロファイル**」とは、組織が現在達成しているCSFの成果を明示し、各成果がどのように、あるいはどの程度達成されているかを特徴づけるものである。
- 「**目標プロファイル**」は、組織がサイバーセキュリティリスクマネジメントの目標を達成するために選択し、優先順位を付けた望ましいCSFの成果を規定するものである。これには、新たな要件、新技術の採用、脅威情報の動向など、組織のサイバーセキュリティ態勢に予想される変化を考慮する。
- **注：**これらは、CSF組織プロファイルテンプレート内で1つの成果物として並べて表示され、組織が「現状」と「目標」の間のギャップに存在するリスクを識別及び分析するのに役立つ。

このステップの活動例

1. CSFの機能、カテゴリ、およびサブカテゴリを確認し、組織が現在達成している成果とその程度を判断する。このステップは、事業体のステークホルダーが、事業体のリスク状況およびリスク戦略を考慮しつつ、現在実施されていることをレビューおよび分析する機会を提供する。
2. 組織の優先事項と予算を明確に把握した上で、CSFの機能、カテゴリ、およびサブカテゴリをレビューし、目標状態の成果を決定する。このステップは、サイバーセキュリティリスクの管理者が、現在のプロファイルで定義されたリスクの影響を理解した上で、ステークホルダーの期待を費用対効果が高く効率的に達成するための、望ましい一連のプロセスと活動を決定する機会を提供する。
3. 上記の各活動を通じて、人材マネジメント担当者は、CSRMおよびERMチームと協力し、人材の役割およびスキルがリスクマネジメントの成功にどのように寄与しているか、あるいはそのためにどのように改善できるかを検討する。プロファイルの継続的な更新は、変化するリスク状況に基づく改善および調整を反映する。

CSFプロファイルによる経時的な進捗の推進



注：この図内のギャップは一般的な概念を示すために均一に描かれているが、現状と目標状態の間のギャップは実際には異なる。

リソース

- NISTは、カスタマイズ可能なスプレッドシート形式のCSF組織プロファイルテンプレートを提供している。これをダウンロードして、自組織の現状および目標プロファイルを作成するために使用できる。
- CSF 2.0 リソースライブラリ内の「CSF 2.0 プロファイル」ページを参照。

STEP 4: ANALYZE GAPS BETWEEN CURRENT AND TARGET PROFILES AND CREATE AN ACTION PLAN

Overview: Once the team has completed the Current and Target profiles, conduct a gap analysis to identify, at a very high level, the risks created by gaps exposed between Current and Target. This gap analysis will support the development of a prioritized action plan supported by a risk register.

Sample activities in this step:

1. Using a pre-existing risk register (if available) and NIST CSF outcome statements, review known risks and make necessary adjustments to the risk register. Add risks identified during the gap analysis that may not have been identified.
2. Review the risk register to understand which risks are most critical to achieving the organization's mission and assess who will be the risk owner and risk action owner. The focus shifts to analyzing the internal and external workforce gaps relative to risk.
3. Carefully consider and designate risk ownership. Those designated as the risk owners should continuously monitor risk conditions and remain accountable to internal and external authorities. A gap analysis between the assigned risk owner and the risk work role can be conducted to see if the practitioner has the competencies necessary to address the problem. Since risk conditions may change as information is aggregated, responsibility and accountability should be periodically reviewed to ensure that the risk owner is appropriate.
4. Complete a gap analysis using a crosswalk between the NICE Framework and the CSF. Does the organization have the requisite staff needed to adequately address the risk? Begin considering whether it is possible to hire or upskill employees to fill identified gaps. Are there other gaps that exist, such as in roles or job descriptions, organizational or reporting structure, etc.?

Relevant CSF Core Category and Subcategories: Roles, Responsibilities, and Authorities (GV.RR)

Cybersecurity roles, responsibilities, and authorities to foster accountability, performance assessment, and continuous improvement are established and communicated.

- GV.RR-01: Organizational leadership is responsible and accountable for cybersecurity risk and fosters a culture that is risk-aware, ethical, and continually improving
- GV.RR-02: Roles, responsibilities, and authorities related to cybersecurity risk management are established, communicated, understood, and enforced
- GV.RR-03: Adequate resources are allocated commensurate with the cybersecurity risk strategy, roles, responsibilities, and policies
- GV.RR-04: Cybersecurity is included in human resources practices

Sample Risk Register

ID	Priority	Risk Description	Risk Category	Current Assessment			Risk Response Type	Risk Response Cost	Risk Response Description	Risk Owner	Risk Action Owner	Status
				Likelihood	Impact	Exposure Rating						

Key Term: Risk Register

A risk register is "a repository of risk information, including the data understood about risks over time. Typically, a risk register contains a description of the risk, the impact if the risk should occur, the probability of its occurrence, mitigation strategies, risk owners, and a ranking to identify higher priority risks." Each register evolves and matures as other risk activities take place [NIST IR 8286r1].

ステップ4：現状プロファイルと目標プロファイルのギャップを分析し、行動計画を作成する

概要：チームが「現状」および「目標」のプロファイルを作成したら、ギャップ分析を実施し、「現状」と「目標」の間に生じたギャップによって引き起こされるリスクを、非常に高いレベルで識別する。このギャップ分析は、リスクレジスタに裏付けられた優先順位付けされた行動計画の策定を支援する。

このステップの活動例：

1. 既存のリスクレジスタ（利用可能な場合）とNIST CSFの成果の記述を用いて、既知のリスクをレビューし、リスクレジスタに必要な調整を加える。ギャップ分析の過程で識別されたが、これまで識別されていなかった可能性のあるリスクを追加する。
2. リスクレジスタをレビューし、組織のミッションを達成するために最も重要なリスクを把握し、誰がリスク所有者およびリスク対応責任者となるかをアセスメントする。焦点は、リスクに関連する内部および外部の人材ギャップの分析に移る。
3. リスク所有者を慎重に検討し、指定する。リスク所有者に指定された者は、リスクの状況を継続的に監視し、組織内外の権限を持つ者に対して説明責任を果たさなければならない。割り当てられたリスク所有者とリスク対応業務の役割との間のギャップ分析を行い、担当者が問題に対処するために必要な能力を備えているかを確認することができる。情報の集約に伴いリスクの状況が変化する可能性があるため、リスク所有者が適切であることを確実にするために、責任および説明責任を定期的にレビューすることが望ましい。
4. NICEフレームワークとCSFの対応表（クロスウォーク）を用いて、ギャップ分析を完了する。組織は、リスクに適切に対処するために必要な人員を確保しているか？識別されたギャップを埋めるために、従業員の新規採用またはスキルアップが可能かどうか検討を始める。役割や職務記述書、組織体制や報告体制など、他に存在するギャップはあるか？

関連するCSFコアのカテゴリおよびサブカテゴリ：
役割、責任、権限（GV.RR）

説明責任、実績アセスメント、継続的改善を促進するためのサイバーセキュリティの役割、責任、権限が確立され、周知されている。

- GV.RR-01：組織のリーダーシップが、サイバーセキュリティリスクに対する責任と説明責任を負い、リスクを認識し、倫理的で、継続的に改善する文化を育んでいる。
- GV.RR-02：サイバーセキュリティリスクマネジメントに関連する役割、責任、権限が確立され、周知され、理解され、実施されている。
- GV.RR-03: サイバーセキュリティリスク戦略、役割、責任、ポリシーに見合った適切なリソースが割り振られている。
- GV.RR-04: サイバーセキュリティが、人事のプラクティスに含まれている。

リスクレジスタのサンプル

ID	優先度	リスクの説明	リスクのカテゴリ	現状のアセスメント			リスク対応の種類	リスク対応のコスト	リスク対応の説明	リスク所有者	リスク対応責任者	ステータス
				起こりやすさ	インパクト	外部露出の評価						

重要用語：リスクレジスタ

リスクレジスタとは、「時間の経過とともに把握されたリスクに関するデータを含む、リスク情報の保管場所である。通常、リスクレジスタには、リスクの説明、リスクが発生した場合のインパクト、発生確率、軽減策、リスク所有者、および優先度の高いリスクを識別するためのランク付けが含まれる。」各レジスタは、他のリスク関連活動が行われるにつれて進化し成熟していく [NIST IR 8286r1]。

STEP 5: IMPLEMENT THE ACTION PLAN AND UPDATE THE ORGANIZATIONAL PROFILE

Overview: At this step in the CSRM/ERM/workforce alignment process, cybersecurity risk practitioners understand stakeholder expectations, budget, priorities, high value assets, and risks. Equipped with this information, they can now determine the appropriate workforce or risk responses to adequately address the most critical risks to the organization.

Sample activities in this step:

Convene a team to jointly select workforce responses for identified high-priority risks. Workforce responses can include the following, individually or in combination:

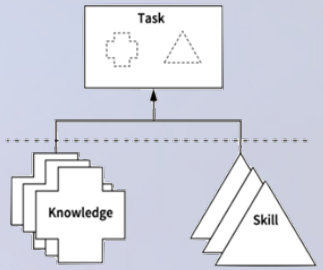
- **Upskill** current employees through professional development, mentorship, or hiring new staff into developmental programs such as internships, apprenticeships, or co-ops.
- **Create new positions**, modify existing ones, or potentially implement a reorganization to address risks.
- **Recruit** fully competent staff to fill a position or positions using the NICE Framework to help identify relevant Work Roles and associated Tasks, Knowledge, and Skills.
- **Augment staff** by contracting with third-parties.

1. Workforce management team: Assign estimated costs for workforce responses selected for each Subcategory, and add details related to timeline, metrics, success criteria, and implementation considerations for associated people, processes, and technology. Costs and timelines will vary depending on organization characteristics. If the identified risks are positive risks, organizations may wish to consider ways to realize, share, or enhance those opportunities [NIST IR 8286r1].
2. If workforce-focused risk responses are not possible, consider adjusting risk response. For example, if training and hiring are not viable options for an absent workforce capability, the organization may consider selecting a different mitigation strategy or changing the risk response type to, for example, accept, avoid, or transfer.
3. The leadership team finalizes and signs off on updated risk register(s).

Key Terms

- **Task:** An activity that is directed toward the achievement of organizational objectives.
- **Knowledge:** A retrievable set of concepts within memory.
- **Skill:** The capacity to perform an observable action.

Relationship Between Task, Knowledge, and Skill Statements.



Credit: NICE Program Office

Resources

- The NICE Framework helps you understand the wide variety of cybersecurity roles and responsibilities that exist across an organization. It can be used to help assess the current workforce as well as identify capability gaps, develop career pathways, create employee upskilling or career plans, and identify courses and training that align with those needs.
- An Employer's Guide to Writing Effective Cybersecurity Job Descriptions provides tips on how to use the NICE Framework when hiring so that you will be equipped to author and communicate about position responsibilities and find the candidate that meets your needs.
- For small businesses with limited resources, the Building Your Small Business' Cybersecurity Team: From In-House to Outsourcing resource helps identify options for possible workforce responses.

ステップ5：行動計画の実施と組織プロファイルの更新

概要：CSRM／ERM／人材整合プロセスのこのステップにおいて、サイバーセキュリティリスク担当者は、ステークホルダーの期待、予算、優先順位、高価値資産、およびリスクを把握する。この情報に基づいて、組織にとって最も重大なリスクに適切に対処するための、適切な人材またはリスク対応を決定できる。

このステップにおける活動例：

チームを招集し、識別された優先度の高いリスクに対する人材対応策を共同で選定する。人材対応策には、以下を単独または組み合わせて含めることができる：

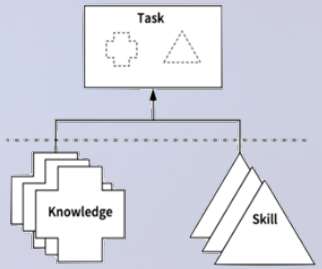
- 専門能力開発、メンター制度、あるいはインターンシップ、見習い制度、協同教育制度（co-ops）などの育成プログラムへの新規採用を通じて、現職従業員の**スキルアップを図る**。
- リスクに対処するため、**新たな役職を創設する**、既存の役職を変更する、あるいは場合によっては組織再編を実施する。
- NICEフレームワークを活用して関連する職務上の役割および関連するタスク、知識、スキルを特定し、1つまたは複数のポストを埋めるために十分な能力を持つスタッフ**を採用する**。
- 第三者との契約により、**人員を増強する**。

1. 人材マネジメントチーム：各サブカテゴリで選択された人材対応策に推定コストを割り当て、関連する人材、プロセス、技術について、スケジュール、指標、成功基準、および実施上の考慮事項に関する詳細を追加する。コストとスケジュールは、組織の特性によって異なる。識別されたリスクがポジティブリスクである場合、組織はそれらの機会を実現、共有、または強化する方法を検討することもできる [NIST IR 8286r1]。
2. 人材に焦点を当てたリスク対応が不可能な場合は、リスク対応の調整を検討する。例えば、不足している人材能力に対して研修や採用が現実的な選択肢でない場合、組織は別の軽減戦略を選択するか、リスク対応の種類を「受容」、「回避」、「移転」などに変更することを検討した方が良い。
3. 経営陣は、更新されたリスクレジスタを確定し、承認する。

重要用語

- **タスク (Task)：**組織の目標達成に向けて行われる活動。
- **知識 (Knowledge)：**記憶の中から引き出せる一連の概念。
- **スキル (Skill)：**観察可能な行動を実行する能力。

タスク、知識、スキルの記述の関係。



出典：NICEプログラム事務局

リソース

- NICEフレームワークは、組織全体に存在する多様なサイバーセキュリティの役割および責任を理解するのに役立つ。これを利用することで、現在の人材を評価するだけでなく、能力のギャップを識別したり、キャリアパスを策定したり、従業員のスキルアップやキャリアプランを作成したり、それらのニーズに沿ったコースやトレーニングを識別したりすることができる。
- 『効果的なサイバーセキュリティ職務記述書を作成するための雇用者ガイド』は、採用時にNICEフレームワークを活用する方法についてヒントを提供している。これにより、職務責任を明確に記述・伝達し、自組織のニーズに合った候補者を見つけるための準備が整う。
- リソースが限られている中小企業向けには、『中小企業のサイバーセキュリティチームの構築：社内体制から外部委託まで』というリソースが、人材対応策の選択肢を識別するのに役立つ。

ITERATION

Overview: In the preceding steps, enterprise stakeholders collected risk information, assessed workforce readiness, and identified workforce and risk responses to address high-priority risks. Now begins the task of continuous monitoring, "which allows organizations to maintain the authorizations of systems and common controls in highly dynamic environments of operation with changing mission and business needs, threats, vulnerabilities, and technologies. Having access to security and privacy information on a continuing basis through reports and dashboards gives organizational officials the ability to make effective and timely risk management decisions, including ongoing authorization decisions" [SP 800-53r5].

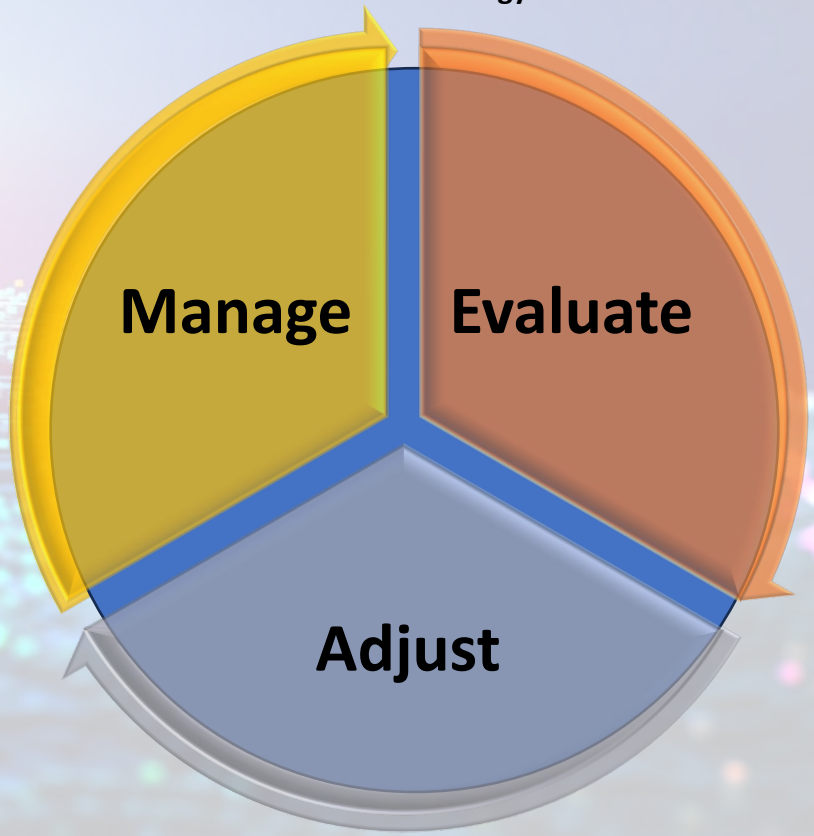
Sample activities:

1. **Manage:** Stakeholders implement identified risk responses and, where applicable, incorporate those responses into broader ERM processes. CSRM/ERM/workforce strategies are continuously monitored, evaluated, and adapted to be successful. Stakeholder teams develop plans and processes for continued collaboration to regularly evaluate how effectively risks are being addressed.

2. **Evaluate:** Establish a process for evaluating how effectively planned interventions have addressed risks, including regular check-ins among stakeholder teams working in priority areas. Consider reassessing the risk after the intervention has been in place for a specified timeframe. Ensure the risk register is updated and that cybersecurity risks are incorporated into broader ERM portfolios, if applicable (see NIST IR 8286r1 for a discussion of risk portfolios). An organization's finance and accounting staff should be involved; if evaluation takes place at the enterprise level, audit committees may be involved as well. This also includes verifying that controls and authorities persist coherently and aren't fragmented across the enterprise.

3. **Adjust:** Once stakeholders have evaluated the chosen workforce intervention and other risk interventions to determine whether they have adequately addressed risk to the organization, the next action is to adjust where necessary. Further workforce responses—such as contracting, temporary workforce augmentation, upskilling, reskilling, reassignment of roles or responsibilities—and risk response adjustments may be necessary.

Continuous Monitoring of CSRM, ERM, and Workforce Strategy.



Learn more about the Manage, Evaluate, Adjust (MEA) lifecycle within NIST IR 8286Cr1

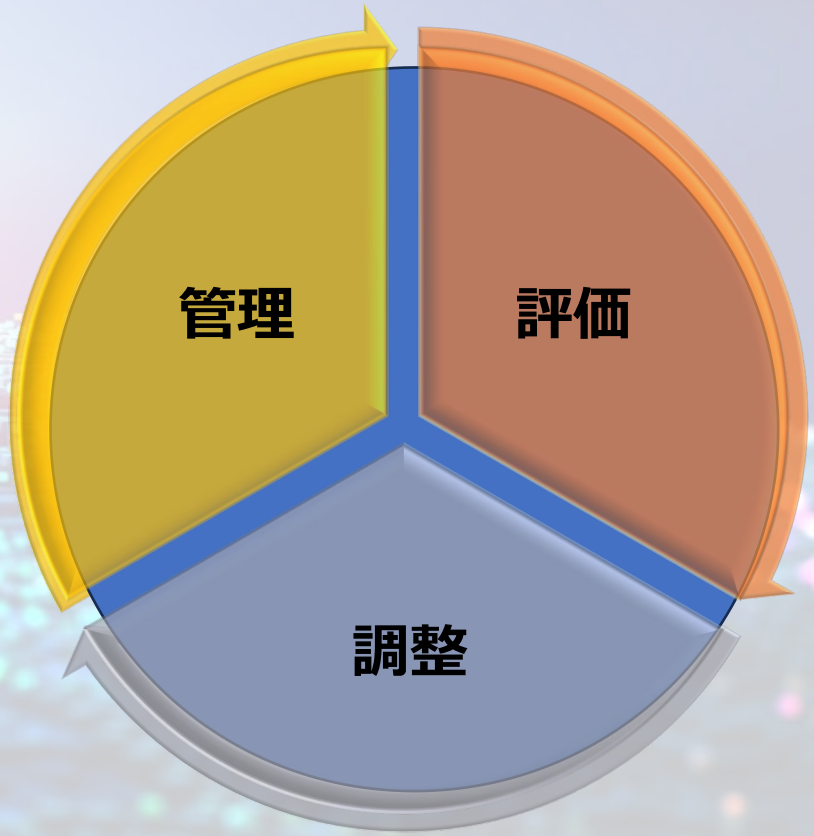
反復

概要：これまでのステップにおいて、企業のステークホルダーはリスク情報を収集し、人材の準備状況を評価し、優先度の高いリスクに対処するための人材対応およびリスク対応策を識別した。 ここから、継続的な監視の作業が始まる。「これにより、組織は、ミッションおよびビジネスニーズ、脅威、脆弱性、技術が変化する極めて動的な運用環境においても、システムおよび共通管理策の認可を維持することができる。レポートやダッシュボードを通じてセキュリティおよびプライバシー情報に継続的にアクセスできることで、組織の責任者は、継続的な認可の判断を含む、効果的かつタイムリーなリスク管理上の意思決定を行うことができる」[SP 800-53r5]。

活動例：

1. **管理：**ステークホルダーは識別されたリスク対応策を実施し、該当する場合はそれらの対応策をより広範なERMプロセスに組み込む。CSRM／ERM／人材戦略は、成功を収めるために継続的に監視、評価、適応される。ステークホルダーチームは、リスクへの対応がどの程度効果的に行われているかを定期的に評価するため、継続的な連携に向けた計画およびプロセスを策定する。
2. **評価：**優先分野で活動するステークホルダーチーム間の定期的な状況確認を含め、計画された対策がリスクにどの程度効果的に対処したかを評価するプロセスを確立する。対策が所定の期間実施された後に、リスクの再評価を検討する。リスクレジスタが更新されていることを確認し、該当する場合はサイバーセキュリティリスクをより広範なERMポートフォリオに組み込む（リスクポートフォリオに関する議論については、NIST IR 8286r1 を参照）。 組織の財務・経理担当者が関与することが望ましい。評価が事業体レベルで行われる場合は、監査委員会も関与することがある。これには、統制と権限が事業体全体で一貫して維持され、分断されていないことを検証することも含まれる。
3. **調整：**ステークホルダーが、選択した人材対策およびその他のリスク対策を評価し、組織に対するリスクが適切に解消されたかどうかを判断した後、次の行動は、必要に応じて調整することである。契約の締結、一時的な人員増強、スキルアップ、再教育、役割または責任の再割り当てといった追加の人材対応策や、リスク対応策の調整が必要となる場合がある。

CSRM、ERM、および人材戦略の継続的モニタリング。

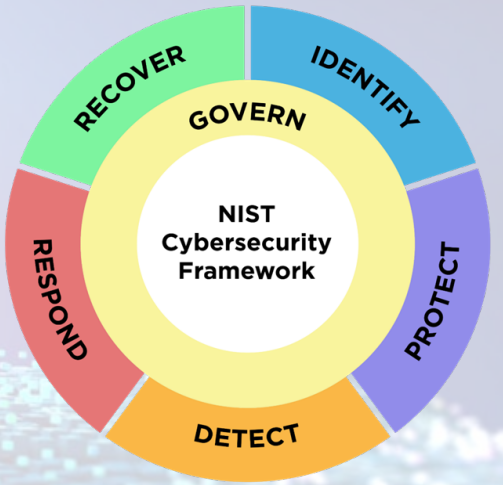


「管理、評価、調整（*MEA*）」ライフサイクルについて詳しく知るにはこちらへ *NIST IR 8286Cr1*

ADDITIONAL RESOURCES

Additional Resources

- **Understanding the Cybersecurity Framework:** Other quick-start guides focused on small businesses, cybersecurity supply chain risk management, ERM, and other subjects are available on the CSF 2.0 Resource Center.
- **Risk identification, analysis, and prioritization:**
  - IR 8286Ar1 provides comprehensive information on risk registers and more granular risk detail records.
  - SP 800-30r1, SP 800-221, and SP 800-221A discuss risk assessments and the integration of information and communications technology into ERM processes.
  - The NIST Risk Management Framework provides a comprehensive process for managing information security and privacy risks at the system level.
- **Workforce assessment and best practices:** The NICE Framework Resource Center provides additional formats for the NICE Framework, in-depth cybersecurity workforce development resources, and information about cybersecurity workforce partnerships, such as the RAMPS communities. Organizations can receive assistance with NICE Framework implementation by emailing NICEframework@nist.gov.
  - Crosswalk for the CSF 2.0 and NICE Framework helps organizations identify priority Work Roles (Note: several Work Roles may map to each CSF Subcategory).
  - NICE Framework Components supports identification of priority Work Roles and relevant Tasks, Knowledge, and Skills to target in training and recruitment.
  - Building a Cybersecurity and Privacy Learning Program helps organizations create or mature an organizational learning program in support of an informed and capable cybersecurity and privacy workforce.
  - The NIST Cybersecurity Career Ambassador Program seeks to create a network of employers, educators, and others who serve as champions to prepare, grow, and sustain a skilled cybersecurity workforce.
  - The NIST Small Business Cybersecurity Corner provides resources specifically tailored to small businesses.



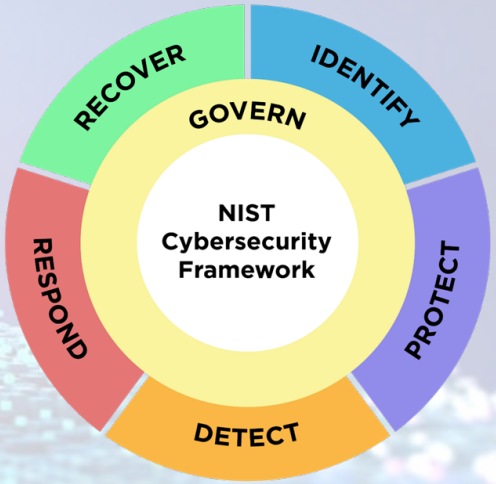
Glossary of Acronyms

- **BIA:** Business Impact Analysis
- **CSRM:** Cybersecurity Risk Management
- **CSF:** Cybersecurity Framework
- **ERM:** Enterprise Risk Management
- **QSG:** Quick-Start Guide
- **TKS:** Task, Knowledge, and Skill

追加リソース

追加リソース

- **サイバーセキュリティフレームワークの理解：**小規模事業者、サイバーセキュリティサプライチェーンリスクマネジメント、ERM、およびその他のテーマに焦点を当てたその他のクイックスタートガイドは、CSF 2.0 リソースセンターで入手可能である。
- **リスクの識別、分析、および優先順位付け：**
  - IR 8286Ar1は、リスクレジスタおよびより詳細なリスク詳細記録に関する包括的な情報を提供している。
  - SP 800-30r1、SP 800-221、およびSP 800-221Aは、リスクアセスメントおよび情報通信技術（ICT）のERMプロセスへの統合について論じている。
  - NIST リスクマネジメントフレームワークは、システムレベルにおける情報セキュリティおよびプライバシーリスクを管理するための包括的なプロセスを提供している。
- **人材評価およびベストプラクティス：**NICEフレームワーク リソースセンターでは、NICEフレームワークの追加フォーマット、サイバーセキュリティ人材育成に関する詳細なリソース、およびRAMPSコミュニティなどのサイバーセキュリティ人材パートナーシップに関する情報を提供している。組織は、NICEframework@nist.gov 宛てにメールを送信することで、NICEフレームワークの導入に関する支援を受けることができる。
  - CSF 2.0とNICEフレームワークの対応表は、組織が優先すべき職務上の役割を識別するのに役立つ（注：各CSFサブカテゴリには複数の職務上の役割が対応する場合がある）。
  - NICEフレームワークのコンポーネントは、優先すべき職務上の役割ならびにトレーニングおよび採用において重点を置くべき関連するタスク、知識、およびスキルの識別を支援する。
  - サイバーセキュリティおよびプライバシー学習プログラムの構築は、組織が、十分な知識と能力を備えたサイバーセキュリティおよびプライバシー担当人材を支援するための組織的な学習プログラムを構築または成熟させるのに役立つ。
  - NISTサイバーセキュリティキャリアアンバサダープログラムは、熟練したサイバーセキュリティ人材を育成・拡大・維持するための推進役となる雇用主、教育者、その他の関係者によるネットワークの構築を目指している。
  - NIST小規模事業者向けサイバーセキュリティコーナーは、小規模事業者向けに特化したリソースを提供している。



略語集

- **BIA：**ビジネスインパクト分析
- **CSRM：**サイバーセキュリティリスクマネジメント
- **CSF：**サイバーセキュリティフレームワーク
- **ERM：**事業体リスクマネジメント
- **QSG：**クイックスタートガイド
- **TKS：**タスク、知識、スキル