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

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

U.S. Department of Commerce
Gina M. Raimondo, Secretary
National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

NIST Special Publication
NIST SP 1303
https://doi.org/10.6028/NIST.SP.1303
Please send your comments to cyberframework@nist.gov.
October 2024

NIST 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:
事業体リスクマネジメント クイックスタートガイド

U.S. Department of Commerce
Gina M. Raimondo, Secretary
National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

NIST Special Publication
NIST SP 1303
https://doi.org/10.6028/NIST.SP.1303
コメントは cyberframework@nist.gov まで送付のこと
2024年10月

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

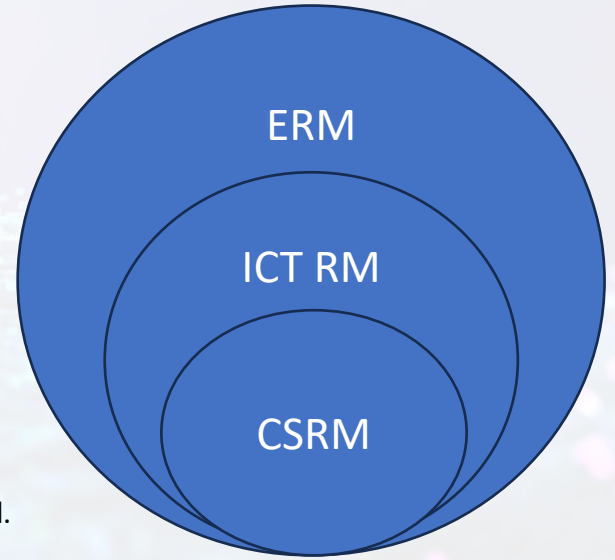
This guide provides an introduction to using the NIST Cybersecurity Framework (CSF) 2.0 for planning and integrating an enterprise-wide process for cybersecurity risk management information, as a subset of information and communications technology risk management, into enterprise risk management. The use of CSF common language and outcomes supports the integration of risk monitoring, evaluation, and adjustment across various organizational units and programs.

Enterprise Risk Management (ERM)

When we use the word *enterprise* in an organizational context, we mean all aspects of that organization, spanning the entire breadth and depth of that org chart. ERM exists at the top level of the organizational hierarchy and spans risk considerations such as mission, financial, reputation, and technical risks thereof. ERM calls for understanding the core risks that an enterprise faces, determining how best to address those risks, and ensuring that the necessary actions are taken. An ERM program allows enterprises to aggregate, prioritize, and analyze risks from across the enterprise in a common risk register format. **Risk appetite** expressed by the ERM program helps inform **risk identification**.

Information and Communications Technology (ICT) Risk Management

The information and communications technology (ICT) on which an enterprise relies is managed through a broad set of risk disciplines that include privacy, supply chain, and cybersecurity. ICT extends beyond traditional information technology (IT) considerations. Many entities rely on operational technology (OT) and Internet of Things (IoT) devices' sensors or actuators for bridging physical and digital environments. Increasingly, artificial intelligence (AI) factors into enterprise risk. NIST SPs 800-221 and 800-221A provide more information.



Cybersecurity Risk Management (CSRM)

Cybersecurity risks are a fundamental type of risk for all organizations to manage. Potential negative impacts to organizations from cybersecurity risks include higher costs, lower revenue, reputational damage, and the impairment of innovation. Cybersecurity risks also threaten individuals' privacy and access to essential services and can result in life-or-death consequences. Risk appetite expressed at other levels of risk management gets translated into more specific CSRM **risk tolerance**, such that cyber risks can be more easily identified.

CSF 2.0 provides guidance for reducing cybersecurity risks by helping organizations discuss, organize, and address gaps in their **cybersecurity program** in a standard way. The cybersecurity outcomes described in CSF affect cybersecurity, ICT, and enterprise risks. Understanding these dependencies is an essential activity in CSRM, ICT RM, and ERM. The Cybersecurity Risk Register (CSRR) described in the NIST IR 8286 series of publications enables organizations to identify, manage, and monitor the relationships between discrete risks and aspects of a CSF-based cybersecurity program that address those risks. The CSRR allows organizations to identify, organize, analyze, and report on cybersecurity risks at the system level. CSF Organizational Profiles are a natural byproduct of a comprehensive CSRR, because the relative priority of CSF outcomes becomes apparent based on how significant the impacts of identified cybersecurity risks might be to the organization's priorities, such as its strategic objectives, products and services, or customers.

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

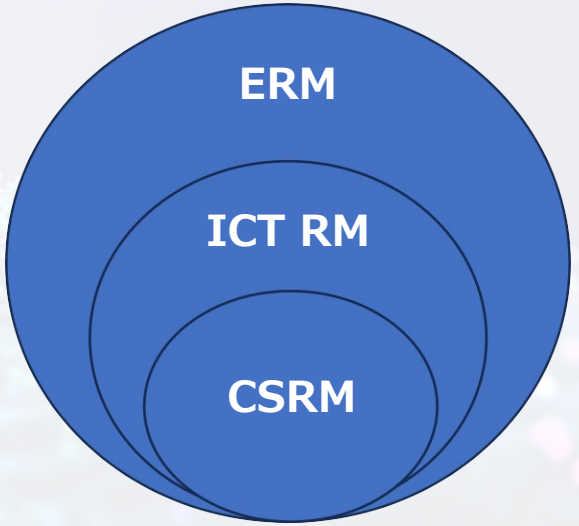
本ガイドでは、サイバーセキュリティリスクマネジメント情報のための事業体全体のプロセスを、情報通信技術リスクマネジメントのサブセットとして計画し、事業体リスクマネジメントに統合するための NIST サイバーセキュリティ フレームワーク (CSF) 2.0 の使用方法について紹介する。CSFの共通言語及び成果の使用が、様々な組織単位及びプログラムにわたるリスクの監視、評価、及び調整の統合を支援している。

事業体リスクマネジメント (ERM)

事業体という言葉を組織の文脈で使う場合、組織図の広がりから深さ全体に及ぶ、組織のあらゆる側面を意味している。ERMは、組織階層の最上位レベルに存在し、ミッション、財務、評判、及び技術的リスクなどのリスク考慮事項に及ぶ。ERMは、事業体が直面する中核的なリスクを理解し、それらのリスクに対処する最善の方法を決定し、必要な行動を確実に実行することを求めている。ERMプログラムにより、事業体は共通のリスクレジスタのフォーマットで、事業体全体のリスクを集約し、優先順を付け、分析することができる。ERMプログラムによって示された**リスク選好度**は、**リスクの識別**に情報を与えるのに役立つ。

情報通信技術 (ICT) リスクマネジメント

事業体が依存している情報通信技術 (ICT) は、プライバシー、サプライチェーン、及びサイバーセキュリティを含む広範な一連のリスク領域を通じて管理される。ICTは、従来の情報技術 (IT) の考慮事項を超えている。多くの事業体は、物理環境及びデジタル環境の橋渡しをするために、制御・運用技術 (OT) 及びモノのインターネット (IoT) デバイスのセンサ又はアクチュエータに依存している。人工知能 (AI) が事業体リスクの要因となることも増えている。NIST SP 800-221 及び NIST SP 800-221A に詳細が記載されている。



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、すべての組織にとって管理すべき基本的な種類のリスクである。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悪影響には、コスト増、収益源、風評被害、及びイノベーションの阻害が含まれる。サイバーセキュリティリスクはまた、個人のプライバシー及び重要なサービスへのアクセスを脅かし、生死に関わる結果をもたらす可能性がある。リスクマネジメントの他のレベルで表明されたリスク選好度は、サイバーリスクをより容易に識別できるように、より具体的なCSRMの**リスク許容度**に変換される。

CSF 2.0は、組織が**サイバーセキュリティプログラム**のギャップを標準的な方法で議論、整理、及び対処できるようにすることで、サイバーセキュリティリスクを軽減するためのガイダンスを提供している。CSFに記述されたサイバーセキュリティの成果は、サイバーセキュリティ、ICT、及び事業体に影響する。これらの依存関係を理解することは、CSRM、ICT RM、及びERMにおける不可欠な活動である。NIST IR 8286シリーズに記載されているサイバーセキュリティリスクレジスタ（CSRR）は、組織が個別のリスクと、それらのリスクに対処するCSFベースのサイバーセキュリティプログラムの側面との関係を識別し、管理し、監視することを可能にする。CSRRを使用すると、組織がシステムレベルでサイバーセキュリティリスクを識別し、整理し、分析し、報告できる。CSF 組織プロファイルは、包括的なCSSRの副産物である。これは、識別されたサイバーセキュリティリスクのインパクトが、組織の戦略的目標、製品及びサービス、又は顧客などの組織の優先事項に対してどの程度重要であるかに基づいて、CSFの成果の相対的な優先順位が明らかになるからである。

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

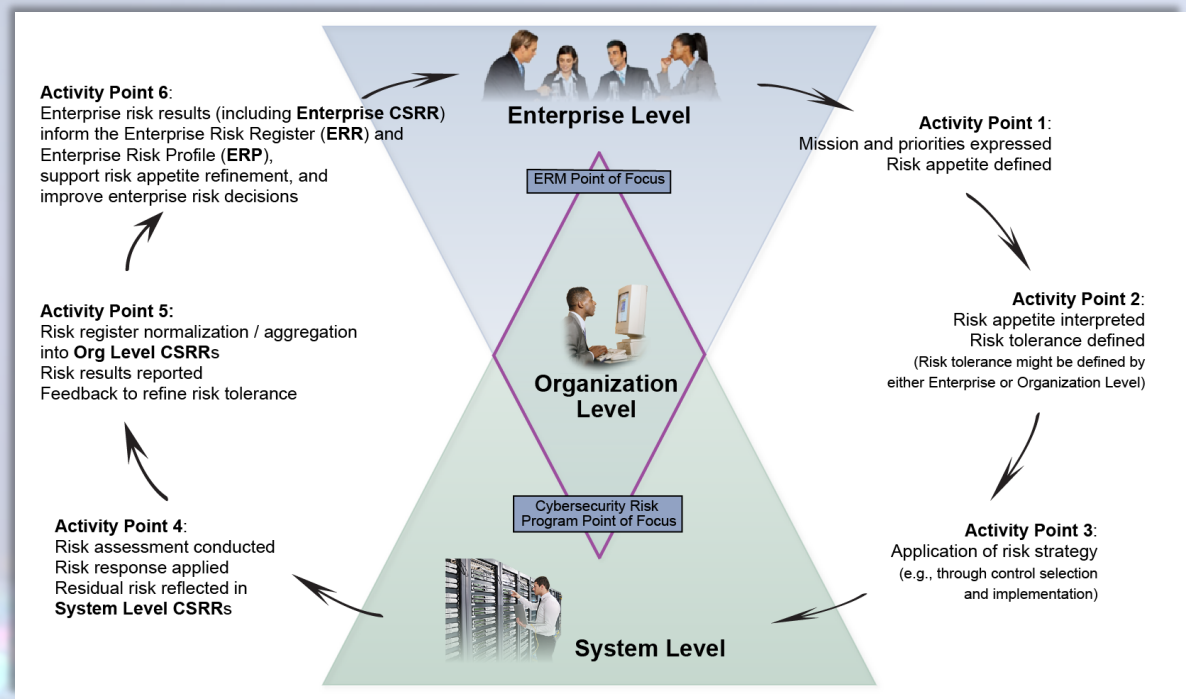


Illustration of enterprise risk management integration and coordination from NIST SP 800-221

CSF 2.0, as part of a holistic ERM approach, helps ensure that leaders continually have the information they need for making informed business/agency decisions.

CSF 2.0 Supports Six Activity Points For Informing, Implementing, and Monitoring ERM

CSF 2.0 is a valuable guide for helping to review and improve security and privacy considerations as part of a holistic enterprise risk approach. CSF is most helpful when it is paired with other ERM elements. For example, as agency officials and corporate boards provide oversight of all relevant risks, the CSF process helps ensure that cybersecurity strategy is well-executed. Managers plan and implement risk treatment based on that strategy, record and report progress, and provide agency/business leaders with information needed for effective operations and mission success.

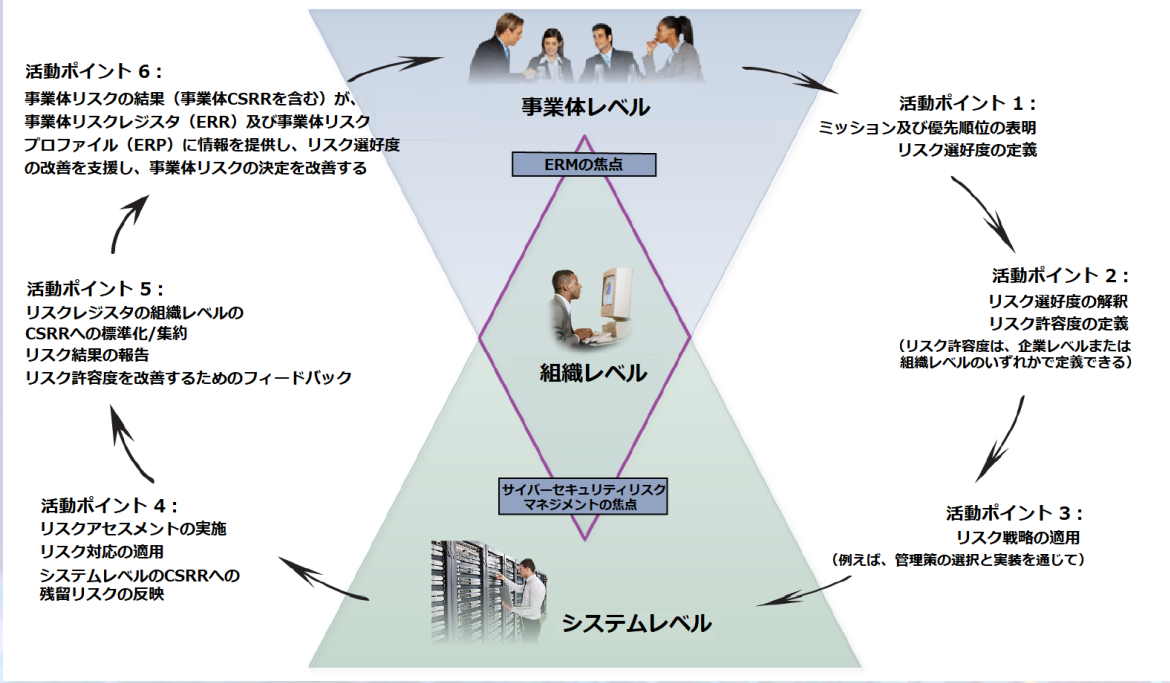
The **Activity Points**, which are further described in subsequent pages, include:

- 1 – Leaders **define and record** enterprise mission, priorities, and risk appetite. **Accountability** is assigned for managing both **positive and negative types of risk**. (GV.OC, GV.RM, GV.SC)
- 2 – Organization-level managers interpret **risk appetite** into specific guidance regarding security and privacy requirements, and associated **risk tolerance**. (GV.RR, GV.PO, ID.RA)
- 3 – **Risk strategy and requirements** aid implementation of shared security solutions and system-level controls to achieve an acceptable level of risk. (PROTECT, DETECT, RESPOND, and RECOVER)
- 4 – Risk response outcomes are reflected as residual risk in **system-level risk registers** as part of **ongoing assessment** and **continuous monitoring** activities. (ID.RA, ID.IM, GV.OV)
- 5 – **Risk registers are normalized and aggregated** at the organizational unit level, supporting reporting, analysis, and organization-level adjustment. (ID.IM, GV.OV)
- 6 – Combined risk results from the enterprise are used to maintain an **enterprise-level risk register and risk profile**, supporting enterprise business decisions and any **adjustments** needed for the risk strategy. (GV.PO, GV.OV)

Supporting Resources:

- SP 800-221, *Enterprise Impact of Information and Communications Technology Risk: Governing and Managing ICT Risk Programs Within an Enterprise Risk Portfolio*
- SP 800-221A, *Information and Communications Technology (ICT) Risk Outcomes: Integrating ICT Risk Management Programs with the Enterprise Risk Portfolio*

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



NIST SP 800-221 の事業体リスクマネジメントの統合及び連携の図

CSF 2.0は、全体的なERMアプローチの一部として、リーダーが、情報に基づいたビジネス/政府機関の意思決定に必要な情報を、継続的に入手できることを確実にするのに役立つ。

CSF 2.0 は、ERMの通知、実装、及び監視のための6つの活動ポイントをサポートしている。

CSF 2.0は、全体的な事業体リスクアプローチの一環として、セキュリティ及びプライバシーの考慮事項をレビューし、改善するのに役立つ貴重なガイドである。CSFは、他のERM要素と組み合わせる際にも役立つ。 例えば、政府機関の職員及び企業の取締役会は、関連するすべてのリスクを監督するため、CSFプロセスはサイバーセキュリティ戦略が適切に実行されることを確実にするのに役立つ。マネージャーは、その戦略に基づいてリスク対応を計画及び実装し、政府機関/ビジネスリーダーに効果的な運用及びミッションの成功に必要な情報を提供する。

活動ポイントには、以下のものが含まれる。詳細については、以降のページで説明する。

- 1 – リーダーが、事業体のミッション、優先順位、及びリスク選好度を**定義し、記録する。説明責任**が、**正のリスク及び負のリスク**両方を管理するために、割り当てられる。(GV.OC, GV.RM, GV.SC)
- 2 – 組織レベルのマネージャーが、**リスク選好度**を、セキュリティ及びプライバシーの要件、並びに**リスク許容度**に関する具体的なガイダンスに解釈する。(GV.RR, GV.PO, ID.RA)
- 3 – **リスク戦略及び要件**が、 受容可能なリスクレベルを達成するための共有セキュリティソリューション及びシステムレベルの管理策の実装を支援する。(「防御」、「検知」、「対応」、「復旧」)
- 4 – リスク対応の成果が、**継続的なアセスメント**及び**継続的な監視**の一環として、**システムレベルのリスクレジスタ**に残留リスクとして反映される。(ID.RA, ID.IM, GV.OV)
- 5 – **リスクレジスタ**が組織単位レベルで**標準化**され、**集計**され、報告、分析、及び組織レベルの調整を支援する。 (ID.IM, GV.OV)
- 6 – 事業体の統合されたリスク結果が、**事業体レベルのリスクレジスタ及びリスクプロファイル**を維持するために使用され、事業体のビジネス上の意思決定及びリスク戦略に必要なあらゆる**調整**を支援する。 (GV.PO, GV.OV)

サポートリソース

- SP 800-221, *Enterprise Impact of Information and Communications Technology Risk: Governing and Managing ICT Risk Programs Within an Enterprise Risk Portfolio*
- SP 800-221A, *Information and Communications Technology (ICT) Risk Outcomes: Integrating ICT Risk Management Programs with the Enterprise Risk Portfolio*

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

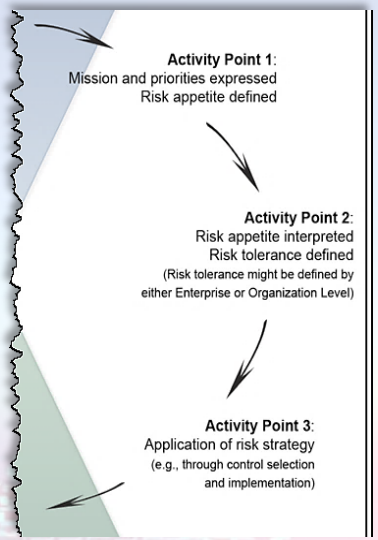
Aligning enterprise priorities with strategic activity

As senior leaders and organizational managers observe and discuss **risk management strategy** (to take advantage of opportunities and to avoid known threats), they develop a plan for managing risk to the optimal level.

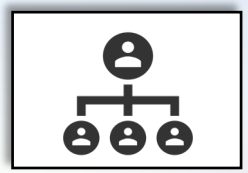
The outcomes in the CSF Govern Function (GV) specifically drive **actionable planning** about how to best manage various enterprise risks to ICT, including privacy, supply chain, AI, IoT, and OT on which the entity depends.

Beginning with an understanding of what information and technology are most important to the **enterprise mission**, leaders define **acceptable levels of risk** for those assets and describe how personnel in various work roles will be **accountable** for risk management success. (ID.AM, ID.RA)

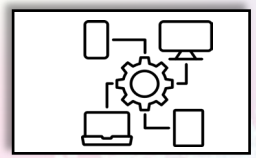
This actionable and proactive strategizing also makes clear to customers and other stakeholders that effective risk management is a priority, that clear and accountable plans are in place to achieve that management, and that monitoring processes are continually identifying opportunities for improvement. These plans specifically apply the outcomes described in the CSF Organizational Profile(s), in particular the PROTECT, DETECT, RESPOND, and RECOVER functions.



Based on internal and external organizational context, leaders use governance systems to set risk priorities, risk appetite, and risk strategy. This understanding sets the tone for how the enterprise conducts, measures, and reports risk management activities and performance. Actions include processes for aligning priorities and risk direction for business partners and other members of the organization's cybersecurity supply chain.



Understanding of objectives and risk appetite enables managers to interpret how to apply those for their organizational units (OUs). Managers create risk tolerance statements and metrics, defining a "target state" that will achieve stakeholder objectives such as through secure shared infrastructure (e.g., organizationally-tailored control baselines, common controls, and monitoring strategy).



The direction from leadership and OU management is applied in an operational context, supporting system-level risk assessment, requirements definition, and allocation. These enable effective categorization, control selection/implementation, and ongoing system-level authorization/monitoring.

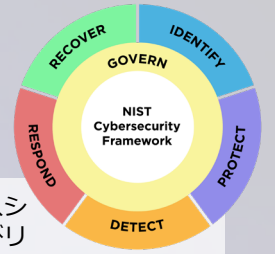
Questions to Consider

- ? **Activity Point 1**: Where do you draw the mission and strategic priorities of the organization from?
  Do you have a process for defining and expressing risk appetite?
- ? **Activity Point 2**: How is risk appetite translated into risk tolerance?
  Are cybersecurity risk management strategy outcomes reviewed to inform and adjust strategy and direction?
- ? **Activity Point 3**: How are organizational priorities, definition of acceptable risk, and performance requirements embedded in your system-level risk activities?
  Are these translated into control selection, system constraints, reporting requirements, and anomaly detection?

Related Resources

- NIST Risk Management Framework (RMF) for Information System and Organizations - a comprehensive, flexible, repeatable, and measurable process to manage information security and privacy risk
- NIST IR 8286 series – specifically NIST IR 8286A - Identifying and Estimating Cybersecurity Risk for ERM
- NIST SP 800-30 Rev. 1 – *Guide for Conducting Risk Assessments*

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



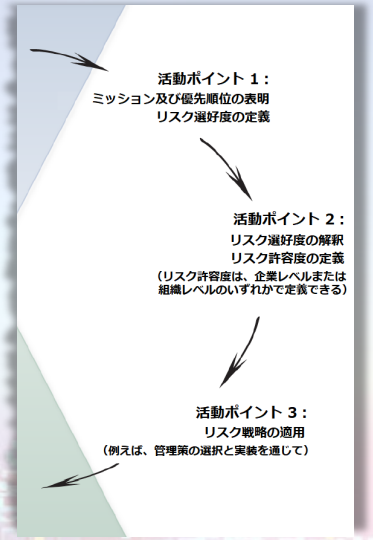
事業体の優先事項と戦略的活動を一致させる

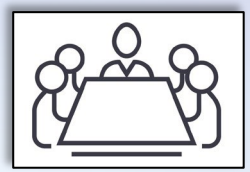
シニアリーダー及び組織マネージャーは、（機会を活用し、既知の脅威を回避するために）**リスクマネジメント戦略**を観察し、議論しながら、最適なレベルまでリスクを管理するための計画を策定する。

CSFの「統治」機能（GV）の成果は、特に、事業体が依存するプライバシー、サプライチェーン、AI、IoT、及びOTを含むICTに対する様々な事業体リスクを最適に管理する方法について、**実行可能な計画**を推進する。

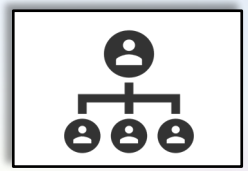
事業体のミッションにとって最も重要な情報及び技術が何かを理解することから始め、リーダーはそれらの資産に対する**受容可能なリスクのレベル**を定義し、様々な職務の要員がリスクマネジメントの成功に対してどのように**責任を負う**かを説明する。(ID.AM, ID.RA)

また、この実行可能で積極的な戦略策定により、効果的なリスクマネジメントが優先事項であること、そのマネジメントを達成するための明確で説明責任のある計画が策定されていること、及び監視プロセスが継続的に改善の機会を識別していることが、顧客及びその他のステークホルダーに明確に示される。これらの計画は、特に「防御」、「検知」、「対応」及び「復旧」機能において、 CSF 組織プロファイル に記載されている成果を具体的に適用するものである。

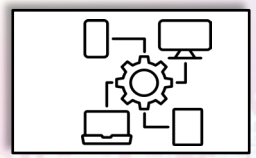




組織の内部及び外部の状況に基づき、リーダーはガバナンスシステムを使用して、リスクの優先順位、リスク選好度、及びリスク戦略を設定する。この理解は、事業体がどのようにリスクマネジメント活動及びパフォーマンスを実施し、測定し、報告するかの基調を定める。行動には、ビジネスパートナー及び組織のサイバーセキュリティサプライチェーンの他のメンバーの優先順およびリスクの方向性を一致させるプロセスが含まれる。



目的及びリスク選好度を理解することで、マネージャーはそれらを組織単位（OU）に適用する方法を解釈できる。マネージャーは、リスク許容度のステートメント及び指標を作成し、セキュアな共有インフラなど（例えば、組織的にテーラリングされた管理策ベースライン、共通管理策、監視戦略）を通じて、ステークホルダーの目的を達成する「目標状態」を定義する。



リーダーシップ及びOUマネジメントからの指示は、システムレベルのリスクアセスメント、要件定義、及び割り振りをサポートする運用のコンテキストに適用される。これらにより、効果的な分類、管理策の選択/実装、及び継続的なシステムレベルの認可/監視が可能になる。

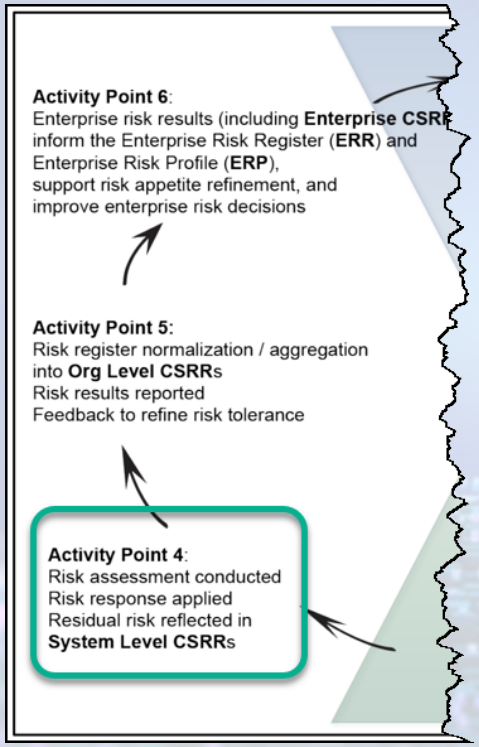
検討すべき質問

- ? **活動ポイント 1：**組織のミッション及び戦略的優先事項はどこから導き出しているか？
  リスク選好度を定義し、表現するためのプロセスはあるか？
- ? **活動ポイント 2：**リスク選好度はどのようにリスク許容度に変換されるのか？
  サイバーセキュリティリスクマネジメント戦略の成果は、戦略及び方向性を通知し、調整するためにレビューされているか？
- ? **活動ポイント 3：**組織の優先事項、受容可能なリスクの定義、及びパフォーマンス要件は、システムレベルのリスク活動にどのように組み込まれているか？
  これらは、管理策の選択、システムの制約、報告要件、及び異常検知に変換されているか？

関連リソース

- NIST Risk Management Framework (RMF) for Information System and Organizations – 情報セキュリティリスク及びプライバシーリスクを管理するための、包括的で、柔軟で、反復可能で、測定可能なプロセス。
- NIST IR 8286 series – 特に、NIST IR 8286A - Identifying and Estimating Cybersecurity Risk for ERM
- NIST SP 800-30 Rev. 1 – *Guide for Conducting Risk Assessments*

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



Risk Assessment, Risk Treatment, and Information Sharing Ensure Value and Risk Optimization

Select Risk Response

After selecting and implementing controls and other methods of risk treatment, system-level personnel assess the effectiveness and efficiency of that treatment (e.g., through the Assess step of the NIST Risk Management Framework). Risk managers evaluate threats and opportunities, in alignment with risk strategy and direction from enterprise- and organization-level guidance. They determine the benefits of the following responses: Mitigate, Accept, Avoid, and Transfer for negative risks; Realize, Share, Enhance, and Accept for positive risks.

Analyze and Prioritize Risks

There are benefits to both qualitative and quantitative risk analysis methodologies and even the use of multiple methodologies, based on enterprise strategy, organization preference, and data availability (ID.RA). The relative priority of various types of risk must be decided upon by those with appropriate authority, usually through guidance provided through the risk management strategy (GV.RM).

Communicate Risk Findings and Decisions

The cybersecurity risk register (CSRR) provides a location to record and communicate the known system-level threats and vulnerabilities, their impact on business objectives, and the responses taken or planned. Risk managers share information about residual risk, including metrics that support ongoing assessment and authorization, and plans of actions & milestones for maintaining the appropriate level of risk based on stakeholders' expectations (as expressed in the target state of the Organizational Profiles, especially the GOVERN and IDENTIFY functions).

Notional Cybersecurity Risk Register

ID	Priority	Risk Description	Risk Category	Current Assessment			Risk Response Type	Risk Response Cost	Risk Response Description	Risk Owner	Status
				Likelihood	Impact	Exposure Rating					
1											
2											
3											
4											
5											

Continually Communicate, Learn, and Update

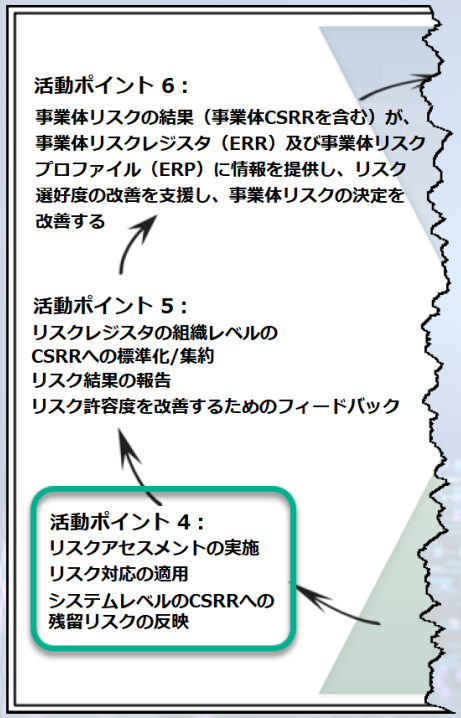
Questions to Consider

- ? How do CSF Target Profile outcomes (organizational agreement on how to best protect, detect, respond, and recover) inform system-specific risk assessment and treatment?
- ? How can we estimate likelihood and impact of those risks given the planned outcomes and knowledge from previous results?
- ? Is our risk response proportionate to the exposure?

Related Resources

- SP 800-221, *Enterprise Impact of Information and Communications Technology Risk: Governing and Managing ICT Risk Programs Within an Enterprise Risk Portfolio*
- NIST IR 8286A, *Identifying and Estimating Cybersecurity Risk for Enterprise Risk Management*
- **Risk Detail Schema** **Risk Detail** **CSRR Schema**

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



リスクアセスメント、リスク対応、及び情報共有が、価値とリスクの最適化を確実にする。

リスク対応を選択する

システムレベルの人員は、管理策及びその他のリスク対応の方法を選択し、実装した後、その対応の有効性及び効率性をアセスメントする（例えば、NISTのリスクマネジメントフレームワークのアセスメントステップを通じて）。リスク管理者は、事業体レベル及び組織レベルのガイダンスからのリスク戦略及び方向性に沿って、脅威及び機会を評価する。リスク管理者は、次の対応の利点を判断する：負のリスクの軽減（Mitigate）、受容（Accept）、回避（Avoid）、転嫁（Transfer）；正のリスクの活用（Realize）、共有（Share）、強化（Enhance）、受容（Accept）。

リスクを分析し、優先順位を付ける

事業体の戦略、組織の優先傾向、及びデータの可用性に基づいて、定性的及び定量的リスク分析手法、さらには複数の手法の使用にも利点がある（ID.RA）。様々な種類のリスクの相対的な優先順位は、通常、リスクマネジメント戦略（GV.RM）を通じて提供されるガイダンスを通じて、適切な権限を持つ者によって決定されなければならない。

リスクの発見と決定を伝達する

サイバーセキュリティリスクレジスタ（CSRR）は、既知のシステムレベルの脅威と脆弱性、ビジネス目的へのインパクト、及び実施又は計画された対応を記録し、伝達するための場所を提供する。リスク管理者は、継続的なアセスメント及び認可を支援する指標、及びステークホルダーの期待（組織プロファイルの目標の状態、特に「統治」と「識別」機能に示されている）に基づいて適切なリスクレベルを維持するための行動計画及びマイルストーンなど、残留リスクに関する情報を共有する。

概念的なサイバーセキュリティリスクレジスタ

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	ステータス
				起こりやすさ	インパクト	曝露の評価					
1											
2											
3											
4											
5											

継続的にコミュニケーションし、学び、更新する

検討すべき質問

- ? CSF 目標プロファイルの成果（最適な防御、検知、対応、及び復旧方法に関する組織的な合意）は、システム固有のリスクアセスメント及び対応に、どのように情報を提供するか？
- ? 計画された成果及び過去の結果から得られた知見を前提として、これらのリスクの起こりやすさとインパクトをどのように推定できるか？
- ? リスク対応は、曝露（エクスポージャー）に比例しているか？

関連リソース

- SP 800-221, *Enterprise Impact of Information and Communications Technology Risk: Governing and Managing ICT Risk Programs Within an Enterprise Risk Portfolio*
- NIST IR 8286A, *Identifying and Estimating Cybersecurity Risk for Enterprise Risk Management*
- **Risk Detail Schema** **Risk Detail** **CSRR Schema**

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

CSF outcomes (e.g., planned and current) support a Monitor-Evaluate-Adjust (MEA) cycle for achieving ERM objectives.

As risk management is applied through various controls (as described above), the results are continually evaluated for effectiveness. CSF provides examples of how to do this through CSF Informative References, described at the Online Informative References (OLIR) web site.

At the organization level, the results of various system-level activities and results (as reflected in CSRRs) are aggregated and normalized. Managers monitor how well the cyber risk strategy is being implemented, evaluate indicators to confirm performance goals and highlight potential changes in the risk landscape, and then make any adjustments necessary to accentuate achievement of opportunities (positive risk) and reduce impactful threat conditions to an acceptable level.

This cycle enables creation and maintenance of an organization-level CSRR, and updates to the Organizational Profiles to reflect refined current state and adjusted Target State.

MONITOR

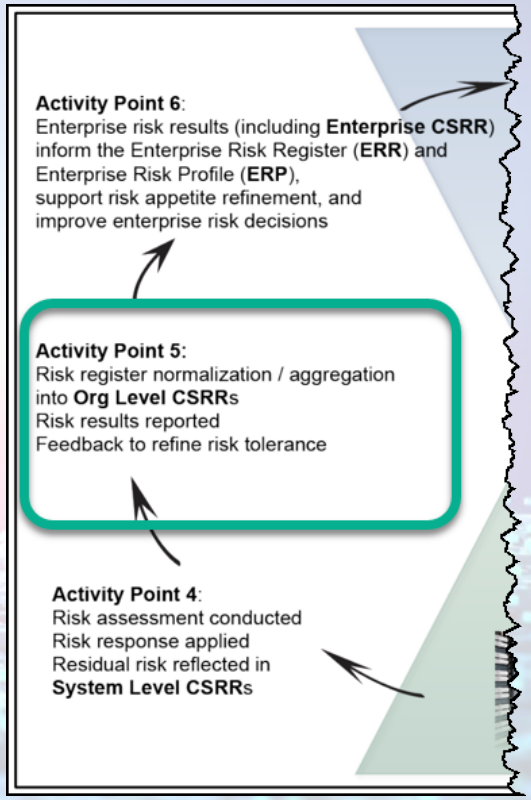
- Measure *whether* controls are still implemented and effective
- Measure the *extent to which* controls are implemented without impairing organizational operations and efficiency

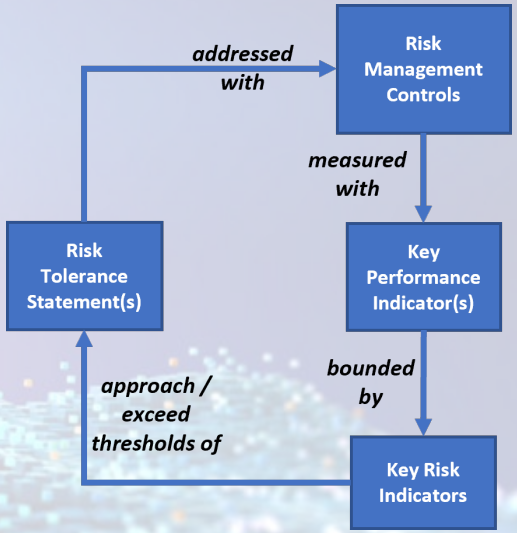
EVALUATE

- Assess if organizational controls are achieving the desired risk results
- Assess if risk management activities are keeping risk within tolerance (e.g., evaluating key risks and key performance indicators)
- Compare current outcomes to the target state described in Organizational Profiles

ADJUST

- Implement additional controls and enhancement as needed
- Implement alternative controls to enhance opportunity





Monitor-Evaluate-Adjust Cycle (from NIST SP 800-221)

Risk registers are aggregated, normalized, and shared based on enterprise-defined risk categories and measurement criteria. Risk tolerance statements are refined, if needed, to ensure balance among ICT value, organizational resources, and optimal risk.

Supporting Resources

- NIST IR 8286C, *Staging Cybersecurity Risks for ERM and Governance Oversight*

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

（例えば、計画された、及び現在の）CSFの成果は、ERMの目的を達成するための監視-評価-調整（MEA）のサイクルを支援する

リスクマネジメントは、上述のように様々な管理策を通じて適用されるので、その結果は有効性について継続的に評価される。Online Informative References (OLIR) ウェブサイトに記載されている参考情報を通じて、CSFを行う例を提供している。

組織レベルでは、様々なシステムレベルの活動及び（CSSRに反映されているとおりの）結果が集約され、標準化される。マネージャーはサイバーリスク戦略がどの程度実装されているかを監視し、パフォーマンス目標を確認するために指標を評価し、リスク状況における潜在的な変化を強調し、機会（正のリスク）の達成を強調し、インパクトの強い脅威の状況を受容可能なレベルにまで軽減するために必要な調整を行う。

このサイクルにより、組織レベルのCSSRの作成及び維持が可能となり、また、「組織プロファイル」を更新して、精緻化された現状及び調整された目標状態を反映できる。

監視する

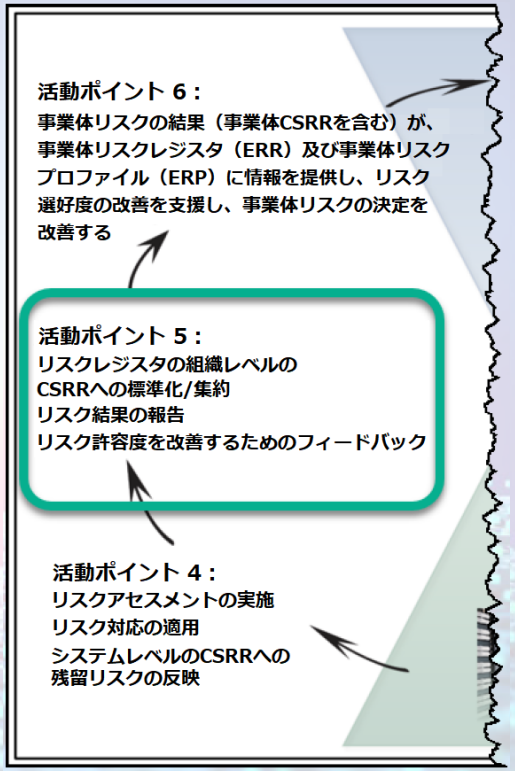
- 管理策が依然として実装され、有効であるかを測定する。
- 組織の運用及び効率性を損なうことなく、管理策がどの程度実装されているかを測定する。

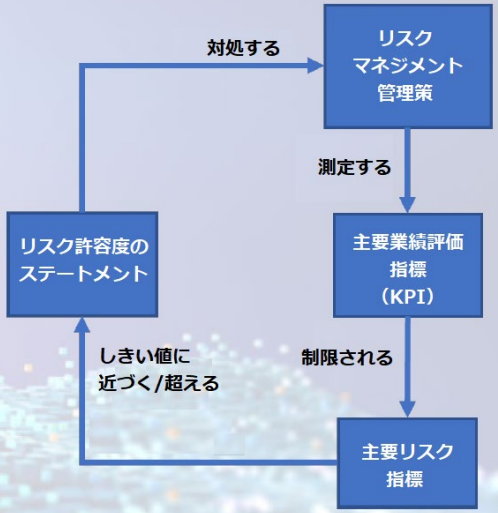
評価する

- 組織の管理策が望ましいリスクの結果を達成しているかどうかをアセスメントする。
- リスクマネジメント活動がリスクを許容度内に維持しているかどうかをアセスメントする（例えば、主要リスク及び主要業績評価指標（KPI）の評価）。
- 現在の成果を「組織プロファイル」に記載された目標状態と比較する。

調整する

- 必要に応じて、追加の管理策及び拡張管理策を実装する。
- 機会を強化するための代替管理策を実装する。





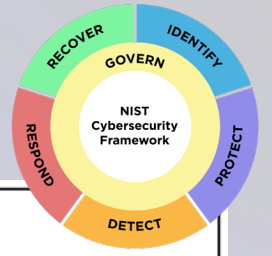
監視-評価-調整のサイクル（NIST SP 800-221より）

リスクレジスタは、事業体が定義したリスクカテゴリー及び測定基準に基づいて集約され、標準化され、共有される。リスク許容度は、ICTの価値、組織のリソース、及び最適なリスクのバランスを確実にするために、必要に応じて精緻化される。

サポートリソース

- NIST IR 8286C, *Staging Cybersecurity Risks for ERM and Governance Oversight*

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



Feedback from CSF Informative References and the MEA cycle help monitor and adjust risk response, appetite/tolerance, and policy.

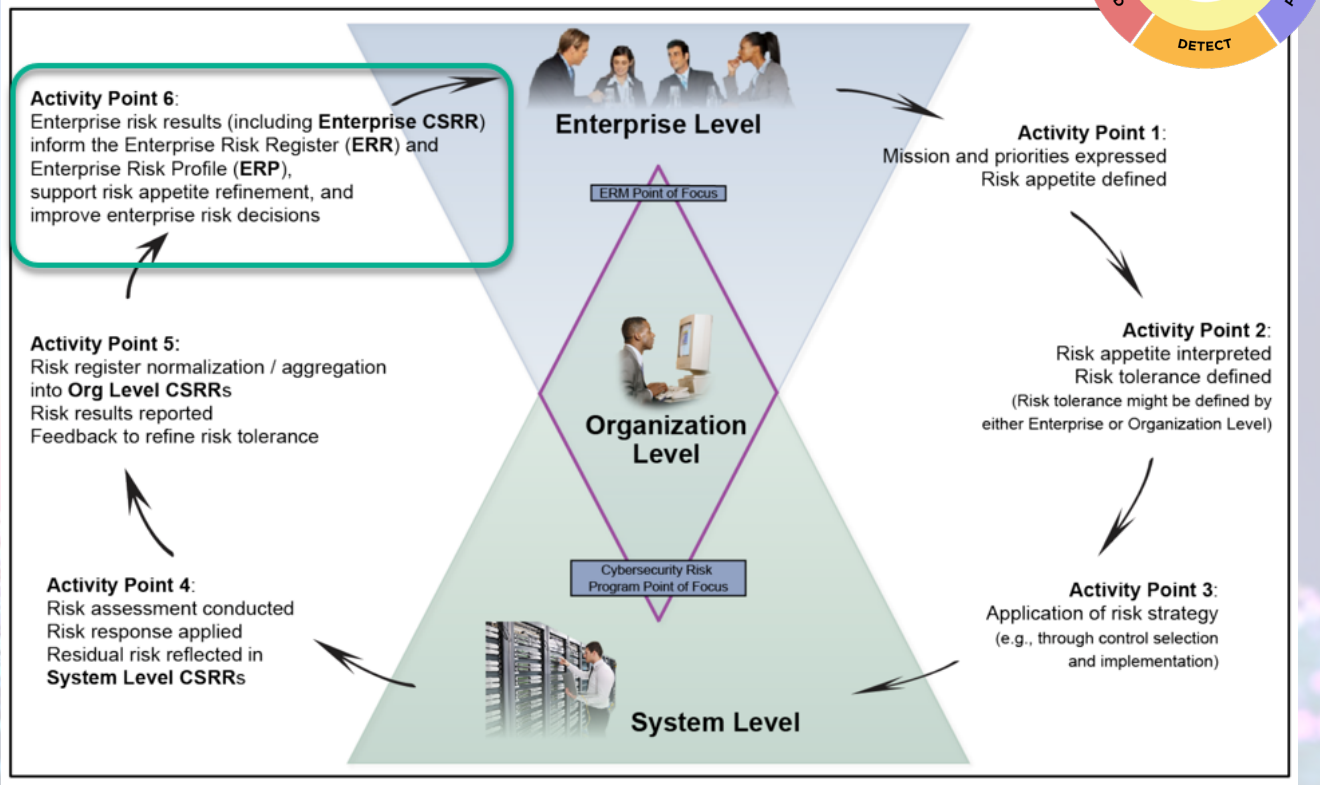
As risk management controls are operated, performance is evaluated and adjusted to improve effectiveness and efficiency. Feedback from the MEA cycle sometimes results in more than just adjustments to controls and other Informative References. Feedback may lead to adjustments in:

- CSF Profile
- Risk Detail Record
- Risk Response Description
- Risk Response
- Risk Tolerance
- Risk Appetite
- Policy
- Strategy

This helps report results back to management and enterprise leadership. Results that particularly reflect operational achievement (key performance indicators, or KPIs) confirm conformance with the strategy (GV.RM, GV.SC). This also supports personnel performance monitoring and reporting (GV.RR, GV.PO).

Managers integrate data from normalized and harmonized risk registers and from organization-level reports, compliance and audit reports. These are considered in light of non-technology risk management activities (e.g., credit risk, market risk, labor risk). Considering composite outcomes of positive and negative risk management enables effective balance among investments in and results of risk management activity. Results are reflected in an **enterprise risk register (ERR)** and **an enterprise risk profile (ERP)** that provides a prioritized ERR.

In this way, CSF helps to guide the selection, implementation, and monitoring of specific controls (such as those in the informative references), and the results ensure an effective and ongoing holistic ERM solution for all types of risk.



Questions to Consider

? How are top cybersecurity risks identified for leadership and recorded in the enterprise risk register?

? Are escalation criteria defined to ensure accountability and information sharing? (NIST IR 8286C)

? Are processes in place to marry system/organization-level risk to enterprise-level considerations?

? How are enterprise security and privacy risks (including opportunities) aligned with other risk types?

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

CSF参考情報及びMEAサイクルからのフィードバックは、リスク対応、リスク選好度/許容度、及びポリシーの監視と調整に役立つ。

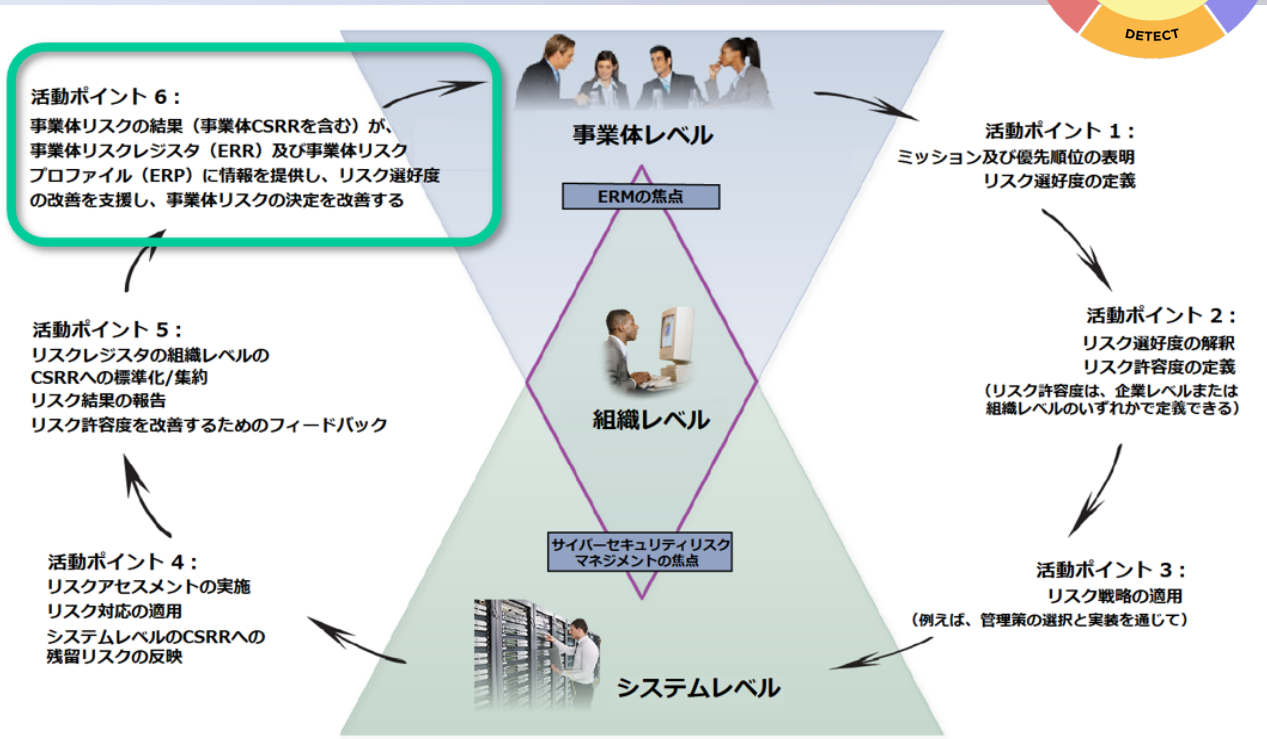
リスクマネジメントの管理策が実施されると、パフォーマンスが評価され、有効性と効率性を改善するために評価される。MEAサイクルからのフィードバックは、管理策及びその他の参考情報の調整以上の結果をもたらすことがある。フィードバックは、以下の調整につながる可能性がある。

- CSFプロファイル
- リスク詳細記録
- リスク対応の説明
- リスク対応
- リスク許容度
- リスク選好度
- ポリシー
- 戦略

これは、経営陣及び事業体のリーダーシップに結果を報告するのに役立つ。特に運用上の成果を反映した結果（主要業績評価指標（KPI））は、戦略 (GV.RM, GV.SC) への適合を確認する。これはまた、人員パフォーマンスの監視及び報告 (GV.RR, GV.PO) もサポートする。

マネージャーは標準化及び調和されたリスクレジスタ、組織レベルの報告書、コンプライアンス及び監査報告書からのデータを統合する。これらは、非技術リスクマネジメント活動（例えば、信用リスク、マーケットリスク、労働者リスク）に照らして考慮される。正と負のリスクマネジメントの複合的な成果を考慮することにより、リスクマネジメント活動への投資とその成果の効果的なバランスをとることができる。結果は、**事業体リスクレジスタ (ERR)** 及び優先順位付けされたERRを提供する**事業体リスクプロファイル (ERP)** に反映される。

このように、CSFは、特定の管理策（参考情報にある管理策など）の選択、実装、及び監視の指針となり、その結果、あらゆる種類のリスクに対する効果的かつ継続的なERMソリューションが確保される。



検討すべき質問

- ? リーダーシップにとって、重要なサイバーセキュリティリスクはどのように識別され、事業体のリスクレジスタに登録されるか？
- ? 説明責任及び情報共有を確実にするためのエスカレーション基準が定義されているか？ (NIST IR 8286C)
- ? システム/組織レベルのリスクと事業体レベルの考慮事項を結びつけるためのプロセスが整備されているか？
- ? 事業体のセキュリティリスク及びプライバシーリスク（機会を含む）は、他の種類のリスクとどのように整合しているか？

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

What We Learned*

Risk Appetite – statements expressing a general way of defining risk you can accept

Risk Tolerance – statements expressing a specific way of defining risk you cannot accept

Risk Identification – the process of understanding your risks

Enterprise Risk Management – the process of managing general high-level risk

Information and Communications Technology Risk Management – the process of managing various ICT risks

Cybersecurity Risk Management – the process of managing specific cybersecurity risks

CSF Govern – one of six high-level outcomes expressed in CSF; oversight to ensure cybersecurity is managed

Negative Risks – things that are weaknesses or threats

Positive Risks – things that are strengths or opportunities

Cybersecurity Risk Register – a list of your high-priority cybersecurity risks

Risk Response Description – the place in the CSRR where you note CSF outcomes and Informative Reference implementations

Cybersecurity Framework Outcome – what cybersecurity capabilities (or activities) you are trying to achieve

Informative Reference Implementation – how you implement cybersecurity

Online Informative References – a catalog of Informative References hosted at a NIST website

SP 800-53 Control – a security or privacy control from the NIST Special Publication 800-53 controls catalog

Monitor, Evaluate, Adjust – how you actualize cybersecurity; in a Deming Cycle, this is the do, check, act

Feedback Loop – how you make adjustments and improvements

*Descriptions provided are intended as plain language. Please see the NIST Glossary for official NIST definitions.

EXPLORE MORE CSF 2.0 RESOURCES

- CSF 2.0 website
- CSF 2.0 Organizational Profiles
- Informative References
- SP 800-53 – security and privacy controls
- SP 800-221 – Integrating ICT risk management and ERM
- SP 800-221A – Outcome Framework for Integrating ICT RM and ERM
- IR 8286 – Overview of integrating CSRM and ERM
- IR 8286A – Deep dive on risk registers
- IR 8286B – Prioritizing and treating risk responses
- IR 8286C – Integrating the CSF with ERM
- IR 8286D – BIA's role in ERM

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

学んだこと*

リスク選好度 – 受容可能なリスクを定義する一般的な方法を表現するステートメント

リスク許容度 – 受容することができないリスクを定義する具体的な方法を表現するステートメント

リスクの識別 – リスクを理解するプロセス

事業体リスクマネジメント – 一般的な高レベルのリスクを管理するプロセス

情報通信技術（ICT）リスクマネジメント – 様々なICTリスクを管理するプロセス

サイバーセキュリティリスクマネジメント – 特定のサイバーセキュリティリスクを管理するプロセス

CSF 「統治（Govern）」 – CSFで示される6つの高レベルの成果の一つで、サイバーセキュリティを確実に管理するための監督

負のリスク – 弱点又は脅威となるもの

正のリスク – 強み又は機会となるもの

サイバーセキュリティリスクレジスタ – 優先順位の高いサイバーセキュリティリスクのリスト

リスク対応の記述 – サイバーセキュリティリスクレジスタで、CSFの成果及び参考情報の実装を記載する場所

サイバーセキュリティフレームワークの成果 – 達成しようとしているサイバーセキュリティ

参考情報の実装 – どのようにサイバーセキュリティリスクを実装するか

オンライン参考情報 – NISTのウェブサイトでホストされている参考情報のカタログ

SP 800-53 管理策 –NIST SP 800-53 管理策カタログのセキュリティ又はプライバシー管理策

監視（Monitor）、評価（Evaluate）、調整（Adjust） – サイバーセキュリティを実現する方法で、デミングサイクル（PDCA サイクル）では、実施（Do）、点検（Check）、処理（Act）

フィードバックのループ – どのように調整及び改善を行うか

*説明は、分かりやすい言葉を意図している。NISTの公式な定義については、 NIST Glossary を参照のこと。

CSF 2.0 のリソースをもっと調べる

- CSF 2.0 website
- CSF 2.0 Organizational Profiles
- Informative References
- SP 800-53 – セキュリティ及びプライバシー管理策
- SP 800-221 – ICTリスクマネジメントとERMの統合
- SP 800-221A – ICTリスクマネジメントとERMを統合するための成果フレームワーク
- IR 8286 –CSRMとERMの統合の概要
- IR 8286A – リスクレジスタの深掘り
- IR 8286B – リスク対応の優先順位付けと処理
- IR 8286C – CSFとERMの統合
- IR 8286D – ERMにおけるBIAの役割