CSF 2.0 Function	CSF 2.0 Category	CSF 2.0 Category Identifier
Govern (GV)	Organizational Context	(GV.OC)
	Risk Management Strategy	(GV.RM)
	Roles and Responsibilities	(GV.RR)
	Policies and Procedures	(GV.PO)

RECOMMENDED REVISION:

CSF 2.0 Function	CSF 2.0 Category	CSF 2.0 Category Identifier
Govern (GV)	Organizational Context	(GV.OC)
	Risk Management Strategy	(GV.RM)
	Roles and Responsibilities	(GV.RR)
	Policies and Procedures	(GV.PO)
	Technology Management	(GV.TM)
	Data Management	(GV.DM)

ID.RA-08: Risks associated with technology suppliers and their supplied products and services are identified, recorded, prioritized, and monitored (formerly ID.SC-2 and PR.DS-8)

RECOMMENDED REVISION: ID.RA-08: Risks associated with technology suppliers, third-party information supply chain, their supplied products, services, and data under their control are identified, recorded, prioritized, and monitored (formerly ID.SC-2 and PR.DS-8).

Policies and Procedures (GV.PO): Organizational cybersecurity policies, processes, and procedures are established and communicated (formerly ID.GV-1)

RECOMMENDED REVISION: Policies and Procedures (GV.PO): Organizational cybersecurity policies, processes, and procedures, covering people, process, technology, as well as data access, handling, and sharing, are established, communicated, and enforced, guided by the tenants of the Zero Trust. (formerly ID.GV-1).

GV.PO-01: Policies, processes, and procedures for managing cybersecurity risks are established based on organizational context, risk management strategy, and priorities and are communicated (formerly ID.GV-1)

RECOMMENDED REVISION: GV.PO-01: Policies, processes, and procedures for managing cybersecurity risks are established, carried out, and scaled using appropriate technology, based on organizational context, risk management strategy, and priorities. These are effectively communicated across the organization (formerly ID.GV-1).

Supply Chain Risk Management (ID.SC): The organization’s supply chain risks are identified, assessed, and managed consistent with the organization’s priorities, constraints, risk tolerances, and assumptions

ID.SC-04: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations

RECOMMENDED REVISION: ID.SC-04: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations. This includes ongoing tracking, control, and protection of data under their custody.

ID.SC-06: Supplier termination and transition processes include security considerations

RECOMMENDED REVISION: ID.SC-06: Supplier termination and transition processes include specific security considerations, particularly focusing on the timely revocation of technology access and secure handling or transfer of data under their control.

Here's how you could articulate the rationale behind these changes:

Technology Management (GV.TM):
In the ever-evolving landscape of technology, it's important for any cybersecurity framework to adequately cover the management of technology within the organization. This is currently missing in CSF 2.0 and would be a beneficial addition for a few reasons:

Technology Proliferation: As the organization adopts and integrates new technologies, it's crucial to have a dedicated category focusing on how these technologies are managed. This could encompass aspects like acquisition, deployment, maintenance, and decommissioning of technology assets.

Risk Exposure: Different technologies carry varying levels of risk, with some introducing new vulnerabilities to the cybersecurity infrastructure. Therefore, having a clear technology management strategy can help mitigate these risks and protect the organization.

Data Management (GV.DM):
Similar to technology, data is a critical asset that's often targeted in cybersecurity threats. However, CSF 2.0 doesn't currently have a distinct focus on data management. Including this as a separate category could benefit the organization by:

Data Protection: The proposed category would cover strategies for data handling, storage, and disposal, leading to enhanced protection of sensitive and business-critical data.

Compliance: With numerous laws and regulations (like GDPR, CCPA) governing data protection, having a data management strategy can help ensure regulatory compliance and avoid potential legal issues.

Incident Response: In case of a data breach, having a pre-established data management strategy could speed up response times, mitigate damages, and help with recovery efforts.

Here's a rationale you can use to validate this change:
In today's interconnected digital ecosystems, organizations do not only depend on technology suppliers for products and services but also engage with various third parties as part of their information supply chain. These third parties could be cloud service providers, data processing agencies, or even business partners with access to the organization's data.
Incorporating the aspect of the "third-party information supply chain" and "data under their control" into this guideline makes it more comprehensive for a few reasons:

1. **Expanded Risk Landscape:** Third-party entities and the data under their control can pose significant security risks. A third party with lax security protocols could be an entry point for attackers to compromise the organization's data.
2. **Regulatory Compliance:** Regulatory frameworks like the GDPR, CCPA, and others have specific requirements related to third-party data processors. Acknowledging the role of these entities in the guideline will help organizations ensure they are compliant with these regulations.
3. **Data Control and Visibility:** The data controlled by third parties is often a blind spot for organizations. This modification emphasizes the importance of visibility into how these third parties are handling the organization's data, enabling better data management and security.

Here's a justification for this revision:
As cyber threats grow in complexity and sophistication, it is critical that organizations apply a comprehensive and holistic approach to cybersecurity. Your revision highlights this by explicitly stating that cybersecurity policies, processes, and procedures must cover people, process, technology, and data access, handling, and sharing.

1. **People, Process, Technology:** By stating these three aspects explicitly, the revised guideline ensures that organizations don't overlook any critical area. People, process, and technology are the cornerstones of a robust cybersecurity posture, and policies and procedures should comprehensively cover all three.
2. **Data Access, Handling, and Sharing:** Your revision places explicit focus on these elements, reflecting their critical importance in the modern digital era. By managing how data is accessed, handled, and shared, organizations can significantly mitigate the risk of data breaches.
3. **Zero Trust:** Zero Trust is a security concept centered on the belief that organizations should not automatically trust anything inside or outside its perimeters and instead must verify anything and everything trying to connect to its systems before granting access. By including Zero Trust in this guideline, you're advocating for a security model that's recognized as best practice for today's threat landscape.
4. **Enforcement:** Your revision adds this keyword, emphasizing the need not only to establish and communicate policies but also to ensure they're being followed. This underlines the importance of accountability in maintaining a strong cybersecurity posture.

Here is a rationale for your proposed change:
Carried Out and Scaled Using Appropriate Technology: The current version of the guideline only mentions the establishment of policies, processes, and procedures. However, establishment is only the first step. For effective cybersecurity, these policies and procedures

must be actively carried out. By mentioning this explicitly, your revision ensures organizations understand the need for active execution.

The addition of 'scaled using appropriate technology' also acknowledges the important role that technology plays in cybersecurity. Policies and procedures should be able to adapt to changes in technology and scale as the organization and its technological infrastructure grow. This ensures that the cybersecurity measures remain effective regardless of the size and complexity of the organization's technological landscape.

Effective Communication Across the Organization: Your proposed change stresses the importance of communication. It's not enough for policies and procedures to be established and executed. They must also be effectively communicated to all relevant parties within the organization. This fosters a culture of cybersecurity awareness, ensuring that all employees understand and adhere to the established policies and procedures.

Here is a rationale for your proposed change:

Data Tracking, Control, and Protection: As the value and sensitivity of data increase, ensuring its safety becomes paramount. It's no longer sufficient to merely meet contractual obligations; third parties must also demonstrate they are actively tracking, controlling, and protecting the data in their custody.

1. **Risk Mitigation:** Unauthorized access or exposure of data is a significant risk that can lead to loss of intellectual property, personal data, and breaches of compliance regulations. This amendment ensures that third parties take a proactive role in risk mitigation by tracking, controlling, and protecting data.
2. **Regulatory Compliance:** This addition aligns the guideline with data protection regulations such as GDPR and CCPA, which place requirements on organizations to ensure third parties are adequately safeguarding the data they handle.
3. **Accountability and Transparency:** By requiring ongoing data management activities, this revision fosters accountability and transparency in the organization's interactions with its third-party partners. It ensures that suppliers and partners are held to a higher standard when handling data, contributing to better overall cybersecurity.

Here's a justification for this change:

Timely Revocation of Technology Access: When a supplier relationship is terminated, it's critical to revoke their technology access promptly to prevent unauthorized access to systems and data. Not doing so can lead to security breaches, data theft, and other cyber threats. By specifically mentioning this in the guideline, you ensure that organizations prioritize this often-overlooked aspect of supplier transitions.

Secure Handling or Transfer of Data: Data handled by suppliers can be sensitive and business-critical, and it's important to manage this data securely during supplier transition. This can involve deleting the data from the supplier's systems, transferring it securely back to the organization, or a combination of both.