Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure

File No. S7-09-22 Release Nos. 33-11216; 34-97989

In March 2022, the SEC finalized rules to enhance disclosures about cybersecurity risk management, strategy, governance, and material incident disclosures. These rules added a new item, Item 106, to Regulation S-K, which requires registrants to describe their processes for assessing, identifying, and managing the material risks from cybersecurity threats. This new item also requires registrants to disclose whether any risks from cybersecurity threats materially affect or are reasonably likely to materially affect the registrant. This includes cybersecurity threats as a result of previous cybersecurity incidents.

Additionally, the new rules added a new item, Item 1.05, to Form 8-K. This item requires registrants to disclose any cybersecurity incident that they determine to be material. In the disclosure, the registrant must describe the material aspects of the nature, scope, and timing of the incident, as well as the material impact or likely material impact of the incident on the registrant.

Rules have also been adopted such that foreign private issuers must make periodic disclosure comparable to that required in new Regulation S-K Item 106 using Form 20-F. Form 6-K has also been amended to require foreign issuers to furnish information on material cybersecurity incidents that they make public (or that they are required to make public or disclose).

These disclosures must be made using the new Cybersecurity Disclosure Taxonomy (CYD) in Inline XBRL.

In the illustrations contained within this guide, Text Block concepts are shown in blue text. Concepts that require a Boolean value are shown in green.

Samples in this guide are shown for purposes of illustrating how to tag a disclosure; samples should not be assumed to show what data should be or must be disclosed according to Regulation S-K.

Effective Date:
September 5, 2023

Read the Release:

https://www.sec.gov/files/rules/final/2023/33-11216.pdf

CYD Taxonomy:

https://xbrl.sec.gov/cyd/2024/cyd-2024.zip

RIN:

3235-AM89

Contents

DISCLAIMER
Novaworks, LLC makes no warranties as to the contents of this documentation or software and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Novaworks, LLC further reserves the right to alter the specifications of the contents of the documentation without obligation to notify any person or organization of these changes. This guide is provided by Novaworks for informational purposes only and not for the purpose of providing legal advice. The summary of changes may not include all portions of the rules put forth by the U.S. Securities and Exchange Commission and is provided as an overview of key changes that have been put forth by the SEC.

We highly recommend reviewing the final rule at https://www.sec.gov/rules-regulations/2023/07/s7-09-22#33-11216final (Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure).

TRADEMARK NOTICE
Novaworks and its products are not endorsed, supported or approved by the U.S. Securities and Exchange Commission. Product names used herein are for identification purposes only and may be trademarks of their respective companies.

PATENT NOTICE
XDX is covered by U.S. Patent Nos. 10,095,672, 10,706,221, 11,210,456.

Novaworks

333 Metro Park
Suite F-500
Rochester, NY 14623
(585) 424-1700
www.novaworks.com
support@novaworks.com

Regulation S-K, Item 106

These new rules add disclosures to Item 106 in Regulation S-K as follows:

Item 106(b) – Risk management and strategy — Registrants must describe their processes, if any, for the assessment, identification, and management of material risks from cybersecurity threats and describe whether any risks from cybersecurity threats have materially affected or are reasonably likely to materially affect their business strategy, results of operations, or financial condition.

Item 106(c) – Governance — Registrants must:

- Describe the board's oversight of risks from cybersecurity threats.
- Describe management's role in assessing and managing material risks from cybersecurity threats.

In the CYD taxonomy, the concepts that correspond to the risk management, strategy, and governance disclosures are generally narrative text blocks. Many text block concepts are paired with concepts that represent Boolean flags to indicate whether certain aspects of the cybersecurity processes and polices are true or false. For example, a Boolean concept can indicate *whether* a process exists or has been implemented and, if the value for that Boolean concept is true, the corresponding Text Block concept will indicate *how* it has been implemented.

The concepts that appear on this disclosure are detailed in the following table. Note that in the Reference Text column, emphasis in bold is added to clarify which portion of the reference text applies to the use of the concept. Additional context has been added to reference text using square brackets ([]).

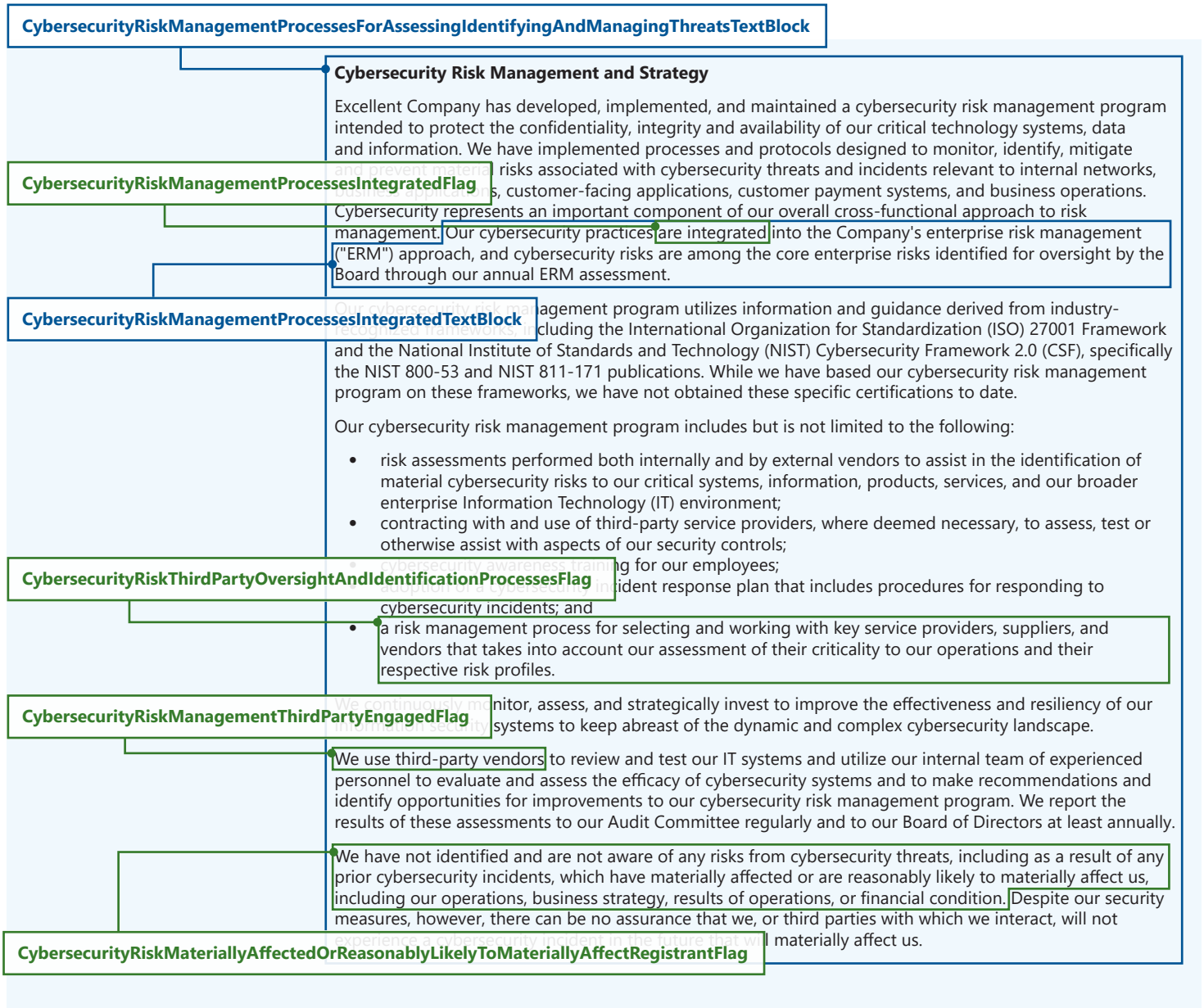
Element Name	Reference	Data Type	Reference Text
cyd:CybersecurityRiskManagementProcesses-ForAssessingIdentifyingAndManagingThreats-TextBlock	Regulation S-K, Item 106(b)(1)	Text Block	(b) Risk management and strategy. (1) Describe the registrant's processes, if any, for assessing, identifying, and managing material risks from cybersecurity threats in sufficient detail for a reasonable investor to understand those processes. In providing such disclosure, a registrant should address, as applicable, the following non-exclusive list of disclosure items: (i) Whether and how any such processes have been integrated into the registrant's overall risk management system or processes; (ii) Whether the registrant engages assessors, consultants, auditors, or other third parties in connection with any such processes; and (iii) Whether the registrant has processes to oversee and identify such risks from cybersecurity threats associated with its use of any third-party service provider.
cyd:CybersecurityRiskManagementProcesses-IntegratedFlag	Regulation S-K, Item 106(b)(1)(i)	Boolean	(i) **Whether** and how **any such processes [for assessing, identifying, and managing material risks from cybersecurity threats] have been integrated into the registrant's overall risk management system or processes**;
cyd:CybersecurityRiskManagementProcesses-IntegratedTextBlock	Regulation S-K, Item 106(b)(1)(i)	Text Block	(i) Whether and **how any such processes [for assessing, identifying, and managing material risks from cybersecurity threats] have been integrated into the registrant's overall risk management system or processes**;
cyd:CybersecurityRiskManagementThirdParty-EngagedFlag	Regulation S-K, Item 106(b)(1)(ii)	Boolean	(ii) Whether the registrant engages assessors, consultants, auditors, or other third parties in connection with any such processes [for assessing, identifying, and managing material risks from cybersecurity threats];
cyd:CybersecurityRiskThirdPartyOversightAnd-IdentificationProcessesFlag	Regulation S-K, Item 106(b)(1)(iii)	Boolean	(iii) Whether the registrant has processes to oversee and identify such risks from cybersecurity threats associated with its use of any third-party service provider.
cyd:CybersecurityRiskMateriallyAffectedOr-ReasonablyLikelyToMateriallyAffectRegistrant-Flag	Regulation S-K, Item 106(b)(2)	Boolean	(2) Describe whether any risks from cybersecurity threats, including as a result of any previous cybersecurity incidents, have materially affected or are reasonably likely to materially affect the registrant, including its business strategy, results of operations, or financial condition ... .
cyd:CybersecurityRiskMateriallyAffectedOr-ReasonablyLikelyToMateriallyAffectRegistrant-TextBlock	Regulation S-K, Item 106(b)(2)	Text Block	(2) Describe whether any risks from cybersecurity threats, including as a result of any previous cybersecurity incidents, have materially affected or are reasonably likely to materially affect the registrant, including its business strategy, results of operations, or financial condition and **if so, how**.

Element Name	Reference	Data Type	Reference Text
cyd:CybersecurityRiskBoardOfDirectors-OversightTextBlock	Regulation S-K, Item 106(c)(1)	Text Block	(c) Governance. (1) Describe the board of directors' oversight of risks from cybersecurity threats. If applicable, identify any board committee or subcommittee responsible for the oversight of risks from cybersecurity threats and describe the processes by which the board or such committee is informed about such risks.
cyd:CybersecurityRiskBoardCommitteeOr-SubcommitteeResponsibleForOversightText-Block	Regulation S-K, Item 106(c)(1)	Text Block	(c) Governance. (1) Describe the board of directors' oversight of risks from cybersecurity threats. **If applicable, identify any board committee or subcommittee responsible for the oversight of risks from cybersecurity threats** and describe the processes by which the board or such committee is informed about such risks.
cyd:CybersecurityRiskProcessForInforming-BoardCommitteeOrSubcommitteeResponsible-ForOversightTextBlock	Regulation S-K, Item 106(c)(1)	Text Block	(c) Governance. (1) Describe the board of directors' oversight of risks from cybersecurity threats. If applicable, identify any board committee or subcommittee responsible for the oversight of risks from cybersecurity threats and **describe the processes by which the board or such committee is informed about such risks**.
cyd:CybersecurityRiskRoleOfManagementText-Block	Regulation S-K, Item 106(c)(2)	Text Block	(2) Describe management's role in assessing and managing the registrant's material risks from cybersecurity threats. In providing such disclosure, a registrant should address, as applicable, the following non-exclusive list of disclosure items: (i) Whether and which management positions or committees are responsible for assessing and managing such risks, and the relevant expertise of such persons or members in such detail as necessary to fully describe the nature of the expertise; (ii) The processes by which such persons or committees are informed about and monitor the prevention, detection, mitigation, and remediation of cybersecurity incidents; and (iii) Whether such persons or committees report information about such risks to the board of directors or a committee or subcommittee of the board of directors.
cyd:CybersecurityRiskManagementPositionsOr-CommitteesResponsibleFlag	Regulation S-K, Item 106(c)(2)(i)	Boolean	(i) **Whether** and which **management positions or committees are responsible for assessing and managing such risks [from cybersecurity threats]**, and the relevant expertise of such persons or members in such detail as necessary to fully describe the nature of the expertise;
cyd:CybersecurityRiskManagementPositionsOr-CommitteesResponsibleTextBlock	Regulation S-K, Item 106(c)(2)(i)	Text Block	(i) Whether and **which management positions or committees are responsible for assessing and managing such risks [from cybersecurity threats]**, and the relevant expertise of such persons or members in such detail as necessary to fully describe the nature of the expertise;
cyd:CybersecurityRiskManagementExpertiseOf-ManagementResponsibleTextBlock	Regulation S-K, Item 106(c)(2)(i)	Text Block	(i) Whether and which management positions or committees are responsible for assessing and managing such risks, and **the relevant expertise of such persons or members in such detail as necessary to fully describe the nature of the expertise**;
cyd:CybersecurityRiskProcessForInforming-ManagementOrCommitteesResponsibleText-Block	Regulation S-K, Item 106(c)(2)(ii)	Text Block	(ii) The processes by which such persons or committees are informed about and monitor the prevention, detection, mitigation, and remediation of cybersecurity incidents;
cyd:CybersecurityRiskManagementPositionsOr-CommitteesResponsibleReportToBoardFlag	Regulation S-K, Item 106(c)(2)(iii)	Boolean	(iii) Whether such persons or committees report information about such risks [from cybersecurity threats] to the board of directors or a committee or subcommittee of the board of directors.

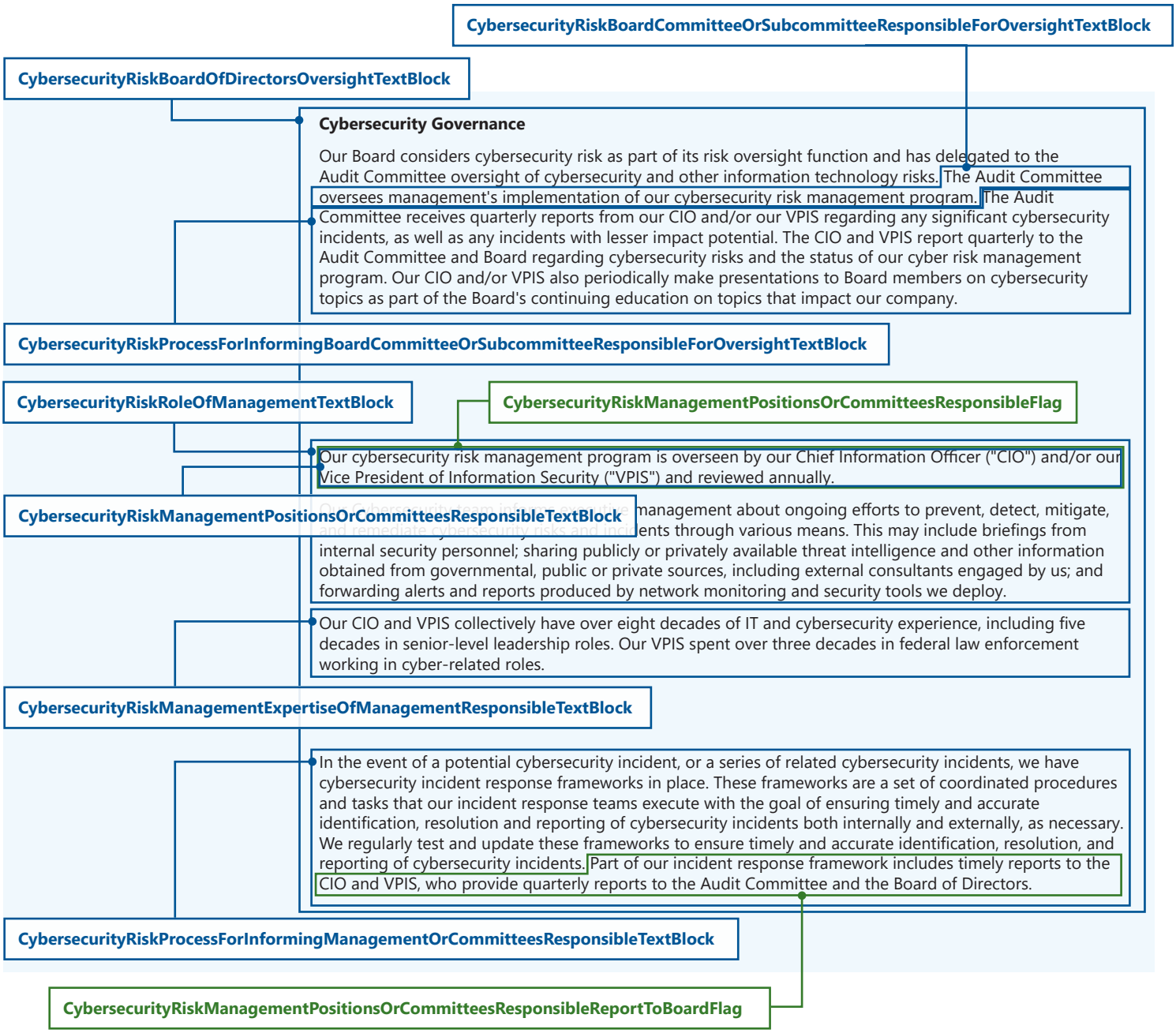
It is important to note that some of these text block elements may have fact values that overlap within the text of the disclosure, which may make tagging the disclosure challenging. In such cases, preparers can use "continuations" to combine data from different HTML blocks into one fact. A continuation can allow an XBRL fact to contain sentences or data from multiple HTML paragraph or table blocks.

The following illustration shows an example of a disclosure containing a registrant's policies for *Cybersecurity Risk Management and Strategy* with the tagging marked. For items in blue, a preparer can tag blocks with the Text Block concept. For items in green, preparers should tag the appropriate text that indicates the disclosure pertaining to the Boolean concept. Once tagged, the text must be transformed using the *ixt:booleantrue* transform to set a fact value of "true" or the *ixt:booleanfalse* transform to set a fact value of "false". While hidden facts may be used for these concepts, it is recommended to find text within the disclosure that corresponds to the fact value so that users of the data may view the fact within the context of the disclosure.

For some concept pairs, the Boolean concept will have a fact value of false. In such instances, the corresponding Text Block concept may not apply. In our example below, there is no value for the *CybersecurityRiskMateriallyAffectedOrReasonablyLikelyToMateriallyAffectRegistrantTextBlock* concept because the value for *CybersecurityRiskMateriallyAffectedOrReasonablyLikelyToMateriallyAffectRegistrantFlag* concept would be set to "false".



The following illustration shows an example of a disclosure containing a registrant's policies for *Cybersecurity Governance* with the tagging marked. For items in blue, a preparer can tag blocks with the Text Block concept. For items in green, preparers should tag the appropriate text that indicates the disclosure pertaining to the Boolean concept. Once tagged, the text must be transformed using the *ixt:booleantrue* transform to set a fact value of "true" or the *ixt:booleanfalse* transform to set a fact value of "false". While hidden facts may be used for these concepts, it is recommended to find text within the disclosure that corresponds to the fact value so that users of the data may view the fact within the context of the disclosure.



In our example, we tagged the same data for both the *CybersecurityRiskManagementPositionsOrCommitteesResponsibleFlag* and *CybersecurityRiskManagementPositionsOrCommitteesResponsibleTextBlock* concepts. Doing so is not required or may not be appropriate depending on your own disclosures. It is important to tag data within the disclosure that relates to the answer for the Boolean concept. In this case, the data that best descibes which management positions or committees are responsible for assessing and managing risks from cybersecurity threats is also the most appropriate to tag to indicate whether our example registrant has management positions that are responsible for assessing and managing cybersecurity risks.

Form 8-K, Item 1.05

The new rules add disclosures to Form 8-K under Item 1.05. Within Item 1.05, registrants must disclose any cybersecurity incident they experience that is determined to be material and describe the material aspects of the incident's nature, scope, and timing, as well as the impact or reasonably likely impact of the incident.

When reporting cybersecurity incidents, the Form 8-K submission with the Item 1.05 disclosure must be filed within *four business days* of determining an incident was material. A registrant may delay filing if the United States Attorney General determines immediate disclosure would pose a substantial risk to national security or public safety.

If information was not determined or was unavailable at the time of the initial 8-K filing, registrants should disclose the incident and any information that is available. Registrants must then amend the prior Item 1.05 Form 8-K to disclose such information when it becomes available.

In the CYD taxonomy, the concepts that correspond to cybersecurity incidents are Text Block concepts. Because more than one incident may be reported on a Form 8-K, incidents are reported using the *MaterialCybersecurityIncidentAxis* concept with a custom member concept that identifies the incident. Preparers may choose an identifying mnemonic such as the date or the nature of the incident to use within the custom member concept name and to distinguish separate incidents. If filing subsequent amendments to a Form 8-K, preparers should use the same member name as was used in the initial filing.

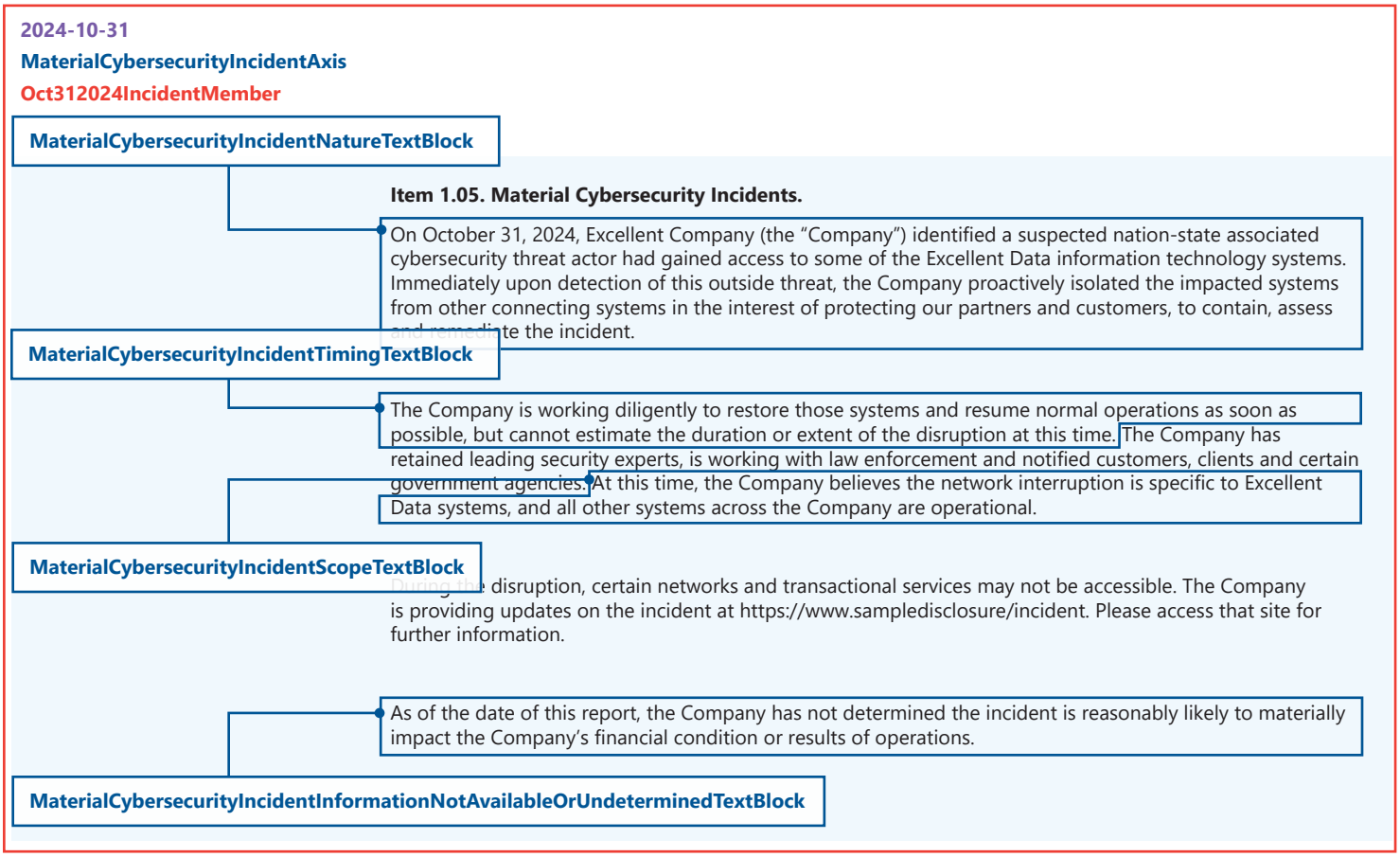
The periods used for the Text Block concepts should be the Date of Report (which corresponds to the date of the earliest event reported on the Form 8-K). If an amendment is filed to provide more information for a previously reported incident, the original date of report should be used as the period for the Text Block concepts, not the date of the amendment.

The concepts that appear on this disclosure are detailed in the following table. Note that in the Reference Text column, emphasis in bold is added to clarify which portion of the reference text applies to the use of the concept.

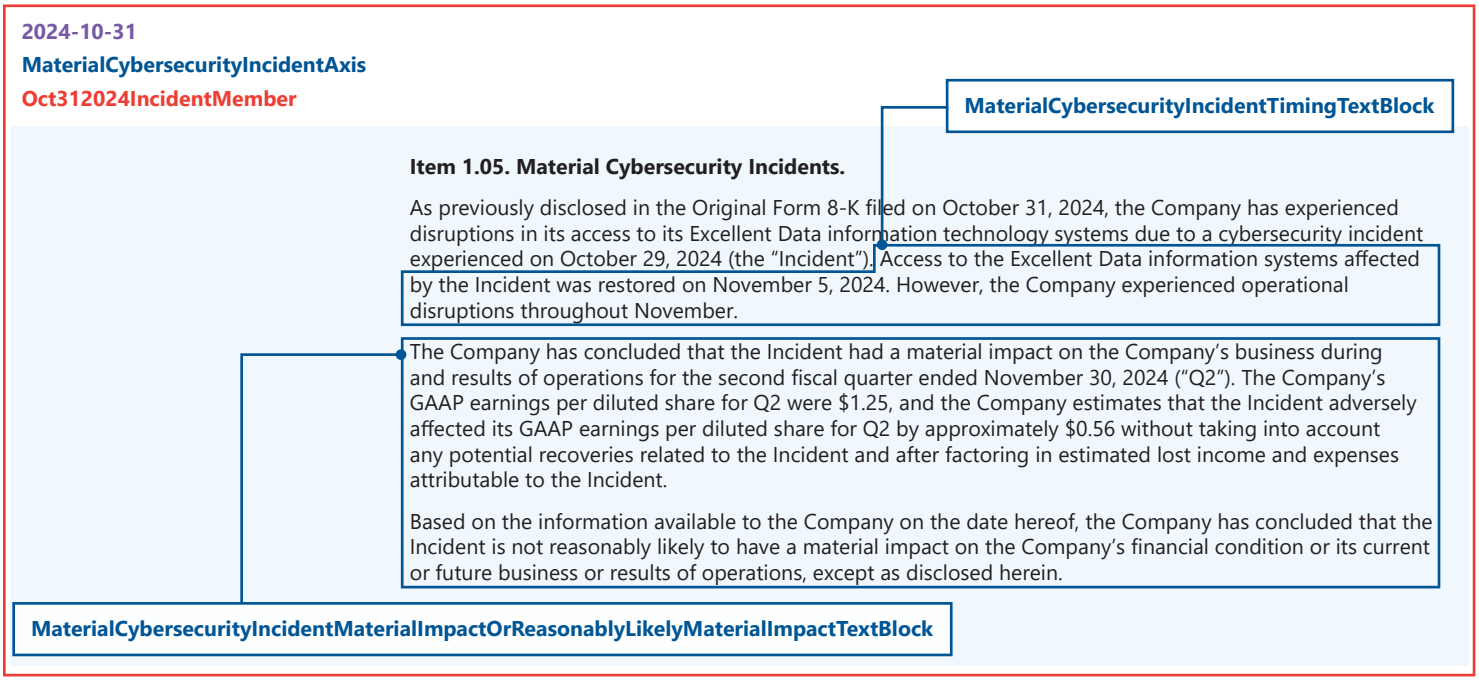
Element Name	Reference	Data Type	Reference Text
cyd:MaterialCybersecurityIncidentNatureTextBlock	Form 8-K, 1.05(a)	Text Block	(a) **If the registrant experiences a cybersecurity incident that is determined by the registrant to be material, describe the material aspects of the nature**, scope, and timing **of the incident**, and the material impact or reasonably likely material impact on the registrant, including its financial condition and results of operations.
cyd:MaterialCybersecurityIncidentScopeTextBlock	Form 8-K, 1.05(a)	Text Block	(a) If the registrant experiences a cybersecurity incident that is determined by the registrant to be material, **describe the material aspects of the** nature, **scope**, and timing **of the incident**, and the material impact or reasonably likely material impact on the registrant, including its financial condition and results of operations.
cyd:MaterialCybersecurityIncidentTimingTextBlock	Form 8-K, 1.05(a)	Text Block	(a) If the registrant experiences a cybersecurity incident that is determined by the registrant to be material, **describe the material aspects** of the nature, scope, and **timing of the incident**, and the material impact or reasonably likely material impact on the registrant, including its financial condition and results of operations.
cyd:MaterialCybersecurityIncidentMaterialImpactOrReasonablyLikelyMaterialImpactTextBlock	Form 8-K, 1.05(a)	Text Block	(a) If the registrant experiences a cybersecurity incident that is determined by the registrant to be material, **describe** the material aspects of the nature, scope, and timing of the incident, and **the material impact or reasonably likely material impact on the registrant, including its financial condition and results of operations**.
cyd:MaterialCybersecurityIncidentInformationNotAvailableOrUndeterminedTextBlock	Form 8-K, 1.05, Instruction 2	Text Block	2. To the extent that the information called for in Item 1.05(a) is not determined or is unavailable at the time of the required filing, the registrant shall include a statement to this effect in the filing and then must file an amendment to its Form 8-K filing under this Item 1.05 containing such information within four business days after the registrant, without unreasonable delay, determines such information or within four business days after such information becomes available.

As mentioned above, each of these concepts will be used to create facts within a context that uses the *MaterialCybersecurityIncidentAxis* and the Date of Report for the initial 8-K filing that first discloses the cybersecurity incident.

The following illustration shows an example of an Item 1.05 8-K disclosure. The custom member element to identify the incident is shown in red text. The period used for the context is shown in purple. Each concept for this incident will be used in conjunction with that member and period combination.



The following illustration shows an example of an Item 1.05 8-K/A disclosure. The custom member element to identify the incident is shown in red text. The period for the context is shown in purple. Note that for the amendment, the period used is the period for the original disclosure, not the date the amendment was filed.



Form 20-F, Item 16K

These new rules add new disclosures to Form 20-F that are essentially identical to the changes made to Regulation S-K. Under Item 16K, foreign private issuers must:

- Describe the board's oversight of risks from cybersecurity threats; and
- Describe management's role in assessing and managing material risks from cybersecurity threats.

In the CYD taxonomy, the concepts used for the Item 16K disclosure are the same concepts that are used for the 10-K Item 106 disclosure. The concepts that correspond to the risk management, strategy, and governance disclosures are generally narrative text blocks. Many text block concepts are paired with concepts that represent Boolean flags to indicate whether certain aspects of the cybersecurity processes and polices are true or false. For example, a Boolean concept can indicate *whether* a process exists or has been implemented and, if the value for that Boolean concept is true, the corresponding Text Block concept will indicate *how* it has been implemented.

The concepts that appear on this disclosure are detailed in the following table. Note that in the Reference Text column, emphasis in bold is added to clarify which portion of the reference text applies to the use of the concept. Additional context has been added to reference text using square brackets ([]).

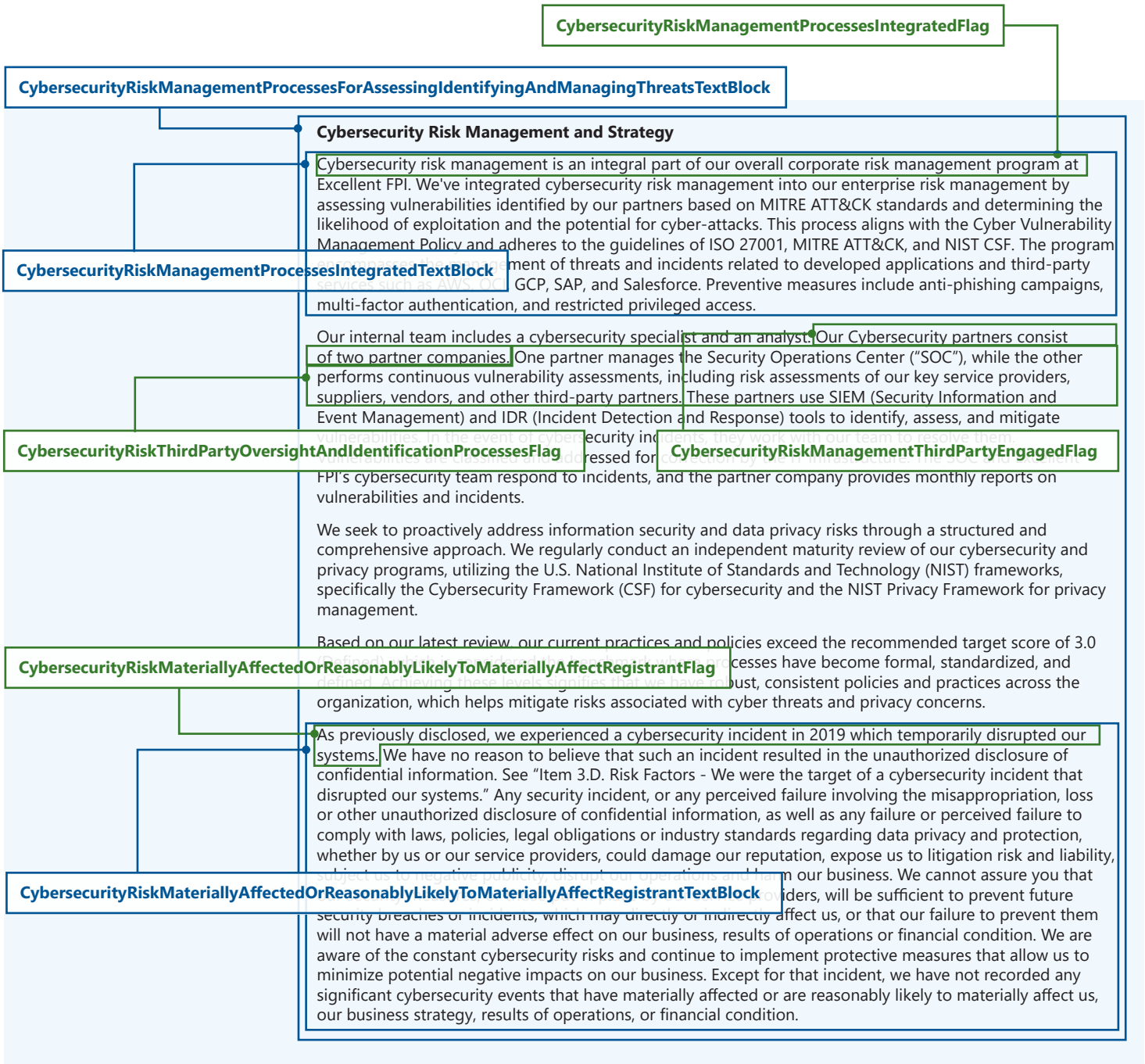
Element Name	Reference	Data Type	Reference Text
cyd:CybersecurityRiskManagementProcesses-ForAssessingIdentifyingAndManagingThreats-TextBlock	Item 16K(b)(1)	Text Block	(b) Risk management and strategy. (1) Describe the registrant's processes, if any, for assessing, identifying, and managing material risks from cybersecurity threats in sufficient detail for a reasonable investor to understand those processes. In providing such disclosure, a registrant should address, as applicable, the following non-exclusive list of disclosure items: (i) Whether and how any such processes have been integrated into the registrant's overall risk management system or processes; (ii) Whether the registrant engages assessors, consultants, auditors, or other third parties in connection with any such processes; and (iii) Whether the registrant has processes to oversee and identify such risks from cybersecurity threats associated with its use of any third-party service provider.
cyd:CybersecurityRiskManagementProcesses-IntegratedFlag	Item 16K(b)(1)(i)	Boolean	(i) **Whether** and how **any such processes [for assessing, identifying, and managing material risks from cybersecurity threats] have been integrated into the registrant's overall risk management system or processes**;
cyd:CybersecurityRiskManagementProcesses-IntegratedTextBlock	Item 16K(b)(1)(i)	Text Block	(i) Whether and **how any such processes [for assessing, identifying, and managing material risks from cybersecurity threats] have been integrated into the registrant's overall risk management system or processes**;
cyd:CybersecurityRiskManagementThirdParty-EngagedFlag	Item 16K(b)(1)(ii)	Boolean	(ii) Whether the registrant engages assessors, consultants, auditors, or other third parties in connection with any such processes [for assessing, identifying, and managing material risks from cybersecurity threats];
cyd:CybersecurityRiskThirdPartyOversightAnd-IdentificationProcessesFlag	Item 16K(b)(1)(iii)	Boolean	(iii) Whether the registrant has processes to oversee and identify such risks from cybersecurity threats associated with its use of any third-party service provider.
cyd:CybersecurityRiskMateriallyAffectedOr-ReasonablyLikelyToMateriallyAffectRegistrant-Flag	Item 16K(b)(2)	Boolean	(2) Describe whether any risks from cybersecurity threats, including as a result of any previous cybersecurity incidents, have materially affected or are reasonably likely to materially affect the registrant, including its business strategy, results of operations, or financial condition ... .
cyd:CybersecurityRiskMateriallyAffectedOr-ReasonablyLikelyToMateriallyAffectRegistrant-TextBlock	Item 16K(b)(2)	Text Block	(2) Describe whether any risks from cybersecurity threats, including as a result of any previous cybersecurity incidents, have materially affected or are reasonably likely to materially affect the registrant, including its business strategy, results of operations, or financial condition and **if so, how**.

Element Name	Reference	Data Type	Reference Text
cyd:CybersecurityRiskBoardOfDirectors-OversightTextBlock	Item 16K(c)(1)	Text Block	(c) Governance. (1) Describe the board of directors' oversight of risks from cybersecurity threats. If applicable, identify any board committee or subcommittee responsible for the oversight of risks from cybersecurity threats and describe the processes by which the board or such committee is informed about such risks.
cyd:CybersecurityRiskBoardCommitteeOr-SubcommitteeResponsibleForOversightText-Block	Item 16K(c)(1)	Text Block	(c) Governance. (1) Describe the board of directors' oversight of risks from cybersecurity threats. **If applicable, identify any board committee or subcommittee responsible for the oversight of risks from cybersecurity threats** and describe the processes by which the board or such committee is informed about such risks.
cyd:CybersecurityRiskProcessForInforming-BoardCommitteeOrSubcommitteeResponsible-ForOversightTextBlock	Item 16K(c)(1)	Text Block	(c) Governance. (1) Describe the board of directors' oversight of risks from cybersecurity threats. If applicable, identify any board committee or subcommittee responsible for the oversight of risks from cybersecurity threats and **describe the processes by which the board or such committee is informed about such risks**.
cyd:CybersecurityRiskRoleOfManagementText-Block	Item 16K(c)(2)	Text Block	(2) Describe management's role in assessing and managing the registrant's material risks from cybersecurity threats. In providing such disclosure, a registrant should address, as applicable, the following non-exclusive list of disclosure items: (i) Whether and which management positions or committees are responsible for assessing and managing such risks, and the relevant expertise of such persons or members in such detail as necessary to fully describe the nature of the expertise; (ii) The processes by which such persons or committees are informed about and monitor the prevention, detection, mitigation, and remediation of cybersecurity incidents; and (iii) Whether such persons or committees report information about such risks to the board of directors or a committee or subcommittee of the board of directors.
cyd:CybersecurityRiskManagementPositionsOr-CommitteesResponsibleFlag	Item 16K(c)(2)(i)	Boolean	(i) **Whether** and which **management positions or committees are responsible for assessing and managing such risks [from cybersecurity threats]**, and the relevant expertise of such persons or members in such detail as necessary to fully describe the nature of the expertise;
cyd:CybersecurityRiskManagementPositionsOr-CommitteesResponsibleTextBlock	Item 16K(c)(2)(i)	Text Block	(i) Whether and **which management positions or committees are responsible for assessing and managing such risks [from cybersecurity threats]**, and the relevant expertise of such persons or members in such detail as necessary to fully describe the nature of the expertise;
cyd:CybersecurityRiskManagementExpertiseOf-ManagementResponsibleTextBlock	Item 16K(c)(2)(i)	Text Block	(i) Whether and which management positions or committees are responsible for assessing and managing such risks, and **the relevant expertise of such persons or members in such detail as necessary to fully describe the nature of the expertise**;
cyd:CybersecurityRiskProcessForInforming-ManagementOrCommitteesResponsibleText-Block	Item 16K(c)(2)(ii)	Text Block	(ii) The processes by which such persons or committees are informed about and monitor the prevention, detection, mitigation, and remediation of cybersecurity incidents;
cyd:CybersecurityRiskManagementPositionsOr-CommitteesResponsibleReportToBoardFlag	Item 16K(c)(2)(iii)	Boolean	(iii) Whether such persons or committees report information about such risks [from cybersecurity threats] to the board of directors or a committee or subcommittee of the board of directors.

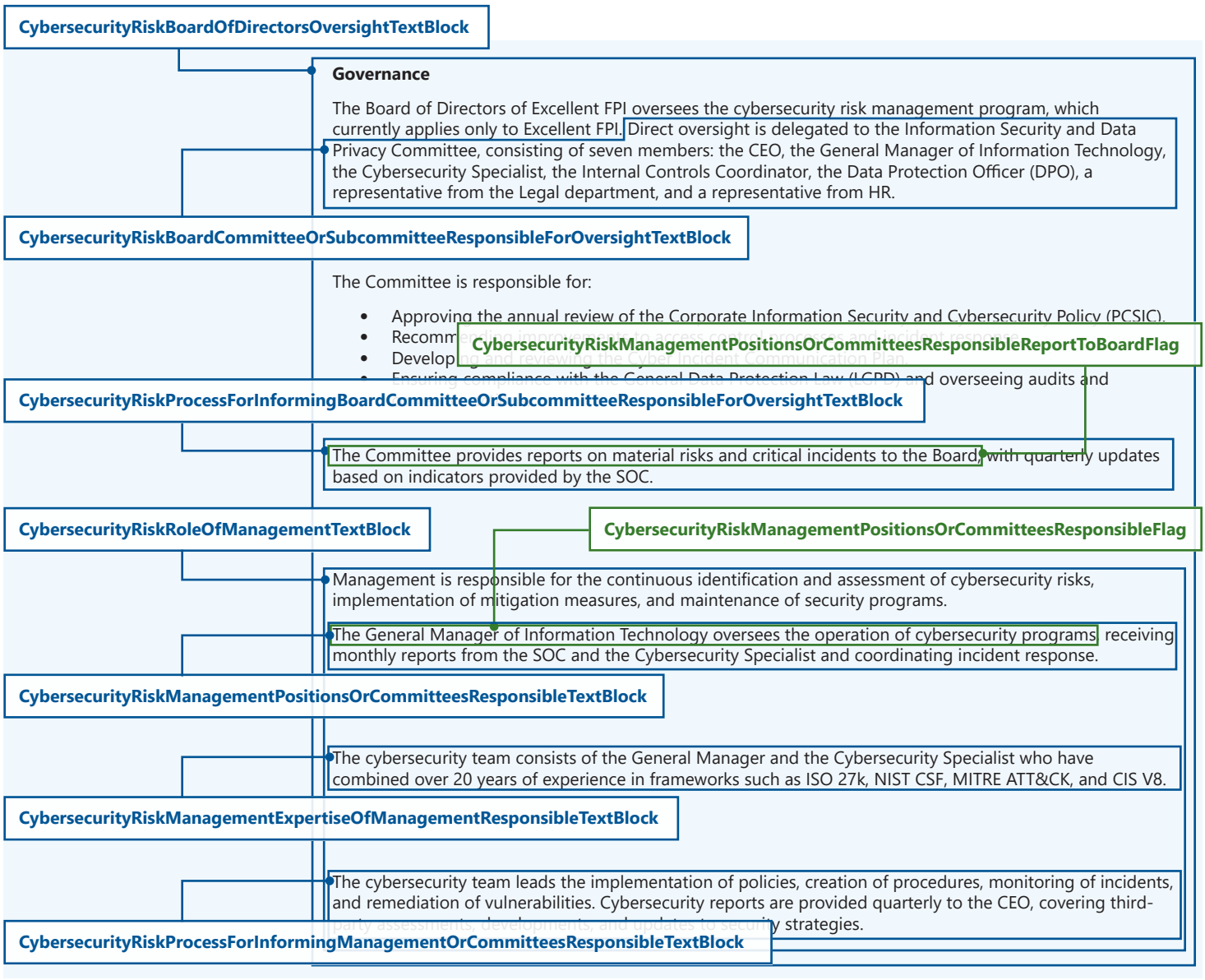
It is important to note that some of these text block elements may have fact values that overlap within the text of the disclosure, which may make tagging the disclosure challenging. In such cases, preparers can use "continuations" to combine data from different HTML blocks into one fact. A continuation can allow an XBRL fact to contain sentences or data from multiple HTML paragraph or table blocks.

The following illustration shows an example of a disclosure containing a registrant's policies for Item 16K(b). For items in blue, a preparer can tag blocks with the Text Block concept. For items in green, preparers should tag the appropriate text that indicates the disclosure pertaining to the Boolean concept. Once tagged, the text must be transformed using the *ixt:booleantrue* transform to set a fact value of "true" or the *ixt:booleanfalse* transform to set a fact value of "false". While hidden facts may be used for these concepts, it is recommended to find text within the disclosure that corresponds to the fact value so that users of the data may view the fact within the context of the disclosure.

For some concept pairs, the Boolean concept will have a fact value of false. In such instances, the corresponding Text Block concept may not apply. In our example below, there is no value for the *CybersecurityRiskMateriallyAffectedOrReasonablyLikelyToMateriallyAffectRegistrantTextBlock* concept because the value for *CybersecurityRiskMateriallyAffectedOrReasonablyLikelyToMateriallyAffectRegistrantFlag* concept would be set to "false".



The following illustration shows an example of a disclosure containing a registrant's policies for Item 16K(c) with the tagging marked. For items in blue, a preparer can tag blocks with the Text Block concept. For items in green, preparers should tag the appropriate text that indicates the disclosure pertaining to the Boolean concept. Once tagged, the text must be transformed using the *ixt:booleantrue* transform to set a fact value of "true" or the *ixt:booleanfalse* transform to set a fact value of false. While hidden facts may be used for these concepts, it is recommended to find text within the disclosure that corresponds to the fact value so that users of the data may view the fact within the context of the disclosure.



In our illustration, we've broken apart paragraphs to allow for an easier visualization of the tagging. Tagging may include multiple Text Block facts within a single HTML paragraph or block. Items may also be nested or overlap within the disclosure.

For example, as you can see in our above sample, we tagged portions of the same HTML paragraph for both the CybersecurityRiskManagementPositionsOrCommitteesResponsibleReportToBoardFlag and the CybersecurityRiskProcessForInformingBoardCommitteeOrSubcommitteeResponsibleForOversightTextBlock concepts. Doing so is not required or may not be appropriate depending on your own disclosures. It is important to tag data within the disclosure that relates to the answer for the Boolean concept. In this case, the data that best descibes the process for reporting to the board is also the most appropriate to tag to indicate whether our example registrant has management positions or committees that are responsible for informing the board of cybersecurity risks.

Form 6-K

The new rules add disclosures to Form 6-K that are substantially the same as the disclosures required by Item 1.05 of Form 8-K. Under the new rules, registrants must disclose any cybersecurity incident they experience that is determined to be material and that they disclose or otherwise publicize in a foreign jurisdiction to any stock exchange or to security holders.

As part of the disclosure, registrants must provide information about the material aspects of the incident's nature, scope, and timing, as well as the impact or reasonably likely impact of the incident.

If information was not determined or was unavailable at the time of the initial 6-K filing, registrants should disclose the incident and any information that is available. Registrants must then amend the 6-K to disclose such information when it becomes available.

In the CYD taxonomy, the concepts that correspond to cybersecurity incidents are Text Block concepts. Because more than one incident may be reported on a Form 6-K, incidents are reported using the *MaterialCybersecurityIncidentAxis* concept with a custom member concept that identifies the incident. Preparers may choose an identifying mnemonic such as the date or the nature of the incident to use within the custom member concept name and to distinguish separate incidents. If filing subsequent amendments to a Form 8-K, preparers should use the same member name as was used in the initial filing.

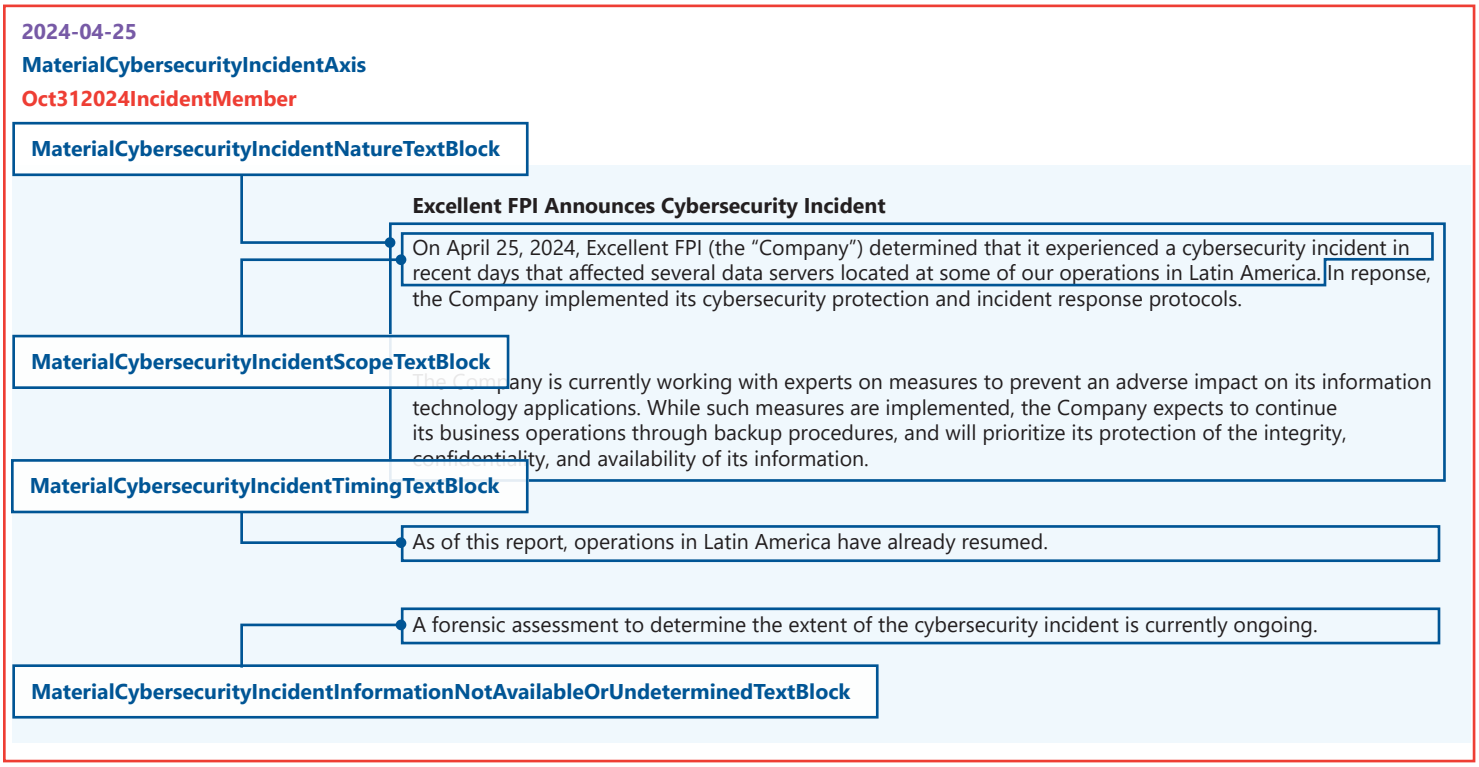
The periods used for the Text Block concepts should be the Date of Report (which corresponds to the date of the earliest event reported on the Form 6-K). If an amendment is filed to provide more information for a previously reported incident, the original date of report should be used as the period for the Text Block concepts, not the date of the amendment.

The concepts that appear on this disclosure are detailed in the following table. Note that in the Reference Text column, emphasis in bold is added to clarify which portion of the reference text applies to the use of the concept. In the taxonomy, the reference for items on Form 6-K is General Instruction B, which contains information on the conditions that trigger a 6-K filing, without express instructions on the meaning of the concepts for disclosing cybersecurity incidents. For that reason, the Reference Text column in the table below contains the reference text for the concept on Form 8-K, Item 1.05, to help preparers distinguish which concepts should be used for which portions of the disclosure.

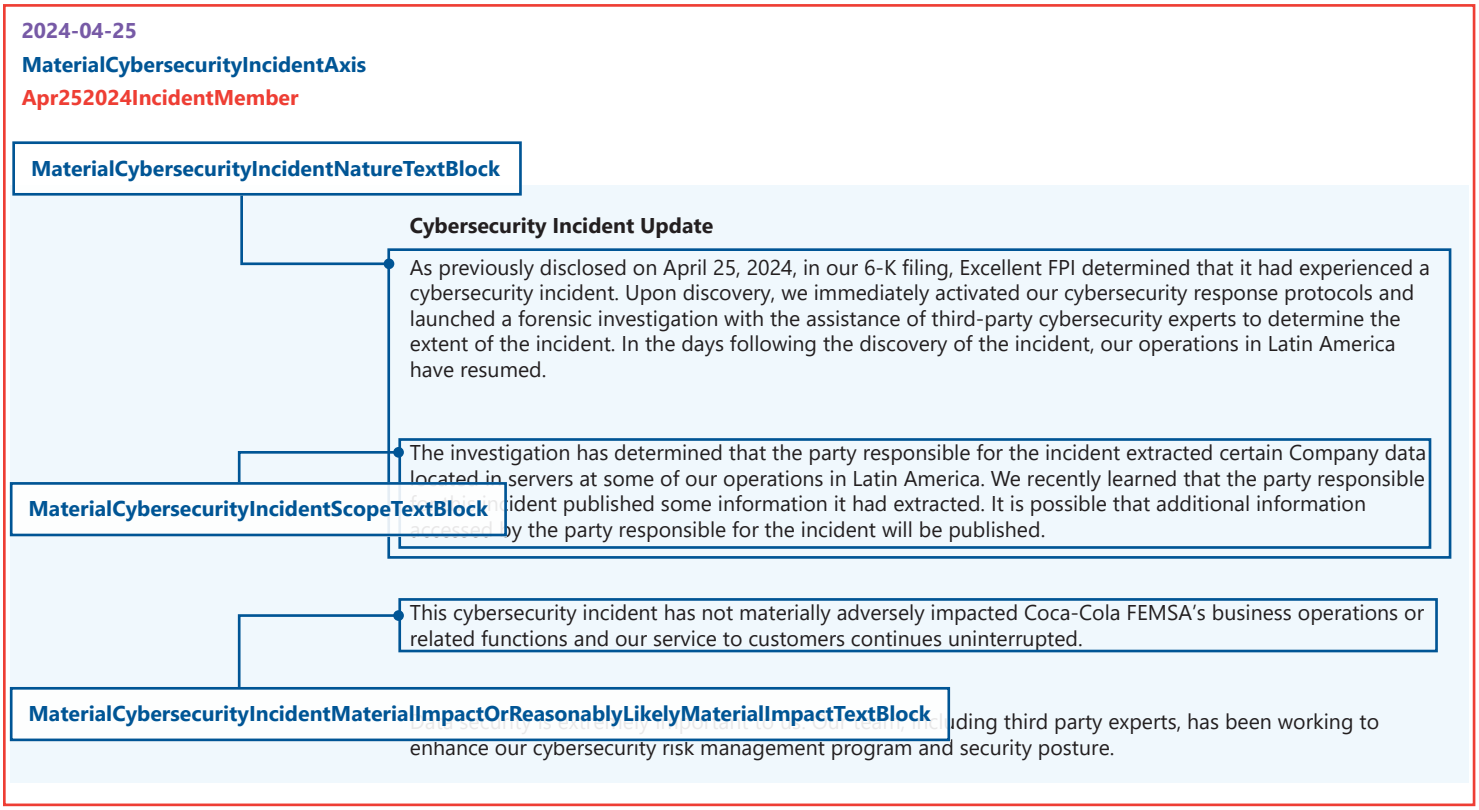
Element Name	Reference	Data Type	Reference Text
cyd:MaterialCybersecurityIncidentNatureTextBlock	Form 6-K, General Instruction B Form 8-K, 1.05(a)	Text Block	(a) **If the registrant experiences a cybersecurity incident that is determined by the registrant to be material, describe the material aspects of the nature**, scope, and timing **of the incident**, and the material impact or reasonably likely material impact on the registrant, including its financial condition and results of operations.
cyd:MaterialCybersecurityIncidentScopeTextBlock	Form 6-K, General Instruction B Form 8-K, 1.05(a)	Text Block	(a) If the registrant experiences a cybersecurity incident that is determined by the registrant to be material, **describe the material aspects of the** nature, **scope**, and timing **of the incident**, and the material impact or reasonably likely material impact on the registrant, including its financial condition and results of operations.
cyd:MaterialCybersecurityIncidentTimingTextBlock	Form 6-K, General Instruction B Form 8-K, 1.05(a)	Text Block	(a) If the registrant experiences a cybersecurity incident that is determined by the registrant to be material, **describe the material aspects** of the nature, scope, and **timing of the incident**, and the material impact or reasonably likely material impact on the registrant, including its financial condition and results of operations.
cyd:MaterialCybersecurityIncidentMaterialImpactOrReasonablyLikelyMaterialImpactTextBlock	Form 6-K, General Instruction B Form 8-K, 1.05(a)	Text Block	(a) If the registrant experiences a cybersecurity incident that is determined by the registrant to be material, **describe** the material aspects of the nature, scope, and timing of the incident, and **the material impact or reasonably likely material impact on the registrant, including its financial condition and results of operations**.
cyd:MaterialCybersecurityIncidentInformationNotAvailableOrUndeterminedTextBlock	Form 6-K, General Instruction B Form 8-K, 1.05, Instruction 2	Text Block	2. To the extent that the information called for in Item 1.05(a) is not determined or is unavailable at the time of the required filing, the registrant shall include a statement to this effect in the filing and then must file an amendment to its Form 8-K filing under this Item 1.05 containing such information within four business days after the registrant, without unreasonable delay, determines such information or within four business days after such information becomes available.

As mentioned above, each of these concepts will be used to create facts within a context that uses the *MaterialCybersecurityIncidentAxis* and the Date of Report for the initial 6-K filing that first discloses the cybersecurity incident.

The following illustration shows an example of a 6-K disclosure. The custom member element to identify the incident is shown in red text. The period used for the context is shown in purple. Each concept for this incident will be used in conjunction with that member and period combination.



The following illustration shows an example of a 6-K/A disclosure. The custom member element to identify the incident is shown in red text. The period for the context is shown in purple. Note that for the amendment, the period used is the period for the original disclosure, not the date the amendment was filed.



333 Metro Park
Suite F-500
Rochester, NY 14623
(585) 424-1700
www.novaworks.com
support@novaworks.com