Cybersecurity Disclosure Taxonomy Guide

March, 2026

CONTENTS

FIGURES

1 GOAL

This guide provides the technical specifications as to the use of the eXtensible Business Reporting Language [XBRL] for the submission of certain required disclosures on Forms 10-K, 20-F, 8-K, and 6-K. It does not provide interpretative guidance for any rule. The taxonomy and guide are intended to cover information that *may* be disclosed pursuant to filers' legal obligations. The inclusion of any information in this taxonomy and guide does not imply every filer must include that information in its disclosures.

2 AUDIENCE

This document explains to a technical audience how to create conforming Interactive Data documents.

Readers should be familiar with Interactive Data as described in the Electronic Data Gathering, Analysis, and Retrieval (EDGAR) Filer Manual [EFM] and EDGAR XBRL Guide [EXG].

Literal technical syntax appears in **`fixed width font`**.

3 STATUS

This document version is for Cybersecurity Disclosure (CYD) 2026. Technical details may change in future CYD versions. For example, elements may be added, deprecated, or deleted. Reference links may be revised to provide greater or less specificity.

4 INSTANCE DOCUMENT CONTENT

The content of an EDGAR submission Inline XBRL document depends on the *form type* (in this case, 10-K, 20-F, 8-K, or 6-K) and its *submission type* (with variants such as 10-K, 10-KT, 20-F, 20-F/A, *etc*.). The concepts in the CYD taxonomy are not limited to any specific Form; they cover both the cybersecurity risk management, strategy, and governance disclosures required in periodic annual forms (10-K, 20-F) as well as disclosures of material cybersecurity incidents in current reports (8-K, 6-K). CYD facts may therefore appear in submissions with only 8-K or 6-K "cover page" concepts from the Document and Entity Information (DEI) taxonomy or may appear with either or both the GAAP Financial Reporting Taxonomy (GRT) and International Financial Reporting Standards (IFRS) concepts, with Executive Compensation Disclosure (ECD) concepts, or in principle any other EDGAR standard taxonomies [STX] depending on the substance of the submission.

5 PHYSICAL LOCATION AND ORGANIZATION

The taxonomy is rooted at URLs of the form

`https://xbrl.sec.gov/cyd/{version}/`

The taxonomy is specifically at the base URL

`https://xbrl.sec.gov/cyd/2026/`

5.1 Versioning

Following the file naming of other standard taxonomies, a file from (for example) a "2nd Quarter 2032" taxonomy file containing reference links would be located at **`https://xbrl.sec.gov/xyz/2032q2/xyz-2032q2_ref.xsd`**.

Following the target namespace conventions of other EDGAR standard taxonomies, the current namespace[1] of the core CYD schema is **`http://xbrl.sec.gov/cyd/2026`** with standard prefix **`cyd`**.

The CYD taxonomy of any given year (irrespective of quarter) is compatible with any other EDGAR standard taxonomy of the same year, and incompatible with other years.

5.2 Imports

EDGAR submissions are required, permitted, or disallowed from referencing various files comprising the CYD taxonomy, as summarized in Figure 1 below.

[1] A namespace URI (uniform resource identifier) is not a URL (uniform resource locator); it does not identify a web address.

Figure 1. Taxonomy files, by type

Taxonomy name and folder	May be referenced in submissions	Used in validation and rendering	Entry point

Cybersecurity Disclosure
`https://xbrl.sec.gov/cyd/2026`
	`cyd-af-2026.xsd`
	`cyd-cr-2026.xsd`
	`cyd-af-sub-2026.xsd`
	`cyd-8k-sub-2026.xsd`
	`cyd-6k-sub-2026.xsd`
	`cyd-2026.xsd`
			`cyd-entire-2026.xsd`

Figure 2 uses indentation and the ↖ character to illustrate the hierarchy of schema imports, and thus implicitly also shows the Discoverable Taxonomy Set (DTS) of each file. Submission set AF (Annual Financials) includes submission types 10-K, 10-K/A, 20-F, *etc.*; all submission sets are defined in [EFM § 6.1.1].

Figure 2. Taxonomy file import relationships

Name	Description
`cyd-2026.xsd`	Root schema with concepts and reference links.
↖ `cyd-af-2026.xsd`	Entry point with definition links for submission set AF
↖ `cyd-af-sub-2026.xsd`	Entry point with presentation and label links for submission set AF
↖ `cyd-cr-2026.xsd`	Entry point with definition links for current reports
↖ `cyd-6k-sub-2026.xsd`	Entry point with presentation links for submission set 6K
↖ `cyd-8k-sub-2026.xsd`	Entry point with presentation links for submission set 8K

Figure 3 shows namespace prefixes and the namespaces in use as of the date of this document.

Figure 3. Namespace URI's and prefixes.

Prefix	Current Namespace URI
`cyd`	`http://xbrl.sec.gov/cyd/2026`

6 TABLES, AXES, AND MEMBERS

Like all XBRL instances, CYD instances contain facts, each defined as a *value* characterized by a set of *dimensions.* The set of dimensions of a fact contain at most one of each *core dimension* (*entity*, *period*, and *concept* among them) and will have zero or more *taxonomy-defined dimensions*. The taxonomy-defined dimensions are used to construct *hypercubes* [DIM]. In this document, as in all SEC standard taxonomies, a taxonomy-defined dimension is called an *axis*. Members of an axis may be its *default* member, a *standard* member, or a *custom* member defined by the filer. In addition to indicators such as names and indentations within tables, concept types are color-coded in this document as shown in Figure 4.

Figure 4. Font and Color-Coding Legend

Concept or value type	Color
Concept core dimension and concepts	Green
Other core dimensions and their members	Gray
Fact values	None
Taxonomy-defined dimension (Axis)	Orange
Standard members	Medium Blue
Custom members	Purple
Abstract placeholder concepts not appearing in instances, such as hypercubes, line items, domain defaults, and non-usable domain members	Light Blue

A hypercube of only a single taxonomy-defined dimension can be visualized as a table as it might be presented in an example disclosure[2] as illustrated in Figure 5:

Figure 5. Example showing presentation of eight text facts with a single taxonomy-defined dimension

entity: Example01 period: 9/13/2030		Concepts Dimension			
		Material Cybersecurity Incident Nature	Material Cybersecurity Incident Scope	Material Cybersecurity Incident Timing	Material Cybersecurity Incident Impact
Incident Axis	Incident A	…text…	…text…	…text…	…text…
	Incident B	…text…	…text…	…text…	…text…

Presentation of the disclosures to a human reader does not change the meaning, and therefore does not change the characterization of each of the eight facts. Figure 6 shows the same facts, with the concept dimension presented as rows, and the incident dimension as columns instead:

Figure 6. Example showing different presentation of the same eight text facts

entity: Example01 period: 9/13/2030		Incident Axis	
		Incident A	Incident B
Concepts Dimension	Material Cybersecurity Incident Nature	…text…	…text…
	Material Cybersecurity Incident Scope	…text…	…text…
	Material Cybersecurity Incident Timing	…text…	…text…
	Material Cybersecurity Incident Impact	…text…	…text…

Finally, the layout in Figure 7 shows the same facts in a manner that more resembles a normal narrative disclosure, with the axis and the concept dimension forming an outline, with all aspects of each incident described before describing the next:

Figure 7. Example showing another alternative presentation of the same eight text facts

entity: Example01 period: 9/13/2030				
Incident Axis	Incident A	Concepts Dimension	Material Cybersecurity Incident Nature	…text…
			Material Cybersecurity Incident Scope	…text…
			Material Cybersecurity Incident Timing	…text…
			Material Cybersecurity Incident Impact	…text…
	Incident B	Concepts Dimension	Material Cybersecurity Incident Nature	…text…
			Material Cybersecurity Incident Scope	…text…
			Material Cybersecurity Incident Timing	…text…
			Material Cybersecurity Incident Impact	…text…

CYD is organized as a pair of hypercubes with zero or one axes; as Figures 6 and 7 show, they are usually thought of – and referred to as – *Tables*. In CYD, the one axis is empty in the taxonomy and is populated only by custom members.

6.1 Zero-axis Tables

Every EDGAR instance document has a zero-axis table. A zero-axis table contains facts that are characterized only by core dimensions - concept, entity, period, and either unit (for numeric facts) or language (for non-numeric facts). Concepts such as the EDGAR Central Index Key (CIK) **`dei:EntityCentralIndexKey`**, or that only appear once on a filing cover page, such as its Form type **`dei:DocumentType`** or the Company "Conformed" name

[2] Material Cybersecurity incident disclosures may contain additional facts, as shown in the Appendix. For simplicity of illustration, the example incident disclosures in this guide are limited to eight text facts.

dei:EntityRegistrantName, are implicitly concepts in a zero-axis table. A zero-axis table contains facts that are characterized only by core dimensions - concept, entity, period, and either unit (for numeric facts) or language (for non-numeric facts). Required Contexts (as defined in [EXG § 3.1.1 Notation and Terminology]) effectively define a zero-axis table for every EDGAR XBRL document. Also, EDGAR instance documents are constrained to have only a single member of the entity dimension represented in a single instance and facts are assumed to have language **en-US** (US English) unless indicated otherwise.

6.1.1 Sample facts with zero axes

Facts in an instance may be visualized as one row per fact and one column per core dimension, so in the case of concepts in the zero-axis table, there are only a few columns, as illustrated in Figure 8.

Figure 8. Sample facts in a CYD instance

concept	entity	period	value
dei:DocumentType	cik:0000012345	2030-01-01/2030-12-31	10-K
dei:EntityRegistrantName	cik:0000012345	2030-01-01/2030-12-31	Example01

Or, using XBRL-JSON syntax, as a list of fact objects:

```
[{ "concept" : "dei:DocumentType",
  "period": "2030-01-01/2030-12-31",
  "entity": "cik:0000012345",
  "value": "10-K" },
 { "concept" : "dei:EntityRegistrantName",
  "period": "2030-01-01/2030-12-31",
  "entity": "cik:0000012345",
  "value": "Example01" }]
```

Or, in the original XML-based XBRL instance syntax:

```
<context id="c1" >
 <entity>
 <identifier scheme="http://www.sec.gov/CIK">0000012345</identifier>
 </entity>
 <period>
 <startDate>2030-01-01</startDate>
 <endDate>2030-12-31</endDate>
 </period>
</context>
<dei:DocumentType contextRef="c1">10-K</dei:DocumentType>
<dei:EntityRegistrantName contextRef id="c1">Example01</dei:EntityRegistrantName>
```

CYD facts are submitted to EDGAR in Inline XBRL. Using the same syntax for **<context> c1**:

```
<ix:nonNumeric name="dei:DocumentType" contextRef="c1">10-K</ix:nonNumeric>
<ix:nonNumeric name="dei:EntityRegistrantName" contextRef id="c1" >Example01</ix:nonNumeric>
```

This taxonomy guide uses a tabular view resembling Figure 8 (usually omitting columns that are less relevant to understanding how to use the CYD taxonomy, such as *entity*) when a set of facts is shown as an example, with the understanding that those facts might be re-serialized from the submission format of xBRL-XML into xBRL-JSON, etc.

Note that concept and member names never contain hyphens (-); they appear only in tabular displays for long elements to introduce line breaks that improves layout in the document.

6.1.2 Cybersecurity Risk Management, Strategy, and Governance Disclosure

CYD contains a few concepts that have no taxonomy-defined dimensions. In Figure 9, the concept dimension shows these concepts, the dimensional relationship (arc) that relates them to their parent concept, and their type.

As detailed in the Dimensional specification [DIM], definition linkbases have arcs that link concepts of different types to define the table structure. Figure 9 illustrates these concepts and relationships as they appear in the taxonomy, a tree pattern that is repeated via naming and ordering conventions throughout CYD and other taxonomies. The concepts

shaded light blue exist as mere placeholders within the dimensional structure. The "line items" concept is a placeholder for all the concepts, the "table" is a placeholder for any axes, and where it appears, the tree root "Abstract" concept ties the concept dimension to the set of axes.

Figure 9. Definition linkbase in zero-axis Cybersecurity Risk Management, Strategy, and Governance Disclosure role

Label	Type	Arcs
Cybersecurity Risk Management, Strategy, and Governance [Abstract]	Abstract	
Cybersecurity Risk Management, Strategy, and Governance [Table]	Hypercube	hypercube-dimension
Cybersecurity Risk Management, Strategy, and Governance [Line Items]	Abstract Line Items	domain-member
Cybersecurity Risk Management Processes for Assessing, Identifying, and Managing Threats [Text Block]	Text Block	domain-member
Cybersecurity Risk Management Processes Integrated [Flag]	Boolean	domain-member
Cybersecurity Risk Management Processes Integrated [Text Block]	Text Block	domain-member
Cybersecurity Risk Management Third Party Engaged [Flag]	Boolean	domain-member
Cybersecurity Risk Third Party Oversight and Identification Processes [Flag]	Boolean	domain-member
Cybersecurity Risk Materially Affected or Reasonably Likely to Materially Affect Registrant [Flag]	Boolean	domain-member
Cybersecurity Risk Materially Affected or Reasonably Likely to Materially Affect Registrant [Text Block]	Text Block	domain-member
Cybersecurity Risk Board of Directors Oversight [Text Block]	Text Block	domain-member
Cybersecurity Risk Board Committee or Subcommittee Responsible for Oversight [Text Block]	Text Block	domain-member
Cybersecurity Risk Process for Informing Board Committee or Subcommittee Responsible for Oversight [Text Block]	Text Block	domain-member
Cybersecurity Risk Role of Management [Text Block]	Text Block	domain-member
Cybersecurity Risk Management Positions or Committees Responsible [Flag]	Boolean	domain-member
Cybersecurity Risk Management Positions or Committees Responsible [Text Block]	Text Block	domain-member
Cybersecurity Risk Management Expertise of Management Responsible [Text Block]	Text Block	domain-member
Cybersecurity Risk Process for Informing Management or Committees Responsible [Text Block]	Text Block	domain-member
Cybersecurity Risk Management Positions or Committees Responsible Report to Board [Flag]	Boolean	domain-member

Concepts in the risk management, strategy, and governance disclosure are generally narrative text blocks, paired with Boolean flags and both corresponding to disclosure requirements. Figure 10 quotes Item 229.106(b) (risk management and strategy) as an example.

In situations where a single paragraph contains information that would need more than one text block or where a section of text contains partial information that could be tagged by one text block and then explained later in another section, text block tagging might be challenging. As disclosure practices develop, staff may consider alternatives in the future.

Figure 10. Fragment of Regulation S-K (17 CFR 229) Item 106

(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.

(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.

(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.

(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.

The disclosure in Figure 10 requires a narrative, which is represented by text block concept **`cyd:CybersecurityRiskManagementProcessesForAssessingIdentifyingAndManagingThreatsTextBlock`**. Within that disclosure, the Boolean flag **`cyd:CybersecurityRiskManagementProcessesIntegratedFlag`** represents "whether" the processes have been integrated, and assuming that value is "true", then the text block **`cyd:CybersecurityRiskManagementProcessesIntegratedTextBlock`** contains the description of "how" the processes have been integrated. This pattern of concepts is followed for the rest of Items 106(b) and (c). For foreign private issuers, a substantially similar disclosure requirement is found in Item 16K to Form 20-F.

Figure 11. Example showing sample facts for a single period

entity: Example01		period FY30
Concepts Dimension	CybersecurityRiskManagementProcessesForAssessingIdentifyingAnd-ManagingThreatsTextBlock	…text…
	CybersecurityRiskManagementProcessesIntegratedFlag	true
	CybersecurityRiskProcessManagementProcessesIntegratedTextBlock	…text…
	CybersecurityThirdPartyOversightAndIdentificationProcessesFlag	false
	CybersecurityRiskMateriallyAffectedOrReasonablyLikelyToMateriallyAffectRegistrantFlag	true
	CybersecurityRiskMateriallyAffectedOrReasonablyLikelyToMateriallyAffectRegistrantTextBlock	…text…
	CybersecurityRiskBoardOfDirectorsOversightTextBlock	…text…
	CybersecurityRiskBoardCommitteeOrSubcommitteeResponsibleForOversight-TextBlock	…text…
	CybersecurityRiskRoleOfManagementTextBlock	…text…
	CybersecurityRiskManagementPositionsOrCommitteesResponsibleFlag	true
	CybersecurityRiskManagementExpertiseOfManagementResponsibleTextBlock	…text…
	CybersecurityRiskProcessForInformingManagementOrCommitteesResponsible-TextBlock	…text…

Rendering (via the presentation and label linkbases) of the facts in a zero-axis table typically resembles the layout of the concept dimension in the definition linkbase. Structural concepts (such as **CybersecurityRiskManagement-StrategyAndGovernanceLineItems** and **CybersecurityRiskManagementStrategyAndGovernanceTable** in the example of Figure 11) do not necessarily appear.

Assuming all the facts are in a single period, there will be a single column of fact values.

The Inline XBRL transformation registry formats **ixt:booleantrue** and **ixt:booleanfalse** can be used to mark a section of text and "flag" it as either true or false. For example, the concept with label "Management Position or Committee Responsible for Cybersecurity Risk [Flag]" may have the value **true** or **false**; it could be reported in narrative form as shown below to indicate that there is no such reporting relationship:

```
<ix:nonNumeric name="CybersecurityRiskManagementPositionsOrCommitteesResponsiblePartyFlag"
contextRef="…" format="ixt:booleanfalse" >The Deputy […] Officer is responsible for
Cybersecurity and chairs the risk management working group that reports to the Chief […]
Officer.</ix:nonNumeric>
```

Or, if there is:

```
<ix:nonNumeric name="CybersecurityRiskManagementPositionsOrCommitteesResponsiblePartyFlag"
contextRef="…" format="ixt:booleantrue" >The Chief […] Officer reporting to the Board of
Directors is responsible for Cybersecurity. </ix:nonNumeric>
```

6.2 Single-axis Tables

6.2.1 Cybersecurity Incident Disclosure, by Incident

Form 8-K requires a set of disclosures that concern specific cybersecurity incidents that a registrant determines to be material, which differs from the cybersecurity risk management and strategy disclosures required in annual reports. Figure 12 shows the specific Item and paragraph of Form 8-K that requires these disclosures, which include the nature, scope, timing, and material impact of each disclosed cybersecurity incident:

Figure 12. Form 8-K Item 1.05(a)

> **Item 1.05 Cybersecurity incidents.**
>
> (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.

For foreign private issuers, a substantially similar disclosure requirement is found in General Instruction B to Form 6-K.

More than one incident is possible, so there is a Material Cybersecurity Incident Axis (**`MaterialCybersecurity-IncidentAxis`**) to permit separate disclosures (Nature, scope, etc.) for each incident. In the custom taxonomy that accompanies an EDGAR submission [EXG § 5.7 Custom Domain Member Declarations] the filer defines a custom domain member, then makes it a domain-member child of the standard concept **`MaterialCybersecurityIncidentDomain`**. In Figure 13, the company Example01 has a custom schema with declared namespace prefix **`e01`**. The custom member **`e01:FirstIncidentMember`** is a domain-member child of **`MaterialCybersecurityIncidentDomain`** in the standard link role **`http://xbrl.sec.gov/cyd/role/Material-CybersecurityIncidentDisclosure`**, the "Material Cybersecurity Incidents" role.

Figure 13. Definition links in the Material Cybersecurity Incidents role, with example custom members.

Label	Type	Arcs
Material Cybersecurity Incident [Abstract]		
Material Cybersecurity Incident [Table]	Hypercube	all
Material Cybersecurity Incident [Axis]	Taxonomy-Defined Dimension (Axis)	hypercube-dimension
Material Cybersecurity Incident [Domain]	Default Member	dimension-domain
First Incident Sep 12, 2030 [Member]	Custom Member	domain-member
Second Incident Sep 12, 2030 [Member]	Custom Member	domain-member
Material Cybersecurity Incident [Line Items]	Abstract Line Items	domain-member
Material Cybersecurity Incident Nature [Text Block]	Text Block	domain-member
Material Cybersecurity Incident Scope [Text Block]	Text Block	domain-member
Material Cybersecurity Incident Timing [Text Block]	Text Block	domain-member
Material Cybersecurity Incident Material Impact or Reasonably Likely Material Impact [Text Block]	Text Block	domain-member
Material Cybersecurity Incident Information Not Available or Undetermined [Text Block]	Text Block	domain-member

By convention, the standard label for member elements ends with "[Member]" making the standard label for this custom element "Incident One [Member]".

Six sample facts are shown in Figure 14, with three facts for **`e01:FirstIncidentMember`** and **`e01:SecondIncidentMember`** respectively.

Figure 14. Example of facts in the Cybersecurity Incidents table

concept	entity	period	incident	value
`MaterialCybersecurity-IncidentNatureTextBlock`	`cik:0000012345`	`2030-09-13/2030-09-13`	`e01:FirstIncidentSep122030Member`	…`text`…
`MaterialCybersecurity-IncidentScopeTextBlock`	`cik:0000012345`	`2030-09-13/2030-09-13`	`e01:FirstIncidentSep122030Member`	…`text`…
`MaterialCybersecurity-IncidentTimingTextBlock`	`cik:0000012345`	`2030-09-13/2030-09-13`	`e01:FirstIncidentSep122030Member`	…`text`…
`MaterialCybersecurity-IncidentMaterialImpact-OrReasonablyLikely-MaterialImpactTextBlock`	`cik:0000012345`	`2030-09-13/2030-09-13`	`e01:SecondIncidentSep122030Member`	…`text`…

These six facts could be displayed in various ways as illustrated earlier in Figure 5, Figure 6, and Figure 7.

The periods used for text blocks should be the Date of Report (Date of earliest event reported) on Form 8-K or 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, not the date of the amendment.

To distinguish separate incidents initially reported on the same Form, it is helpful to provide an identifying mnemonic such as a date or nature of the incident and use the same member name on any subsequent amendments to the Form.

7 PRESENTATION AND LABEL LINKS

Although the CYD taxonomy embeds definition links that group CYD concepts into a zero-axis table (entry point **`cyd-af`**) and a one-axis table entry points (**`cyd-6k`** and **`cyd-8k`**) so as to define which concepts should appear as facts having taxonomy-defined dimensions and which should not, there are no other restrictions on definition, label, or presentation linkbases beyond those that apply to all EDGAR submissions. However, filers can minimize their customization effort by using the standard presentation and label linkbases available to them. Using the **`cyd-8k-sub`** entry point (see Figure 2) provides labels and presentation links sufficient for everything in an 8-K filing for Item 1.05 other than the custom incident member; likewise, the **`cyd-6k-sub`** entry point is sufficient in a 6-K current report filing. Entry point **`cyd-af`** does not include presentation and label links because these could interfere with the substantial customization of presentation and label linkbases usually found in annual financial statements regardless of submission type. Entry point **`cyd-af-sub`** provides them for filers that nevertheless wish to use them.

8 CUSTOM CONCEPTS

Cybersecurity disclosures fall under the Interactive Data requirements of 17 CFR 232.405(d)(4)(i), indicating that numeric values are tagged separately:

> (d) ***
>
> (4) ***
>
> (i) Each amount (i.e., monetary value, percentage, and number) must be tagged separately;

The current version of the CYD taxonomy includes no quantitative standard concepts; filers should refer to [EXG § 5.6 Custom Concept Declarations in General] for guidance on defining custom concepts and [EXG § 5 Custom Taxonomies] generally with regards to custom label, presentation and definition links.

9 REFERENCES

[DIM] XBRL Dimensions 1.0
https://specifications.xbrl.org/spec-group-index-group-dimensions.html

[EFM] EDGAR Filer Manual, Volume II, sections 5.2.5 and 6 on Interactive Data
www.sec.gov/submit-filings/edgar-filer-manual

[EXG] EDGAR XBRL Guide
www.sec.gov/submit-filings/technical-specifications#xbrl

[STX] EDGAR Standard Taxonomies
www.sec.gov/data-research/taxonomies

[XBRL] XBRL 2.1
https://specifications.xbrl.org/work-product-index-group-base-spec-base-spec.html

10 APPENDIX: CONCEPT REFERENCES

10.1 Cybersecurity Risk Management, Strategy and Governance Disclosure

label	references	name
Cybersecurity Risk Management, Strategy, and Governance [Abstract]	Regulation S-K 106, Form 20-F 16K	CybersecurityRiskManagementStrategyAndGovernanceAbstract
Cybersecurity Risk Management, Strategy, and Governance [Table]	Regulation S-K 106, Form 20-F 16K	CybersecurityRiskManagementStrategyAndGovernanceTable
Cybersecurity Risk Management, Strategy, and Governance [Line Items]	Regulation S-K 106, Form 20-F 16K	CybersecurityRiskManagementStrategyAndGovernanceLineItems
Cybersecurity Risk Management Processes for Assessing, Identifying, and Managing Threats [Text Block]	Regulation S-K 106 (b)(1), Form 20-F 16K (b)(1)	CybersecurityRiskManagementProcessesForAssessingIdentifyingAndManagingThreatsTextBlock
Cybersecurity Risk Management Processes Integrated [Flag]	Regulation S-K 106 (b)(1)(i), Form 20-F 16K (b)(1)(i)	CybersecurityRiskManagementProcessesIntegratedFlag
Cybersecurity Risk Management Processes Integrated [Text Block]	Regulation S-K 106 (b)(1)(i), Form 20-F 16K (b)(1)(i)	CybersecurityRiskManagementProcessesIntegratedTextBlock
Cybersecurity Risk Management Third Party Engaged [Flag]	Regulation S-K 106 (b)(1)(ii), Form 20-F 16K (b)(1)(ii)	CybersecurityRiskManagementThirdPartyEngagedFlag
Cybersecurity Risk Third Party Oversight and Identification Processes [Flag]	Regulation S-K 106 (b)(1)(iii), Form 20-F 16K (b)(1)(iii)	CybersecurityRiskThirdPartyOversightAndIdentificationProcessesFlag
Cybersecurity Risk Materially Affected or Reasonably Likely to Materially Affect Registrant [Flag]	Regulation S-K 106 (b)(2), Form 20-F 16K (b)(2)	CybersecurityRiskMateriallyAffectedOrReasonablyLikelyToMateriallyAffectRegistrantFlag
Cybersecurity Risk Materially Affected or Reasonably Likely to Materially Affect Registrant [Text Block]	Regulation S-K 106 (b)(2), Form 20-F 16K (b)(2)	CybersecurityRiskMateriallyAffectedOrReasonablyLikelyToMateriallyAffectRegistrantTextBlock
Cybersecurity Risk Board of Directors Oversight [Text Block]	Regulation S-K 106 (c)(1), Form 20-F 16K (c)(1)	CybersecurityRiskBoardOfDirectorsOversightTextBlock
Cybersecurity Risk Board Committee or Subcommittee Responsible for Oversight [Text Block]	Regulation S-K 106 (c)(1), Form 20-F 16K (c)(1)	CybersecurityRiskBoardCommitteeOrSubcommitteeResponsibleForOversightTextBlock
Cybersecurity Risk Process for Informing Board Committee or Subcommittee Responsible for Oversight [Text Block]	Regulation S-K 106 (c)(1), Form 20-F 16K (c)(1)	CybersecurityRiskProcessForInformingBoardCommitteeOrSubcommitteeResponsibleForOversightTextBlock
Cybersecurity Risk Role of Management [Text Block]	Regulation S-K 106 (c)(2), Form 20-F 16K (c)(2)	CybersecurityRiskRoleOfManagementTextBlock
Cybersecurity Risk Management Positions or Committees Responsible [Flag]	Regulation S-K 106 (c)(2)(i), Form 20-F 16K (c)(2)(i)	CybersecurityRiskManagementPositionsOrCommitteesResponsibleFlag
Cybersecurity Risk Management Positions or Committees Responsible [Text Block]	Regulation S-K 106 (c)(2)(i), Form 20-F 16K (c)(2)(i)	CybersecurityRiskManagementPositionsOrCommitteesResponsibleTextBlock
Cybersecurity Risk Management Expertise of Management Responsible [Text Block]	Regulation S-K 106 (c)(2)(i), Form 20-F 16K (c)(2)(i)	CybersecurityRiskManagementExpertiseOfManagementResponsibleTextBlock
Cybersecurity Risk Process for Informing Management or Committees Responsible [Text Block]	Regulation S-K 106 (c)(2)(ii), Form 20-F 16K (c)(2)(ii)	CybersecurityRiskProcessForInformingManagementOrCommitteesResponsibleTextBlock

label	references	name
Cybersecurity Risk Management Processes for Assessing, Identifying, and Managing Threats [Text Block]	Regulation S-K 106 (b)(1), Form 20-F 16K (b)(1)	CybersecurityRiskManagement-ProcessesForAssessingIdentifying-AndManagingThreatsTextBlock

10.2 Cybersecurity Incident Disclosure

label	references	concept
Material Cybersecurity Incident [Abstract]	Form 8-K 1.05, Form 6-K General Instruction B	MaterialCybersecurityIncident-Abstract
Material Cybersecurity Incident [Table]	Form 8-K 1.05, Form 6-K General Instruction B	MaterialCybersecurityIncident-Table
Material Cybersecurity Incident [Axis]	Form 8-K 1.05, Form 6-K General Instruction B	MaterialCybersecurityIncident-Axis
Material Cybersecurity Incident [Domain]	Form 8-K 1.05, Form 6-K General Instruction B	MaterialCybersecurityIncident-Domain
Material Cybersecurity Incident [Line Items]	Form 8-K 1.05(a), Form 6-K General Instruction B	MaterialCybersecurityIncident-LineItems
Material Cybersecurity Incident Nature [Text Block]	Form 8-K 1.05(a), Form 6-K General Instruction B	MaterialCybersecurityIncident-NatureTextBlock
Material Cybersecurity Incident Scope [Text Block]	Form 8-K 1.05(a), Form 6-K General Instruction B	MaterialCybersecurityIncident-ScopeTextBlock
Material Cybersecurity Incident Timing [Text Block]	Form 8-K 1.05(a), Form 6-K General Instruction B	MaterialCybersecurityIncident-TimingTextBlock
Material Cybersecurity Incident Material Impact or Reasonably Likely Material Impact [Text Block]	Form 8-K 1.05(a), Form 6-K General Instruction B	MaterialCybersecurityIncident-MaterialImpactOrReasonably-LikelyMaterialImpactTextBlock
Material Cybersecurity Incident Information Not Available or Undetermined [Text Block]	Form 8-K 1.05 Instruction 2, Form 6-K General Instruction B	MaterialCybersecurityIncident-InformationNotAvailableOr-UndeterminedTextBlock

11 CHANGE LOG

June 24, 2024	Public draft
August, 2024	*Substantive changes* • To distinguish the relevant disclosure requirement, adjusted all standard labels so that concepts either start with "Cybersecurity Risk" or "Material Cybersecurity Incident". • Removed enclosing text block for material incident disclosure to reduce the need for "nested" markup. • Removed terse labels from the taxonomy and guide. • Added section regarding custom concepts. Updates and errata • Updated web site references to conform to current sec.gov URLs • Updated formatting to current taxonomy guide conventions.

March, 2026	• Update from 2024 to 2026 taxonomy URI and URLs. • Update cross-references to EFM and EXG sections.