Cybersecurity Disclosure Taxonomy Guide DRAFT

June 24, 2024

CONTENTS

1 Goal ... 1
2 Audience ... 2
3 Status ... 2
4 Instance document content ... 2
5 Physical Location and Organization ... 2
5.1 Versioning ... 2
5.2 Imports ... 3
6 Tables, Axes, and Members ... 3
6.1 Zero-axis Tables ... 5
6.1.1 Sample facts with zero axes ... 5
6.1.2 Cybersecurity Risk Management, Strategy, and Governance Disclosure ... 6
6.2 Single-axis Tables ... 8
6.2.1 Cybersecurity Incident Disclosure, by Incident ... 8
7 Presentation and Label Links ... 9
8 References ... 9
9 Appendix: Concept References ... 10
9.1 Cybersecurity Risk Management, Strategy and Governance Disclosure ... 10
9.2 Cybersecurity Incident Disclosure ... 11

FIGURES

Figure 1. Taxonomy files, by type ... 3
Figure 2. Taxonomy file import relationships ... 3
Figure 3. Namespace URI's and prefixes. ... 3
Figure 4. Font and Color-Coding Legend ... 4
Figure 5. Example showing presentation of eight text facts with a single taxonomy-defined dimension ... 4
Figure 6. Example showing different presentation of the same eight text facts ... 4
Figure 7. Example showing another alternative presentation of the same eight text facts ... 5
Figure 8. Sample facts in a CYD instance ... 5
Figure 9. Definition linkbase relationships in zero-axis Cybersecurity Risk Management, Strategy, and Governance Disclosure role ... 6
Figure 10. Fragment of Regulation S-K (17 CFR 229) Item 106 ... 7
Figure 11. Example showing sample facts for a single period ... 7
Figure 12. Form 8-K Item 1.05(a) ... 8
Figure 13. Definition links in the Material Cybersecurity Incidents role, with example custom members. ... 8
Figure 14. Example of facts in the Cybersecurity Incidents table ... 9

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.

Please provide any comments on the Cybersecurity Disclosure (CYD) Taxonomy Guide via email to StructuredData (at) sec.gov and include "CYD Taxonomy Guide" in the "General Subject Matter" section.

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 is a draft. Technical details may change between this draft and the final version to be published upon its implementation in EDGAR. For example, element names may change to become more explicit or compact. 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 draft taxonomy is specifically at the base URL

```
https://xbrl.sec.gov/cyd/2024/
```

There is a zip file containing all files located at

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

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/2024` with standard prefix `cyd`.

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

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.

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/2024	cyd-af-2024.xsd cyd-cr-2024.xsd cyd-af-sub-2024.xsd cyd-8k-sub-2024.xsd cyd-6k-sub-2024.xsd cyd-2024.xsd		cyd-entire-2024.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].

Figure 2. Taxonomy file import relationships

Name	Description
cyd-2024.xsd	Root schema with concepts and reference links.
↖ cyd-af-2024.xsd	Entry point with definition links for submission set AF
↖ cyd-af-sub-2024.xsd	Entry point with presentation and label links for submission set AF
↖ cyd-cr-2024.xsd	Entry point with definition links for current reports
↖ cyd-6k-sub-2024.xsd	Entry point with presentation links for submission set 6K
↖ cyd-8k-sub-2024.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	Namespace URI
cyd	http://xbrl.sec.gov/cyd/2024

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			
		Nature of Material Cybersecurity Incident	Scope of Material Cybersecurity Incident	Timing of Material Cybersecurity Incident	Material Impact of Cybersecurity Incident
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	Nature of Material Cybersecurity Incident	…text…	…text…
	Scope of Material Cybersecurity Incident	…text…	…text…
	Timing of Material Cybersecurity Incident	…text…	…text…
	Material Impact of Cybersecurity Incident	…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:

[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.

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	Nature of Material Cybersecurity Incident	…text…
			Scope of Material Cybersecurity Incident	…text…
			Timing of Material Cybersecurity Incident	…text…
			Material Impact of Cybersecurity Incident	…text…
	Incident B	Concepts Dimension	Nature of Material Cybersecurity Incident	…text…
			Scope of Material Cybersecurity Incident	…text…
			Timing of Material Cybersecurity Incident	…text…
			Material Impact of Cybersecurity Incident	…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`, Investment Company Type `dei:EntityInvCompanyType`, or that only appear once on a filing cover page, such as its Form type `dei:DocumentType` or the Company "Conformed" name `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 effectively define a zero-axis table for every EDGAR XBRL document [EXG]. 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 relationships 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
Processes for Assessing, Identifying, and Managing Material Risks from Cybersecurity Threats [Text Block]	Text Block	domain-member
Cybersecurity Risk Management Processes Integrated [Flag]	Boolean	domain-member
How Cybersecurity Risk Management Processes are Integrated [Text Block]	Text Block	domain-member
Cybersecurity Risk Management Third Party Engaged [Flag]	Boolean	domain-member
Cybersecurity Third Party Risk Oversight and Identification Processes [Flag]	Boolean	domain-member
Cybersecurity Risk Materially Affected or Reasonably Likely to Affect Registrant [Flag]	Boolean	domain-member
Cybersecurity Risk Materially Affected or Reasonably Likely to Affect Registrant [Text Block]	Text Block	domain-member
Board Oversight of Cybersecurity Risk [Text Block]	Text Block	domain-member
Board Committee or Subcommittee Responsible for Cybersecurity Risk Oversight [Text Block]	Text Block	domain-member
Process for Informing Board Committee or Subcommittee of Cybersecurity Risk [Text Block]	Text Block	domain-member
Management Role in Assessment and Management of Material Risks from Cybersecurity Threats [Text Block]	Text Block	domain-member
Management Position or Committee Responsible for Cybersecurity Risk [Flag]	Boolean	domain-member
Management Position or Committee Responsible for Cybersecurity Risk [Text Block]	Text Block	domain-member
Expertise of Management Position or Committee Responsible for Cybersecurity Risk [Text Block]	Text Block	domain-member
Process for Monitoring and Informing Management of Cybersecurity Incidents [Text Block]	Text Block	domain-member
Cybersecurity Risk Management Strategy and Governance [Text Block]	Text Block	domain-member
Management Position or Committee for Cybersecurity Risk Reports 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 12 quotes Item 229.106(b) (risk management and strategy) as an example.

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

> (b) Risk management and strategy. 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:
>
> (1) Whether and how any such processes have been integrated into the registrant's overall risk management system or processes;

The disclosure in Figure 10 requires a narrative, which is represented by text block concept **`cyd:CybersecurityRiskProcessTextBlock`**. Within that disclosure, the Boolean flag **`cyd:CybersecurityRiskProcessIntegratedFlag`** represents "whether" the processes have been integrated, and assuming that value is "true", then the text block **`cyd:CybersecurityRiskProcessIntegratedTextBlock`** 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	**CybersecurityRiskProcessTextBlock**	…**text**…
	CybersecurityRiskProcessIntegratedFlag	**true**
	CybersecurityRiskProcessIntegratedTextBlock	…**text**…
	CybersecurityThirdPartyOversightAndIdentificationProcessFlag	**false**
	CybersecurityRiskMateriallyAffectedFlag	**true**
	CybersecurityRiskMateriallyAffectedTextBlock	…**text**…
	CybersecurityRiskBoardOversightTextBlock	…**text**…
	CybersecurityRiskBoardOversightResponsiblePartyTextBlock	…**text**…
	CybersecurityRiskAssessmentManagementRoleTextBlock	…**text**…
	CybersecurityRiskManagementResponsiblePartyFlag	**true**
	CybersecurityRiskResponsiblePartyTextBlock	…**text**…
	CybersecurityIncidentMonitorAndReportToManagementProcessTextBlock	…**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 **`CybersecurityRiskManagementStrategyAndGovernanceLineItems`** 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="CybersecurityRiskManagementResponsiblePartyFlag" 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="CybersecurityRiskManagementResponsiblePartyFlag" 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 its 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 (see EFM 6.7) the filer defines a custom domain member, then makes it a domain-member child of the standard concept `MaterialCsybersecurityIncidentDomain`. 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/MaterialCybersecurityIncidentDisclosure`, 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 [Member]	Custom Member	domain-member
Second Incident [Member]	Custom Member	domain-member
Material Cybersecurity Incident [Line Items]	Abstract Line Items	domain-member
Material Cybersecurity Incident [Text Block]	Text Block	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 [Text Block]	Text Block	domain-member
Material Cybersecurity Incident Material Impact on Financial Condition [Flag]	Boolean	domain-member
Material Cybersecurity Incident Material Impact on Results of Operations [Flag]	Boolean	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
`MaterialCybersecurityIncidentNatureTextBlock`	`cik:0000012345`	`2030-09-13/2030-09-13`	`e01:FirstIncidentMember`	…text…
`MaterialCybersecurityIncidentScopeTextBlock`	`cik:0000012345`	`2030-09-13/2030-09-13`	`e01:FirstIncidentMember`	…text…
`MaterialCybersecurityIncidentTimingTextBlock`	`cik:0000012345`	`2030-09-13/2030-09-13`	`e01:FirstIncidentMember`	…text…
`MaterialCybersecurityIncidentMaterialImpactTextBlock`	`cik:0000012345`	`2030-09-13/2030-09-13`	`e01:SecondIncidentMember`	…text…
`MaterialCybersecurityIncidentMaterialImpactOnFinancialConditionFlag`	`cik:0000012345`	`2030-09-13/2030-09-13`	`e01:SecondIncidentMember`	`false`
`MaterialCybersecurityIncidentMaterialImpactOnResultsOfOperationsFlag`	`cik:0000012345`	`2030-09-13/2030-09-13`	`e01:SecondIncidentMember`	`false`

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

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.[3] 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 financials statement submissions. Entry point **`cyd-af-sub`** provides them for filers wish to use them nonetheless.

8 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/edgar/filer-information
[EXG]	EDGAR XBRL Guide www.sec.gov/edgar/filer-information
[STX]	EDGAR Standard Taxonomies www.sec.gov/edgar/information-for-filers/standard-taxonomies
[XBRL]	XBRL 2.1 https://specifications.xbrl.org/work-product-index-group-base-spec-base-spec.html

[3] Unlike taxonomies such as OEF, there are currently no sections of [EXG] specific to submissions that use the CYD taxonomy.

9 APPENDIX: CONCEPT REFERENCES

9.1 Cybersecurity Risk Management, Strategy and Governance Disclosure

terse 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**
Risk process	Regulation S-K 106 (b)(1), Form 20-F 16K (b)(1)	**CybersecurityRiskProcessTextBlock**
Is risk process integrated?	Regulation S-K 106 (b)(1)(i), Form 20-F 16K (b)(1)(i)	**CybersecurityRiskProcessIntegratedFlag**
Risk process integration	Regulation S-K 106 (b)(1)(i), Form 20-F 16K (b)(1)(i)	**CybersecurityRiskProcessIntegratedTextBlock**
Does management engage a third party?	Regulation S-K 106 (b)(1)(ii), Form 20-F 16K (b)(1)(ii)	**CybersecurityThirdPartyEngagedFlag**
Is there a third party risk oversight and identification process?	Regulation S-K 106 (b)(1)(iii), Form 20-F 16K (1)(iii)	**CybersecurityThirdPartyRiskOversightAndIdentificationProcessFlag**
Have the risks materially affected or are they reasonably likely to materially affect the registrant?	Regulation S-K 106 (b)(2), Form 20-F 16K (b)(2)	**CybersecurityRiskMateriallyAffectedOrReasonablyLikelyToAffectFlag**
Material effects from risks	Regulation S-K 106 (b)(2), Form 20-F 16K (b)(2)	**CybersecurityRiskMateriallyAffectedOrReasonablyLikelyToAffectTextBlock**
Board oversight of risk	Regulation S-K 106 (c)(1), Form 20-F 16K (c)(1)	**CybersecurityRiskBoardOversightTextBlock**
Committee or subcommittee responsible for board oversight of risk	Regulation S-K 106 (c)(1), Form 20-F 16K (c)(1)	**CybersecurityRiskBoardOversightResponsibleCommitteeOrSubcommitteeTextBlock**
Process for informing board or committee of risk	Regulation S-K 106 (c)(1), Form 20-F 16K (c)(1)	**ProcessforInformingCommitteeorSubcommitteeAboutCybersecurityRisksTextBlock**
Management's role in risk assessment	Regulation S-K 106 (c)(2), Form 20-F 16K (c)(2)	**CybersecurityRiskAssessmentManagementRoleTextBlock**
Is management position or committee responsible for risk assessment and management?	Regulation S-K 106 (c)(2)(i), Form 20-F 16K (c)(2)(i)	**CybersecurityRiskManagementPositionOrCommitteeResponsibleFlag**
Management position or committee responsible for risk assessment	Regulation S-K 106 (c)(2)(i), Form 20-F 16K (c)(2)(i)	**CybersecurityRiskManagementPositionOrCommitteeResponsibleTextBlock**
Process for monitoring and informing management of incidents	Regulation S-K 106 (c)(2)(ii), Form 20-F 16K (c)(2)(ii)	**CybersecurityIncidentMonitorAndReportToManagementProcessTextBlock**
Management position or committee reports to board on cybersecurity risk?	Regulation S-K 106 (c)(2)(iii), Form 20-F 16K (c)(2)(iii)	**ManagementPositionorCommitteeForCybersecurityRiskReportstoBoardFlag**
Cybersecurity risk management strategy and governance	Regulation S-K 106, Form 20-F 16K	**CybersecurityRiskManagementStrategyAndGovernanceTextBlock**
Management expertise	Regulation S-K 106 (c)(2)(i), Form 20-F 16K (c)(2)(i)	**CybersecurityManagementExpertiseTextBlock**

9.2 Cybersecurity Incident Disclosure

terse label	references	concept
Material Cybersecurity Incident [Abstract]	Form 8-K 1.05(a), Form 6-K General Instruction B	**MaterialCybersecurityIncidentAbstract**
Material Cybersecurity Incident [Table]	Form 8-K 1.05(a), Form 6-K General Instruction B	**MaterialCybersecurityIncidentTable**
Material Cybersecurity Incident [Axis]	Form 8-K 1.05(a), Form 6-K General Instruction B	**MaterialCybersecurityIncidentAxis**
Material Cybersecurity Incident [Domain]	Form 8-K 1.05(a), Form 6-K General Instruction B	**MaterialCybersecurityIncidentDomain**
Material Cybersecurity Incident [Line Items]	Form 8-K 1.05(a), Form 6-K General Instruction B	**MaterialCybersecurityIncidentLineItems**
Incident Disclosure	Form 8-K 1.05(a), Form 6-K General Instruction B	**MaterialCybersecurityIncidentTextBlock**
Nature of Incident	Form 8-K 1.05(a), Form 6-K General Instruction B	**MaterialCybersecurityIncidentNatureTextBlock**
Scope of Incident	Form 8-K 1.05(a), Form 6-K General Instruction B	**MaterialCybersecurityIncidentScopeTextBlock**
Timing of Incident	Form 8-K 1.05(a), Form 6-K General Instruction B	**MaterialCybersecurityIncidentTimingTextBlock**
Material Impact of Incident	Form 8-K 1.05(a), Form 6-K General Instruction B	**MaterialCybersecurityIncidentMaterialImpactTextBlock**
Financial Condition Materially Impacted?	Form 8-K 1.05(a), Form 6-K General Instruction B	**MaterialCybersecurityIncidentMaterialImpactOnFinancialConditionFlag**
Results of Operations Materially Impacted?	Form 8-K 1.05(a), Form 6-K General Instruction B	**MaterialCybersecurityIncidentMaterialImpactOnResultsOfOperationsFlag**
Incident Information Not Available or Undetermined	Form 8-K 1.05 Instruction 2, Form 6-K General Instruction B	**MaterialCybersecurityIncidentInformationNotAvailableOrUndeterminedTextBlock**