

Technology Obsolescence Risk Guide

for the Financial Industry in Singapore



December 2025



Contents

1. Background	3
2. Key Definitions	4
2.1. System	4
2.1.1. Examples of IT components associated with a system	4
2.1.2. Examples of IT components within a shared infrastructure	4
2.2. Critical System	4
2.3. IT component	5
2.4. Extended Support	5
3. Obsolescence Common Term and Metric	6
3.1. No Obsolescence	6
3.1.1. General Availability (GA):	6
3.2. Obsoleting	7
3.2.1. EOS with Extended Support (EOES)	7
3.3. Obsolete	7
4. Technology Obsolescence Reporting Framework	8
4.1.1. System-Level Metrics	8
4.1.2. Component-Level Metrics	10
5. Appendix	122
1.1. Reporting Sample data	122
1.2. System Level Metric based on the sample data	133
1.3. Component Level Metric	155

1. Background

- 1.1. Financial institutions (FIs) actively manage technology obsolescence in IT systems and components, including hardware, software, operating systems, middleware, and applications.
- 1.2. Currently, different FIs adopt varying definitions and risk reporting approaches for Technology Obsolescence.
- 1.3. It is essential for all FIs and stakeholders to adopt a common, standards-based definition and approach to risk reporting. This will enhance alignment with industry benchmarks, foster collaboration among FIs, improve risk transparency, and support clearer communication with regulators, senior management, and boards through a shared, standards-based framework.
- 1.4. A joint working group with representatives from the ABS Standing Committee on Technology Risk and Resiliency (SCTRR) was formed to address the need. This guide represents the working group's collective effort to establish standardised reporting guidelines for technology obsolescence risk across FIs.
- 1.5. The target audience for this guide comprises ABS member banks. It establishes consensus on the foundational elements of the reporting guidelines, such as:
 - Key definitions
 - Common terms and metrics for technology obsolescence
 - Reporting framework

2. Key Definitions

2.1. System

A collection of IT components including hardware, software, operating systems (OS), middleware, and applications designed to support a specific business or enterprise function.

2.1.1. Examples of IT components associated with a system

A system can be a 'Business Application' such as Core Banking Applications, Payments Systems, Customer-Facing Internet Banking comprising of the following IT components:

- Hardware (e.g., servers)
- Appliances (hardware and firmware)
- Dedicated Hypervisor (e.g., VMWare)
- Operating Systems (e.g., Linux, Windows)
- Middleware (e.g., JBOSS, Connect Direct)
- Software (e.g., End-user Applications)
- Databases (e.g., Oracle, MariaDB)

2.1.2. Examples of IT components within a shared infrastructure

A system can be 'Shared Infrastructure' that supports a Business Application, such as:

- Shared Network (e.g. firewall, switches)
- Shared Storage (e.g., SAN, NAS, Cloud storage solutions)
- Shared Backup Platform (E.g., Dell EMC Data Domain, AWS Backup)
- Shared Hypervisor (e.g. VMWare)

2.2. Critical System

Critical System refers to a system that supports operations or services where a disruption could have a material impact on the following:

- The institution's ability to provide essential services to customers
- Customer confidence
- Regulatory obligations

Examples include core banking systems, Internet/Mobile banking application, payment processing application. FIs should refer to MAS Notice FSM-N05 for regulatory requirements on critical system identification.

2.3. IT component

All IT components essential for delivering the intended business or enterprise functions must be included in Technology Obsolescence assessments. Components that are not critical—such as peripheral devices or those used exclusively in development environments—may be excluded from the assessment.

Each FI is responsible for assessing the criticality of its IT components based on its specific operational and risk context.

2.4. Extended Support

Extended Support refers to the continued provision of patches or fixes by the vendor after the official End of Support (EOS) date. This is important because it helps mitigate security and operational risks associated with using technology that has reached EOS, ensuring essential systems remain secure and functional during the transition period.

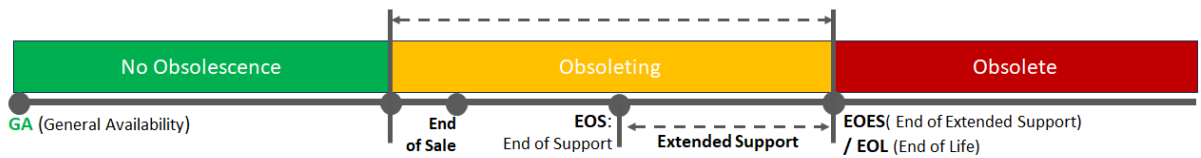
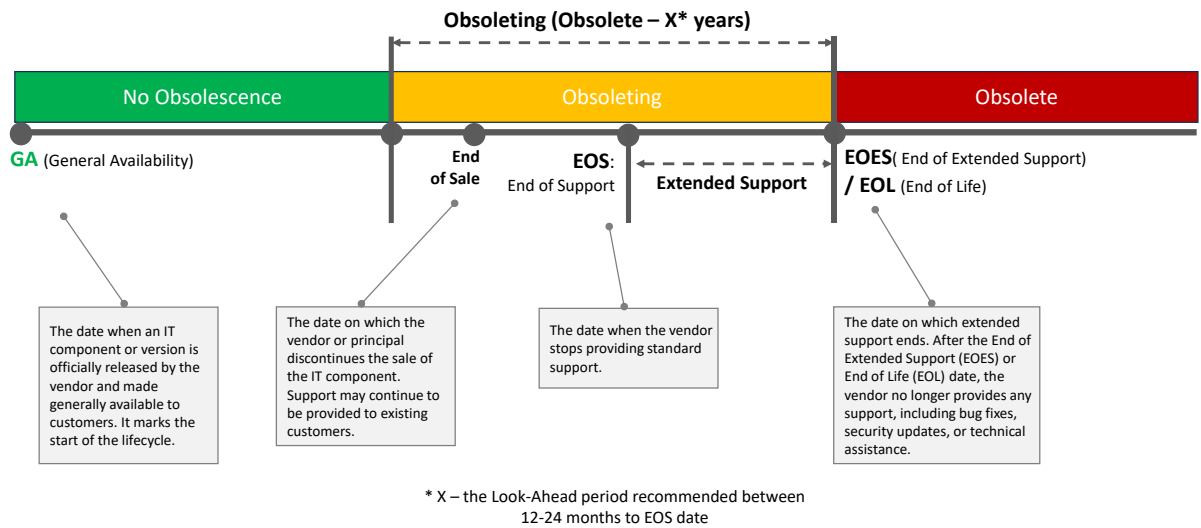
To qualify as Extended Support under the technology obsolescence guidelines, the vendor¹ must continue to provide patches or fixes for High and Critical² beyond the official End Of Support (EOS) date. Therefore, access solely to previously released bug fixes or best-effort support without ongoing provision of new patches does not qualify as Extended Support.

¹ The vendor may be either the original manufacturer of the IT components or a third party with the capability to deliver equivalent outcomes required for Extended Support.

² The definitions of "High" and "Critical" patches or fixes are determined based on the respective guidelines of each FI.

3. Obsolescence Common Term and Metric

This section aims to establish a common understanding of the terminology and metrics used to describe the *IT component lifecycle* within the context of Technology Obsolescence.



Common Term	GA	End of Sales	EOS with ES	End of Extended Support (EOES) / End of Life (EOL)
Description	IT component officially released with full support	IT component is no longer offered to new customers	Extended Support (ES) provided beyond the standard support period.	Extended support is not available; no further support or security patching will be provided.
Enhancement	Yes	No	No	No
Feature Bugfix	Yes	Yes (existing customers)	Limited	No
Vulnerability Bugfix	Yes	Yes (existing customers)	Critical / High	Goodwill based
Obsolete	No	No	No, if ES is provided for vulnerability and security patching which can be used to extend the obsolescence date	Yes
Risk	Still in Support			Obsolete (No Support)

* X - the Look-Ahead period recommended between 12-24 months to EOS date

3.1. No Obsolescence

'No Obsolescence' refers to the period during which an IT component remains under warranty support by the vendor, spanning from its General Availability (GA) date until it enters the 'Obsolescing' stage (see Section 3.2).

3.1.1. General Availability (GA):

The date when an IT component or version is officially released by the vendor and made generally available to customers, marking the start of the IT component lifecycle.

3.2. Obsoleteing

'Obsoleteing' refers to the forward-looking period that precedes the 'Obsolete' stage (see Section 3.3) of an IT component's lifecycle. During this stage, the FI is required to develop a technology refresh plan to remediate or replace the IT component before it reaches EOS. The recommended look-ahead period for identifying and addressing obsoleteing components is typically 18 to 24 months prior to the EOS date.

3.2.1. EOS with Extended Support (EOES)

EOS refers to the date on which a vendor ceases to provide standard support for an IT component under the standard support agreement. EOES refers to vendor support that is provided only through an extended support arrangement beyond the EOS date. Extended vendor support is typically offered under a separate contract that goes beyond the standard licensing terms.

3.3. Obsolete

'Obsolete' refers to the point at which an IT component is no longer supported by the vendor, whether through standard or extended support contracts. This includes the cessation of bug fixes, security updates, and technical assistance. No extended support is available or in place beyond this date, rendering the IT component fully unsupported. An IT component is considered obsolete when it reaches EOS or EOES, whichever occurs later.

4. Technology Obsolescence Reporting Framework

Technology obsolescence reporting is a critical component of managing operational risks associated with aging systems. It provides decision-makers with clear visibility into potential impacts on business services, enabling them to prioritize remediation efforts effectively.

Technology obsolescence reporting should be primarily performed at the system level to provide better alignment for managing obsolescence risk, as it reflects the level at which a business or service is delivered to customers. This approach facilitates clearer communication with senior management by presenting technology obsolescence risk in business-relevant terms rather than technical component details.

Critical systems classified under MAS Notice FSM-N05 and internet-facing systems pose elevated risk due to their operational importance and exposure to external threats and vulnerabilities. Therefore, additional metrics are necessary to provide management with enhanced visibility and risk mitigation for these systems.

4.1.1. System-Level Metrics

#	Metric	Scope	% or Count	Description
1a	Total number of Systems	All	Count	Total number of systems that are (1) hosted in and used by Singapore or, (2) hosted offshore but used by Singapore .
1b	Total number of Critical Systems	Critical Systems (FSM-N05)	Count	Total number of critical systems that are (1) hosted in and used by Singapore or, (2) hosted offshore but used by Singapore .
2a	Total % of System Obsolete (Critical and Non-Critical Systems)	All	% (2b+2c) / 1a	Percentage of systems currently operating with one or more obsolete IT components. If any IT component within a system is obsolete , the entire system is considered obsolete .
2b	Number of Critical Systems Obsolete	Critical Systems (FSM-N05)	Count	Number of critical systems currently operating with one or more obsolete* IT components. If any IT component within a system is obsolete , the entire system is considered obsolete .
2c	Number of Non-Critical Systems Obsolete	Non-Critical Systems	Count	Number of non-critical systems currently operating with one or more obsolete* IT components. If any IT component within a system is obsolete , the entire system is considered obsolete .
2d	Number of Critical Internet Facing Systems Obsolete	Critical Systems (FSM-N05)	Count	Number of critical internet-facing systems currently operating with one or more obsolete IT components. This is a subset of critical systems obsolete (2b)
2e	Number of Non-Critical Internet Facing Systems Obsolete	Non-Critical Systems	Count	Number of non-critical internet-facing systems currently operating with one or more obsolete IT components. This is a subset of non-critical systems obsolete (2c)

#	Metric	Scope	% or Count	Description
3a	% of System Obsoleting (Critical and Non-Critical Systems)	All	% (3b+3c) /1a	Percentage of systems currently operating with one or more obsoleting IT components. If any IT component within a system is obsoleting , the entire system is considered obsoleting
3b	Number of Critical Systems Obsoleting	Critical Systems (FSM-N05)	Count	Number of critical systems currently operating with one or more obsoleting IT components. If any IT component within a system is obsoleting , the entire system is considered obsoleting .
3c	Number of Non-Critical Systems Obsoleting	Non-Critical Systems	Count	Number of non-critical systems currently operating with one or more obsoleting IT components. If any IT component within a system is obsoleting , the entire system is considered obsoleting .
3d	Number of Critical Internet Facing Systems Obsoleting	Critical Internet Facing Systems (FSM-N05)	Count	Number of critical internet-facing systems currently operating with one or more obsoleting IT components. This is a subset of critical systems obsoleting (3b) .
3e	Number of Non-Critical Internet Facing Systems Obsoleting	Non-Critical Internet Facing Systems	Count	Number of non-critical internet-facing systems currently operating with one or more obsoleting IT components. This is a subset of non-critical systems obsoleting (3c)

Note:

- Systems within scope are defined as those that are either (1) hosted in and used within Singapore, or (2) hosted offshore but used by Singapore.
- If a system includes a mix of “obsolete”, “obsoleting”, and “no obsolescence” IT components, the status “obsolete” shall take precedence. Accordingly, the system will be classified as “obsolete”.
- If a system includes both “obsoleting” and “no obsolescence” IT components, the status “obsoleting” shall take precedence. Accordingly, the system will be classified as “obsoleting”.
- A system will be classified as “no obsolescence” if it contains neither obsolete nor obsoleting IT components.

4.1.2. Component-Level Metrics

While the system-level metrics remain the primary measure of technology obsolescence, component-level metrics provides an additional perspective that complements the overall measurement.

#	Metric	Scope	% or Count	Description
4a	Total number of IT Components	All	Count	Total number of IT components deployed across critical and non-critical systems.
4b	Number of IT Components Obsolete	All	Count	Number of obsolete IT components deployed across critical and non-critical systems.
4c	% of IT Components Obsolete	All	% 4b/4a	Percentage of obsolete IT components deployed across critical and non-critical systems, that are (1) hosted in and used by Singapore or, (2) hosted offshore but used by Singapore.
4d	Number of IT Components Obsoleting	All	Count	Number of obsoleting IT components deployed across critical and non-critical systems.
4e	% of IT Components Obsoleting	All	% 4d/4a	Percentage of obsoleting IT components deployed across critical and non-critical systems

Acknowledgement

This guideline is developed by the Technology Obsolescence working group members from the following FIs:

1. DBS Bank Ltd (Working Group Lead)
2. United Overseas Bank Limited (Working Group Lead)
3. Maybank Singapore Limited (Working Group Lead)
4. OCBC Bank
5. ANZ
6. Bank of America (BOA)
7. Citibank
8. HSBC Bank (Singapore) Limited
9. MUFG Bank Ltd
10. Standard Chartered Bank (SCB)
11. Sumitomo Mitsui Banking Corporation (SMBC)
12. JP Morgan
13. SGX

In addition, the paper was completed with the guidance and support of:

1. ABS Standing Committee on Technology Risk & Resilience (SCTRR)

5. Appendix

1.1. Reporting Sample data

- Note: The data shown is for illustrative purposes only and represents mock-up content.

Systems Supported	Critical System?	Type	Vendor	Product	Version	Quantity	EOS/ES Date	Internet Facing?	Status
Consumer Finance	Yes	OS/Firmware	IBM	Aix	AIX 7.2 TL5	2	Not Announced	No	No Obsolescence
Consumer Finance	Yes	Application	IBM	WebSphere	WebSphere 8.5	7	Not Announced	No	No Obsolescence
Blockchain & Distributed Ledger	No	OS/Firmware	Microsoft	Windows	Windows 2016	4	12/01/2027	No	No Obsolescence
Blockchain & Distributed Ledger	No	Application	IBM	MQ	MQ 9.3	4	22/01/2026	No	Obsoleting
Blockchain & Distributed Ledger	No	OS/Firmware	Redhat	OpenShift	Openshift 4.14	26	31/10/2025	No	Obsoleting
Blockchain & Distributed Ledger	No	OS/Firmware	Redhat	Linux	RHEL 8	4	31/05/2029	Yes	No Obsolescence
ATM	Yes	Application	Redhat	JBOSS	JBOSS 7.4	7	30/06/2025	Yes	Obsoleting
ATM	Yes	OS/Firmware	Redhat	Linux	RHEL 8	4	31/05/2029	Yes	No Obsolescence
Digital Bank	Yes	Application	IBM	WebSphere	WebSphere 8.5	7	Not Announced	Yes	No Obsolescence
Digital Bank	Yes	Application	Redhat	JBOSS	JBOSS 6.4	38	30/05/2025	Yes	Obsolete
Branch	Yes	Application	Microsoft	MSSQL	MSSQL V2016	8	14/07/2026	No	Obsoleting
Branch	Yes	Application	Microsoft	MSSQL	MSSQL V2019	8	8/01/2030	No	No Obsolescence
Branch	Yes	OS/Firmware	Microsoft	Windows	Windows 2016	4	12/01/2027	No	No Obsolescence
Branch	Yes	Application	IBM	Connect Direct	Connect Direct 6.1	4	30/04/2026	No	Obsoleting
Core Banking	Yes	OS/Firmware	Redhat	Linux	RHEL 7	7	30/06/2026	No	Obsoleting
Core Banking	Yes	OS/Firmware	Redhat	Linux	RHEL 6	7	30/06/2025	No	Obsolete
Core Banking	Yes	Application	Redhat	JBOSS	JBOSS 7.4	7	30/06/2026	No	Obsoleting
Network	Yes	OS/Firmware	Cisco	Cisco IOS Switch	17.09.05	172	31/03/2027	No	No Obsolescence
Network	Yes	OS/Firmware	Cisco	Cisco Router	17.09.05a	462	31/03/2027	No	No Obsolescence
Network	Yes	Hardware	Arista	Arista Switch	DCS-7508N	2	Not Announced	No	No Obsolescence
Enterprise Risk	No	Application	Microsoft	MSSQL	MSSQL V2022	5	11/01/2033	No	No Obsolescence
						789			

1.2. System Level Metric based on the sample data

Note: The data shown is for illustrative purposes only and represents mock-up content.

#	Metric	Scope	% or Count	Value	Description
1a	Total number of Systems	All	Count	8	Total number of systems that are (1) hosted in and used by Singapore or, (2) hosted offshore but used by Singapore.
1b	Total number of Critical Systems	Critical Systems (FSM-N05)	Count	6	Total number of critical systems that are (1) hosted in and used by Singapore or, (2) hosted offshore but used by Singapore.
2a	% of System Obsolete (Critical and Non-Critical Systems)	All	% (2b+2c) / 1a	25% (2/8)	Percentage of systems currently operating with one or more obsolete IT components. If any IT component within a system is obsolete, the entire system is considered obsolete.
2b	Number of Critical Systems Obsolete	Critical Systems (FSM-N05)	Count	2	Number of critical systems currently operating with one or more obsolete* IT components. If any IT component within a system is obsolete, the entire system is considered obsolete.
2c	Number of Non-Critical Systems Obsolete	Non-Critical Systems	Count	0	Number of non-critical systems currently operating with one or more obsolete* IT components. If any IT component within a system is obsolete, the entire system is considered obsolete.
2d	Number of Critical Internet Facing Systems Obsolete	Critical Systems (FSM-N05)	Count	1	Number of critical internet-facing systems currently operating with one or more obsolete IT components. This is a subset of critical systems obsolete (2b)
2e	Number of Non-Critical Internet Facing Systems Obsolete	Non-Critical Systems	Count	0	Number of non-critical internet-facing systems currently operating with one or more obsolete IT components. This is a subset of non-critical systems obsolete (2c)

Note:

- Systems within scope are defined as those that are either (1) hosted in and used within Singapore, or (2) hosted offshore but used by Singapore.
- If a system includes a mix of “obsolete”, “obsoleting”, and “no obsolescence” IT components, the status “obsolete” shall take precedence. Accordingly, the system will be classified as “obsolete”.
- If a system includes both “obsoleting” and “no obsolescence” IT components, the status “obsoleting” shall take precedence. Accordingly, the system will be classified as “obsoleting”.
- A system will be classified as “no obsolescence” if it contains neither obsolete nor obsoleting IT components.

#	Metric	Scope	% or Count	Value	Description
3a	% of System Obsolescing (Critical and Non-Critical Systems)	All	% (3b+3c) /1a	38% (3/8)	Percentage of systems currently operating with one or more obsolescing IT components. If any IT component within a system is obsolescing , the entire system is considered obsolescing
3b	Number of Critical Systems Obsolescing	Critical Systems (FSM-N05)	Count	2	Number of critical systems currently operating with one or more obsolescing IT components. If any IT component within a system is obsolescing , the entire system is considered obsolescing .
3c	Number of Non-Critical Systems Obsolescing	Non-Critical Systems	Count	1	Number of non-critical systems currently operating with one or more obsolescing IT components. If any IT component within a system is obsolescing , the entire system is considered obsolescing .
3d	Number of Critical Internet Facing Systems Obsolescing	Critical Internet Facing Systems (FSM-N05)	Count	1	Number of critical internet-facing systems currently operating with one or more obsolescing IT components. This is a subset of critical systems obsolescing (3b) .
3e	Number of Non-Critical Internet Facing Systems Obsolescing	Non-Critical Internet Facing Systems	Count	0	Number of non-critical internet-facing systems currently operating with one or more obsolescing IT components. This is a subset of non-critical systems obsolescing (3c)

1.3. Component Level Metric

#	Metric	Scope	% or Count	Value	Description
4a	Total number of IT Components	All	Count	789	Total number of IT components deployed across critical and non-critical systems.
4b	Number of IT Components Obsolete	All	Count	45	Number of obsolete IT components deployed across critical and non-critical systems.
4c	% of IT Components Obsolete	All	% 4d/4c	5.70%	Percentage of obsolete IT components deployed across critical and non-critical systems
4d	Number of IT Components Obsoleting	All	Count	63	Number of obsoleting IT components deployed across critical and non-critical systems.
4e	% of IT Components Obsoleting	All	% 4e/4c	7.98%	Percentage of obsoleting IT components deployed across critical and non-critical systems