This is a guidance box. Remove all guidance boxes after filling out the template. Items highlighted in turquoise should be edited appropriately. After all edits have been made, all highlights should be cleared.

Insert organization logo by clicking on the placeholder to the left.

Cybersecurity Event Logs and Monitoring Management Standard Template

Choose Classification

DATE: Click here to add date
VERSION: Click here to add text
REF: Click here to add text

Replace <organization name> with the name of the organization for the entire document. To do so, perform the following

- Press "Ctrl" + "H" keys simultaneously
- Enter "<organization name>" in the Find text box
- Enter your organization's full name in the "Replace" text box
- Click "More", and make sure "Match case" is ticked
- Click "Replace All"
- Close the dialog box.

Disclaimer

This template has been developed by the National Cybersecurity Authority (NCA) as an illustrative example that can be used by organizations as a reference and guide. This template must be customized and aligned with the <organization name>'s business and relevant legislative and regulatory requirements. This template must be approved by the head of the organization (Authorizing official) or his/her delegate. The NCA is not responsible for any use of this template as is, and it affirms that this template is solely an illustrative example.

Document Approval

Role	Job Title	Name	Date	Signature
Choose Role	<Insert job title>	<Insert individual's full personnel name>	Click here to add date	<Insert signature>

Version Control

Version	Date	Updated By	Version Details
<Insert version number>	Click here to add date	<Insert individual's full personnel name>	<Insert description of the version>

Review Table

Periodical Review Rate	Last Review Date	Upcoming Review Date
<Once a year>	Click here to add date	Click here to add date

Table of Contents

Purpose

This Standard aims to define the detailed cybersecurity requirements for cybersecurity event logs and monitoring management of <organization name> to achieve the main objective of this Standard which is minimizing cybersecurity risks resulting from internal and external threats at <organization name>.

The requirements in this standard are aligned with the Cybersecurity Event Logs and Monitoring Management Policy and the cybersecurity requirements issued by the National Cybersecurity Authority (NCA) including but not limited to (ECC-1:2018) and (CSCC-1:2019), in addition to other related cybersecurity legal and regulatory requirements.

Scope

This standard covers all <organization name> cybersecurity event logs and monitoring management and applies to all personnel (employees and contractors) in the <organization name>. This standard must follow the NCA’s operating model for cybersecurity operation centers and NCA’s regulatory cybersecurity requirements.

Standards

1	Log Format
Objective	To enforce a standard and consistent log format including all the required information.
Risk Implication	If logs are recorded on an inconsistent basis, it may be difficult to compare multiple different logs. This leads to a higher risk of misinformation, thus potentially making security incidents more challenging to remediate.
Requirements	
1-1	Events log format must include:

	1-1-1 **Event Log Type:** Such as System, Security, Audit, Kernel, Authorization, Mail, etc. 1-1-2 **Location** of the event or source/system of the log. 1-1-3 **Date** and **Timestamp** of the event log. 1-1-4 **Event Status:** Success, Failure, Up, Down, Allow, Deny, etc. 1-1-5 **Event Severity:** Emergency, Alert, Critical, Error, Warning, Notice, Informational, etc. 1-1-6 **Event Message:** Actual message of the event.
1-2	Additional details must be included in logs wherever applicable, such as user, source address/port, destination address/port, and other useful elements.
2	Timestamps - Synchronized Redundant Time Servers
Objective	To enforce a credible system for internal information and technology assets.
Risk Implication	If logs are recorded on an inconsistent basis, it may be difficult to compare multiple different logs. This leads to a higher risk of misinformation, thus potentially making security incidents more challenging to remediate.
Requirements	
2-1	The information and technology assets must be synchronized with three redundant central time servers within milliseconds from a trusted synchronization source.
3	Event Logging
Objective	

	To ensure that cybersecurity incidents and unauthorized activity in the environment do not go undocumented and unnoticed.
Risk Implication	It is important to record main events executed in the environment. If fails to log the specified events in the control requirements, this would lead to an increased risk of unidentified and possible unauthorized events occurring in the environment, which could cause potential business impact depending on the severity of the incident.
Requirements	
3-1	All the events specified under these control requirements must be logged: 3-1-1 Successful login attempts. 3-1-2 Unsuccessful login attempts, along with the identification of whether the login attempt involved an invalid password. 3-1-3 All logoffs. 3-1-4 Additions, deletions and modifications to user accounts/privileges. 3-1-5 Users switching IDs during an online session. 3-1-6 Attempts to perform unauthorized functions. 3-1-7 Activities performed by privileged accounts. 3-1-8 Modifications to system settings (parameters). 3-1-9 Read or write access to protected information, where there is a potential for theft of that information. 3-1-10 Exfiltration of materials related to classified information outside <organization name>. 3-1-11 Detections in inbound and outbound communications for unusual or unauthorized activities including the detection of malware (such as malicious code, spyware, and adware). 3-1-12 Additions, deletions and modifications to security/audit log parameters.

	3-1-13 Faults (technical problems in information and technology assets) that could potentially be attributed to a security event. 3-1-14 Activation or deactivation of activities by a specific service. 3-1-15 System crashes or restarts. 3-1-16 Password changes. 3-1-17 Enablement of all critical systems logs.
4	Event Sources
Objective	Ensure all <organization name>'s information and technology assets event logs are monitored to identify unauthorized network activity that may indicate a security incident.
Risk Implication	Failure to detect unauthorized activity will prevent to respond to suspicious events appropriately before they expand into a greater security incident.
Requirements	
4-1	The event log sources, and logging systems must be configured to transport logs over reliable and commonly used event log transport protocols such as syslog, Windows Instrumentation Interface (WMI), SNMP traps, etc.
4-2	All event logs must be collected from the sources specified under this requirement: 4-2-1 Systems, including Operating Systems, Databases, Storage, Networks, Applications, etc., covering system events and security/audit logs. 4-2-2 Critical Systems, including Operating Systems, Databases, Storage, Networks, Applications, etc., covering system events and security/audit logs. 4-2-3 Events of sensitive and privileged accounts. 4-2-4 Operating System Events (e.g., Linux)

	4-2-5 Database Events 4-2-6 Security solution events (e.g., Web application Firewall (WAF), Data Loss Prevention (DLP), Multifactor Authentication (MFA), etc.) 4-2-7 Logs generated in the events of Internet browsing, Internet connections and Wi-Fi connections. 4-2-8 Events generating from data transfer to external storage. 4-2-9 File Integrity Monitoring (FIM) event logs. 4-2-10 Event logs generated from system configuration changes, system updates and patches, and application changes. 4-2-11 Abnormal activities such as those detected by Intrusion Prevention System (IPS). 4-2-12 Events generated by security solutions including Antimalware, Remote-Access Technologies (such as Virtual Private Network VPN), Web Proxies, Vulnerability Management Software, Host Intrusion Prevention System (HIPS), Authentication Servers, etc. 4-2-13 Events generated by perimeter devices including firewalls, routers, traffic managers, etc. 4-2-14 Sysmon Event Logs (SEL), a Microsoft tool that records events that the operating system does not log and is very important and useful in security monitoring and incident response. 4-2-15 Events generated by virtualization environments and their underlying tools and infrastructure. 4-2-16 Enable Domain Name System (DNS) query logging wherever technically applicable. 4-2-17 Event logs generated by Industrial Control Systems (ICS).

4-3	All levels of logging as well as audit trail and security logs must be enabled on all web application and technical components.
4-4	Server logging and audit trail must be configured to be forwarded to a centralized logging system as per NCA's regulatory cybersecurity requirements <organization name>'s Cybersecurity Event Logs and Monitoring Management Policy and Standard.
5	Events Monitoring
Objective	To identify unauthorized network activity that may indicate a security incident.
Risk Implication	Failure to detect unauthorized network activity will prevent an organization to respond to suspicious events appropriately before they expand into a greater security incident.
Requirements	
5-1	Security event alerts generated from firewalls must be reviewed on continuing bases to detect any unauthorized access attempts or unusual behaviour. <organization name> can monitor alerts from firewalls, for example, by observing logs daily or by observing other system aspects such as access attempt patterns, characteristics of access, etc.
5-2	Wireless network monitoring must be enabled to detect unauthorized wireless access points. Wireless signals may radiate beyond the confines of organization-controlled facilities. Organizations must proactively search for unauthorized wireless connections including performing thorough scans for unauthorized wireless access points. Scans must not be limited to those areas within facilities containing information and technology assets, but also must include areas outside facilities

	as needed to verify that unauthorized wireless access points are not connected to the systems.
5-3	Host-based monitoring mechanisms must be implemented on endpoint system components for high-risk information and technology assets. Information and technology asset components where host-based monitoring can be implemented include servers, workstations, and mobile devices.
5-4	Signature-based and behaviour-based code monitoring mechanisms (such as Antivirus, EDR, and APT tools) must be implemented on information and technology assets to detect malicious code.
5-5	Signature-based and behavior-based code monitoring mechanisms must be kept current with all available signatures or indicators.
5-6	Monitoring devices must be deployed to monitor communications at the external boundary of the system (e.g., *system perimeter*) and at key internal boundaries *(e.g., logical/physical interfaces within the information and technology asset*) to discover anomalies, detect covert exfiltration of information and track specific types of transactions of interest to <organization name>. For example, *Network segments* where systems that are accessible from the Internet are located.
5-7	Monitoring tools must be employed to detect indicators of *denial-of-service* attacks against <organization name>'s information and technology assets and infrastructure.
6	Event Alerting
Objective	To ensure event alerting is enabled and configured and the appropriate personnel in <organization name> are notified to be able to handle a security incident most effectively.

Risk Implication	If alerting is not configured on logging systems, then security incidents could be addressed incorrectly or may not even be addressed at all.
Requirements	
6-1	Alerts for information and technology assets must be generated when previously defined security monitoring events occur and/or thresholds for indications of potentially malicious activity are met.
6-2	Alerting methods, including email, SMS, video wall systems, etc., must be configured to notify the appropriate personnel.
7	Alert Threshold
Objective	To have a documented approach for the cases when alerts should be triggered.
Risk Implication	If the scope and intent of alerts are not documented, they may not be appropriately configured and potentially malicious events may go unnoticed.
Requirements	
7-1	Specific thresholds for alerting on security monitoring events must be identified and documented. Thresholds must be periodically revised and updated to stay current with trending security attacks.
8	Firewall Event Alerting

Objective	To notify appropriate personnel who are able to address possible security-related events originating from a security incident.
Risk Implication	If personnel are not notified of events, <organization name> will be unaware of malicious unauthorized attempts to connect to the network. Accordingly, if such event is successful, <organization name>'s business will be compromised as a result.
Requirements	
8-1	Alarms or monitoring tools must be configured to alert the appropriate personnel of security-related events originating from the firewall.
9	Application Event Alerting
Objective	To ensure that security incidents and unauthorized activity in the environment do not go undocumented and unnoticed.
Risk Implication	It is important to record main events of <organization name>'s applications. If <organization name> fails to log the specified application related events in the control requirements, this would lead to an increased risk of unidentified and possible unauthorized events occurring in the application, which could cause potential business impact depending on the severity of the incident.
Requirements	
9-1	All client requests and server responses must be logged.
9-2	All account information (e.g., successful and failed authentication attempts and account changes) must be logged.
9-3	All usage information (e.g., the number of transactions occurring in a certain period) must be logged.

9-4	All significant operational actions (e.g., application startup and shutdown, application failures, and application configuration changes) must be logged.
10	Malware in Communication Monitoring
Objective	To identify the presence of malware (e.g., malicious code, spyware, adware) in <organization name>'s communications before it can cause damage.
Risk Implication	If unauthorized use of activities including malware presence goes unnoticed, <organization name> will not become aware of the malware before it spreads, which will put the business at risk of a widespread security attack.
Requirements	
10-1	Inbound and outbound <organization name>'s communications (such as emails, file attachments, downloads) must be monitored for malware (such as malicious code, spyware and adware).
11	Event Log Review Analytics
Objective	Log analysis and SIEM can help detect abnormalities and anomalies, enhance the incident response capabilities, and detect attacks that other security systems missed, and this must be aligned with NCA's operating model for cybersecurity operation centers and NCA's regulatory cybersecurity requirements.
Risk Implication	Failure to recognize security events and incidents will increase the risk that cyber-attacks will go unnoticed and will compromise <organization name>'s information and technology assets as a result.

Requirements	
11-1	All event logs must be forwarded to a centralized log analytics or Security Information and Event Management (SIEM) system for log correlation, analysis and alerting.
11-2	Regular review on SIEM must be performed to monitor and detect abnormal behavior and anomalies.
11-3	SIEM system must be tuned on a regular basis to better identify actionable events and decrease event noise.
11-4	Event logs and alerts must be periodically reviewed, using manual and automated techniques.
11-5	Significant unauthorized activity related to information and technology assets must be detected.
11-6	Misuse of privileged user accounts must be detected.
12	Log Conversion and Parsing
Objective	To ensure all <organization name>'s information and technology assets event logs are monitored to identify unauthorized network activity that may indicate a security incident.
Risk Implication	It is important to record the main events executed in the environment. If <organization name> fails to log the specified events in the control requirements, this would lead to an increased risk of unidentified and possible unauthorized events occurring in the environment, which could cause potential business impact depending on the severity of the incident.

Requirements	
12-1	Log conversion utilities must be used to convert logs unsupported by <organization name>'s logging system to a standard or supported log format.
12-2	Logging software with parsing mechanisms must be implemented to retrieve logs properly from unsupported systems.
13	Continuous Monitoring
Objective	To enable continuous monitoring of all information and technology assets logs to detect malicious activity and to maintain the effectiveness of the monitoring over time, and this must be aligned with NCA's operating model for cybersecurity operation centers and NCA's regulatory cybersecurity requirements.
Risk Implication	If a monitoring plan is not defined and documented, the risk of ad hoc or inadequate monitoring increases, which increases the risk that malicious activity may go unnoticed.
Requirements	
13-1	Develop and prepare a plan for continuous monitoring (such as: aspects that must be monitored within the scope of work, the monitoring method, and testing the effectiveness of monitoring) for information and technology assets and updating them when needed.
14	Logging System Security
Objective	To ensure the protection and security of the logging system underlying infrastructure including log collectors, log aggregators and correlation engines.

Risk Implication	Leaving <organization name>'s logging infrastructure unprotected could allow the attackers to leverage weaknesses in the logging systems and exploit vulnerabilities to gain unauthorized access to <organization name>'s network and data.
Requirements	
14-1	Logging systems software must be installed on dedicated servers.
14-2	A log collector must be implemented in each zone in the network architecture, and only these collectors must be allowed to communicate with the centralized logging system or logging aggregation systems. A log collector must be placed, at a minimum, in the following zones: 14-14-1 Place a log collector in the DMZ. 14-14-2 Place a log collector in the database zone. 14-14-3 Place a log collector in the application zone. 14-14-4 Place a log collector in the corporate services zone. 14-14-5 Place a log collector in the user zone. 14-14-6 Place a log collector in the management zone.
15	Retaining Event Logs
Objective	To avoid deleting security event logs during a period where they can be of use.
Risk Implication	If security event logs are deleted before an audit or investigation, <organization name> would be left unable to defend or investigate activities that occurred on its information and technology assets.
Requirements	

15-1	Event logs must be retained for at least twelve (12) months for all assets, and at least eighteen (18) months for critical assets, or for a longer period, as per <organization name>’s Cybersecurity Policy.
15-2	The archival and deletion of event logs must be restricted to authorized users and only after the expiration of the retention period. Appropriate information and technology asset administrators must be authorized to carry out event log archival and deletion.
16	Alternate Logging Capability
Objective	To enable <organization name> to continue to capture critical security event activity even when the primary logging method (such as central logging) fails, and this must be aligned with NCA’s operating model for cybersecurity operation centers and NCA’s regulatory cybersecurity requirements.
Risk Implication	If the primary logging method fails for a critical technology asset and there is no alternate logging capability, it may not be possible to create an audit trail or identify malicious activity because there are no records that can be used by <organization name> for monitoring and investigation actions. Higher risk assets have a greater impact on the organization's business in the event of a security incident.
Requirements	
16-1	High risk information and technology assets must be configured to maintain local logs in the event of network connectivity failure.
17	Event Log Availability

Objective	To maintain the continuous operation of log capturing functionality and reliability for critical information and technology assets.
Risk Implication	If log functionality is unavailable, this would increase the likelihood of a malicious activity going unnoticed and the inability to conduct incident investigation which could result in a costly security incident.
Requirements	
17-1	<Organization name>'s information and technology assets with **protected** information or designated through risk management assessment as requiring event logs, must be configured to generate event logs at all times.
17-2	Multiple redundant logging systems with failover capabilities must be configured.
18	Log Classification
Objective	To protect all cybersecurity event logs in a secure manner.
Risk Implication	If logs that contain data classified as **Highly Confidential** enforce the controls required for a lower classification of data, then this data will be at a higher risk of compromise due to less strict controls.
Requirements	
18-1	Centralized logging solutions must be treated as if they contain, at a minimum, <organization name>'s **Secret** and **Confidential** data, and as if they comply with all relevant confidentiality controls.

18-2	For any application log or transaction record(s) that contains data classified as **Top Secret**, the controls required for that classification of data must be enforced.
19	Log Integrity and Security
Objective	To maintain a mechanism capable of detecting modification of security event logs to show they have maintained original integrity.
Risk Implication	If security event logs are able to be modified without a means to detect that modification, a malicious user could hide their own malicious activity within the information and technology asset. In such case, if an investigation were to occur based on the malicious user's actions, there would be no evidence to prosecute the user and <organization name>'s claims against the malicious user would not be defensible. Further, if log integrity is compromised, they may not be admissible in court proceedings.
Requirements	
19-1	Rate limiting must be configured to prevent *denial of service* attacks for the logging system. Additionally, it must be configured to a reasonable threshold.
20	Logging Resources
Objective	To avoid losing logs to storage overwriting.

Risk Implication	Failure to configure log storage space with sufficient log capacity for maximum thresholds could result in log overwriting, and <organization name> could lose valuable data. In such case, sensitive logs could be deleted entirely and <organization name> would not be able to rely on these logs in case of a lawsuit or investigation, which could impact its business.
Requirements	
20-1	Sufficient resources (e.g., system resources, data storage, and network bandwidth) must be provided to accommodate prescribed logging activities. Log storage devices must have sufficient log storage for collecting logs.
21	Logging Configuration Changes
Objective	To limit the chance that unauthorized or malicious changes will be made to logging being performed on system components.
Risk Implication	If no limitations are in place for who, where, and when log settings can be changed, a malicious user could turn off logging on sensitive machines to facilitate an unnoticed attack.
Requirements	
21-1	Security event log configuration changes, including scope and monitoring frequency, must be restricted to authorized users.
22	Use of Monitoring Devices
Objective	To prevent overexposure of sensitive data and impact on <organization name>'s network (such as exhaustion of network resources or introduction of compromised/malicious tools into the environment).

Risk Implication	If <organization name>'s cybersecurity function does not authorize and approve the use of monitoring and scanning devices/tools to specific personnel, a tool used could be harmful to the environment and would increase the risk of a data compromise or security incident.
Requirements	
22-1	The use of monitoring and scanning devices or tools must be limited to authorized users.
22-2	The results of all monitoring and scanning activities must be classified as Confidential, at minimum.

Roles and Responsibilities

1- **Standard Owner:** <head of the cybersecurity function>

2- **Standard Review and Update:** <cybersecurity function>

3- **Standard Implementation and Execution:** <information technology function>

4- **Standard Compliance Measurement:** <cybersecurity function>

Update and Review

<cybersecurity function> must review the standard at least once a year or in case any changes happen to the infrastructure, policy, or the regulatory procedures in <organization name> or the relevant regulatory requirements.

Compliance

1- The <head of the cybersecurity function> will ensure compliance of <organization name> with this standard on a regular basis.

2- All personnel at <organization name> must comply with this standard.

3- Any violation of this standard may be subject to disciplinary action according to <organization name>'s procedures.