



Event Logging Guidance

Published: 2020-08-07

© Her Majesty the Queen in Right of Canada,
represented by the President of the Treasury Board 2020,

Published by Treasury Board of Canada, Secretariat
90 Elgin, Ottawa, Ontario, K1A 0R5, Canada

Catalogue Number: BT39-52/2020E-PDF
ISBN: 978-0-660-36826-9

This document is available on the Government of Canada website, Canada.ca

This document is available in alternative formats upon request.

Aussi offert en français sous le titre : Guide sur la consignation d'événements

Event Logging Guidance

From [Treasury Board of Canada Secretariat](#)

On this page

[1. Introduction](#)

[2. References](#)

[Appendix A - Recommended Events to Log](#)

1. Introduction

► In this section

1.1 Purpose and Scope

Bolstering security and increasing network protection requires collection, monitoring and the detection of security incidents through log data analysis. To achieve this, event logging must be enabled on all Information Technology (IT) assets throughout the enterprise.

This document provides high-level guidance on where to configure event logging on IT assets for subsequent forwarding to an approved Government of Canada (GC) centralized security event and information log system.

1.2 Background

In light of an increasingly hostile threat environment, and to better respond to incidents that arise from attacks, GC organizations must perform collection, management and analysis of event logs that could help detect, determine the scope of, understand, or recover from an attack.

As defined by NIST, "an event is any observable occurrence in a system or network." Events are captured in logs and other structured and unstructured data which contain a record of the events occurring within an asset or network. Log data can provide a means for individual accountability,

reconstruction of events, intrusion detection and/or prevention, and problem identification. One or more events analyzed in a security context may trigger an IT security incident. The GC Cyber Security Event Management Plan (CSEMP) ¹ defines an IT security incident as, “Any event (or collection of events), act, omission or situation that has resulted in a compromise ...”

To respond quickly and effectively to attacks and to support the management of incidents, logs must include sufficient information to establish what events occurred, and who or what caused them. Without comprehensive event logs, an attack may go unnoticed indefinitely and the particular damages done may be irreversible. Since every operating system, application, and network device writes event logs, it is important to find an appropriate balance and baseline for logging across the enterprise.

1.3 Requirements

The following are requirements identified from various GC references as described in the table below.

Table 1-1 Requirements

Item	Requirements	Reference
1.	Security event management practices are defined, documented, implemented and maintained to monitor, respond to and report on threats, vulnerabilities, security incidents and other security events, and ensure that such activities are effectively coordinated within the department, with partners and government-wide, to manage potential impacts, support decision-making and enable the application of corrective actions.	Policy on Government Security (PGS) ² , A.7
2.	Create, protect and retain information system audit logs and records to enable monitoring, reporting, analysis, investigation and implementation of corrective actions, as required, for each system, in accordance with departmental practices.	Directive on Security Management (DSM) ³ , B.2.3.8
3.	Analyze information system audit logs and records; Review the results of system monitoring, security assessments, tests and post-event analysis; and, Take pre-emptive, reactive and corrective actions to remediate deficiencies and ensure that IT security practices and controls continue to meet the needs of the department.	DSM, B.2.7.1, B.2.7.2, B.2.7.3, B.2.7.4
4.	Continuously monitoring system events and performance, and including a security audit log function in all information systems, enables the detection of incidents in support of continued delivery of services. It is essential that an adequate level of logging and reporting is configured for the scope of the cloud-based service within the GC’s responsibility. Such documentation will help: <ul style="list-style-type: none">• enable the prompt detection of suspicious activities• facilitate investigation of and response to security incidents• support auditing	Direction on Secure Use of Cloud: SPIN 2017-01 ⁴ , Section 6.3.1 Information system monitoring

	<p>These measures also extend to Cloud Service Providers (CSPs) that are expected to continuously monitor the cloud-based service components within their scope of responsibility.</p> <p>Retention policies for the audit log function should be set in accordance with:</p> <ul style="list-style-type: none"> Library and Archives Canada’s generic valuation tool for information technology other departmental requirements and standards 	
5.	Discovery of potential cyber security events, including confirmed cyber security incidents, through the monitoring of various information sources (including departmental and GC wide hardware/software solutions) and submission of reports by affected departments and agencies as part of the Detection and Assessment phase.	GC Cyber Security Event Management Plan 1
6.	To prevent compromise of assets and infrastructures that are connected to the Internet, disable all non-essential ports and services, and remove unnecessary accounts. Both an enterprise-level auditing and anti-virus solution are key elements of any secure configuration.	Canadian Centre for Cyber Security (CCCS) Top 10 Security Actions, #4 5
7.	Monitoring host-based intrusion prevention system (HIPS) alerts and logging information will provide early indications of intrusions.	CCCS Top 10 Security Actions, #8 5

1.4 Related Security Controls

The following are related security controls from the CCCS’s ITSG-33 IT Security Risk Management Framework [6](#) document that have a dependency on logging and monitoring.

Table 1-2 Related Security Controls

Security Control	Name
AC-3	Access Enforcement
AC-4	Information Flow Enforcement
AC-5	Separation of Duties
AC-8	System Use Notification
AC-17	Remote Access
AU-2	Auditable Events
AU-3	Content of Audit Records
AU-4	Audit Storage Capacity
AU-5	Response to Audit Processing Failures
AU-6	Audit Review, Analysis, and Reporting

AU-7	Audit Reduction and Report Generation
AU-8	Time Stamps
AU-9	Protection of Audit Information
AU-11	Audit Record Retention
AU-12	Audit Generation
AU-14	Session Audit
CA-7	Continuous Monitoring
IR-4	Incident Handling
IR-5	Incident Monitoring
PE-3	Physical Access Control
PE-6	Monitoring Physical Access
RA-3	Risk Assessment
RA-5	Vulnerability Scanning
SC-7	Boundary Protection
SC-26	Honeypots
SI-4	Information System Monitoring
SC-35	Honeyclients
SI-3	Malicious Code Protection
SI-7	Software, Firmware, and Information Integrity

1.5 Implementation Guidance

The following implementation guidance should be considered:

1.5.1 Logging and Monitoring Strategy

The foundation for effective log management is a defined organizational logging and monitoring strategy, as articulated in ITSG-33 Information System Monitoring (SI-4) control family:

A. The organization monitors information systems to detect:

1. Attacks and indicators of potential attacks in accordance with [Assignment: Organization-defined monitoring objectives]; and
2. Unauthorized local, network, and remote connections;

- B. Identifies unauthorized use of the information system through [Assignment: organization-defined techniques and methods];
- C. Deploys monitoring devices:
 - 1. Strategically within the information system to collect organization-determined essential information; and
 - 2. At ad hoc locations within the system to track specific types of transactions of interest to the organization;
- D. The organization protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion.

Information system monitoring is a baseline requirement for related controls, specifically the families and controls identified in **Table 1-2 Related Security Controls**.

Supplemental to these general requirements, **Appendix A - Recommended Events to Log** provides a list of events from common IT event sources which should be logged by GC organizations.

The GC policy and directive instruments referenced in **Table 1-1 Requirements** touch upon logging and auditing but do not provide details for how to establish a foundational logging and monitoring strategy that satisfies the ITSG-33 control requirements specified above. Accordingly, the following external resources are recommended for review:

- NIST’s comprehensive guidance on developing a log management capability, including policy components [7](#).
- The SANS Institute’s template for creating a policy and defining logging requirements, and roles and responsibilities [8](#). This template poses questions that should be answered in a typical logging and monitoring policy.

1.5.2 Log Retention and Preservation

Library and Archives Canada (LAC) recommends a retention period of 2 years after last administrative use for information with business value in IT or security processes [9](#). ITSG-33’s AU-11 stipulates that retention and preservation periods for audit records (i.e. log records related to auditable events) are “organization-defined”; however, the Government of Canada Security Control Profile for Cloud-based GC Services [10](#), establishes for such records the following retention requirements:

- CSP: Time period = [**at least 90 days**]
- GC: Time period = [**events and logs at least 3 months online and at least 6 months in storage; events and logs associated with a security incident for at least 2 years**]

The above requirements, specific to Protected B, medium integrity and medium availability (PBMM) systems hosted in the cloud, can be equally applied to PBMM systems on premises, including the security logging for systems listed in **Appendix A - Recommended Events to Log**.

Log retention and preservation requirements for other event data collected from GC IT systems above or below PBMM, including those listed in the Appendix should be defined within organizational policy instruments, IT security control profiles, and other types of standards. The policy should balance risk reduction requirements with operational impacts such as capital costs and resource requirements.

1.5.3 Protecting Log Information

Logging facilities and log information must be protected against tampering and unauthorized access, because no matter how extensively an organization performs logging, those logs are worthless if their integrity cannot be trusted. Administrator and operator logs are often targets for erasing trails of activities and evidence of an attacker's presence.

Common controls for protecting log information include the following:

- Verifying that event logging is enabled and active for system components.
- Ensuring that only individuals who have a job-related need can view log files.
- Confirming that current log files are protected from unauthorized modifications via access control mechanisms, physical segregation, and/or network segregation.
- Ensuring that current log files are promptly backed up to a centralized log server or write once media.
- Using file integrity verification mechanisms to detect unauthorized changes to event logging configuration files and log files.

1.6 Supplemental Guidance

1.6.1 Windows

Additional guidance for Windows environments can be found in the following documents:

- **NSA's Spotting the Adversary with Windows Event Log Monitoring (Aug 2015)** [11](#) - This paper provides an introduction to collecting important Windows workstation event logs and storing them in a central location for easier searching and monitoring of network health. The focus is for administrators in configuring central event log collection. It recommends a basic set of events to collect on an enterprise network using Group Policy and the built-in tools already available in the Microsoft Windows operating system (OS).
- **Microsoft's Best Practices for Securing Active Directory** [12](#) [13](#) - This paper focuses on several topics from defending against different attacks on Active Directory installations to recommending an extensive list of events to monitor in a domain.
- **National Cyber Security Centre's Introduction to Logging for Security Purposes** [14](#) - This guidance will help to devise an approach to logging that will help answer some of the typical questions asked during a cyber incident, such as:
 - What has happened?

- What is the impact?
- What should we do next?
- Has any post-incident remediation been effective?
- Are our security controls working?

1.6.2 Cloud

Approaches for security monitoring of public cloud have similarities to and differences from those of traditional IT environments. Cloud-specific threats exist, but organizations are more likely to contend with traditional threats that affect their cloud environment, and with threats from the cloud that affect their traditional IT environment.

Event monitoring in a cloud requires a combination of traditional tools such as SIEM or Data Loss Prevention (DLP) and cloud-native tools, such as Cloud Access Security Brokers (CASB), Cloud Security Posture Management (CSPM) or Cloud Workload Protection Platforms (CWPP) to cover detection needs. The major CSPs all offer native event logging and log management options, the suitability of which will need to be evaluated by individual organizations based on their requirements and constraints. It is recommended to enable and leverage these logging and monitoring functions within each platform; however, GC organizations should be mindful of the financial and logistical impacts.

Additional guidance for three common Cloud environments can be found in the following documents:

- **Azure Logging and Auditing** ¹⁵ - Azure provides a wide array of configurable security logging and auditing options to help you identify gaps in your security policies and mechanisms. This article discusses generating, collecting, and analyzing security logs from services hosted on Azure.
- **Amazon Web Services (AWS)** ¹⁶ ¹⁷ - Amazon CloudWatch Logs is used to monitor, store, and access log files from Amazon Elastic Compute Cloud (Amazon EC2) instances, AWS CloudTrail, Route 53, and other sources.
- **Google Cloud** ¹⁸ - Cloud Audit Logs helps security teams maintain audit trails in Google Cloud Platform (GCP). With this tool, enterprises can attain the same level of transparency over administrative activities and accesses to data in Google Cloud Platform as in on-premises environments. Every administrative activity is recorded on a hardened, always-on audit trail, which cannot be disabled by any rogue actor.

2. References

1

Treasury Board of Canada Secretariat, "GC Cyber Security Event Management Plan," [Online]. Available: <https://www.canada.ca/en/treasury-board-secretariat/services/access->

information-privacy/security-identity-management/government-canada-cyber-security-event-management-plan.html.

2

Government of Canada, "Policy on Government Security," July 2019.

3

Government of Canada, "Directive on Security Management," July 2019.

4

Treasury Board of Canada Secretariat, "Direction on the Secure Use of Commercial Cloud Services: Security Policy Implementation Notice," November 2017.

5

Canadian Centre for Cyber Security, "Top 10 IT Security Actions to Protect Government of Canada Internet-Connected Networks and Information," November 2014.

6

Canadian Centre for Cyber Security, "IT Security Risk Management: A Lifecycle Approach (ITSG-33)," 2012.

7

National Institute of Standards and Technology, "Guide to Computer Security Log Management," [Online]. Available:
<https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-92.pdf>.

8

SANS Institute, "SANS Information Logging Standard," [Online]. Available:
<https://www.sans.org/security-resources/policies/server-security/pdf/information-logging-standard>.

9

Library and Archives Canada, "Information Management," [Online]. Available:
<https://www.bac-lac.gc.ca/eng/services/government-information-resources/guidelines/generic-valuation-tools/Pages/information-management.aspx#TOC5>.

10

Government of Canada, "Government of Canada Security Control Profile for Cloud-based GC Services," [Online]. Available: <https://www.canada.ca/en/government/system/digital-government/modern-emerging-technologies/cloud-services/government-canada-security-control-profile-cloud-based-it-services.html>.

11

National Security Agency, "Spotting the Adversary with Windows Event Log Monitoring (version 2)," 2015. [Online]. Available:
<https://apps.nsa.gov/iaarchive/library/reports/spotting-the-adversary-with-windows-event-log-monitoring.cfm>.

12

Microsoft, "Best Practices for Securing Active Directory," [Online]. Available:
<https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory>.

13

"Monitoring Active Directory for Signs of Compromise," [Online]. Available: Microsoft, Monitoring Active Directory for Signs of Compromise, <https://docs.microsoft.com/en->

us/windows-server/identity/ad-ds/plan/security-best-practices/monitoring-active-directory-for-signs-of-compromise.

14

National Cyber Security Centre, "Introduction to logging for security purposes," July 2018. [Online]. Available: <https://www.ncsc.gov.uk/guidance/introduction-logging-security-purposes>.

15

Microsoft, "Azure logging and auditing," January 2019. [Online]. Available: <https://docs.microsoft.com/en-us/azure/security/azure-log-audit>.

16

Amazon Web Services, "What Is Amazon CloudWatch Logs?," [Online]. Available: <https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/WhatIsCloudWatchLogs.html>.

17

Amazon, "AWS Logging General Information," [Online]. Available: <https://aws.amazon.com/answers/logging/>.

18

Google, "Cloud Audit Logs," [Online]. Available: <https://cloud.google.com/audit-logs/>.

19

Australian Government, "Guidelines for System Monitoring," [Online]. Available: <https://www.cyber.gov.au/ism>.

Appendix A - Recommended Events to Log

Table A-1 System Configuration and Performance reflects guidance to collect configuration and performance data within information systems.

Table A-1 System Configuration and Performance

Recommended Data	Format	Priority
System status (resource utilization, performance)	Log Database Query Script	MEDIUM
Software Updates User Agent in the case of device /host software updates	Log Database Query Script	MEDIUM
Configuration – collected regularly	Database Query Script	HIGH
Configuration Changes Success and Failure	Log following a management action or administrative login	MEDIUM

Table A-2 Authentication and Authorization

Recommended Data	Format	Priority
As per the Australian 2019 Information Security Manual ⁸ . 1. Security related system alerts and failures 2. User and group additions, deletions and modification to permissions 3. Unauthorized access attempts to critical systems and file 4. Authentication Success Logons 5. Authentication Failed Logon Attempts 6. Authentication Logoffs	Log	MEDIUM
Administrative Authentication 1. Authentication Success Logons 2. Authentication Failed Logon Attempts 3. Authentication Logoffs 4. Privilege elevation – success 5. Privilege elevation – failed	Log	HIGH
Authorization All privileged operations including “sudo”, enabling CLI access, system administrative commands, PowerShell	Log	HIGH

Table A-3 Email Filtering, SPAM, and Phishing

Recommended Data	Format	Priority
Raw and Metadata - Filtering events 1. Date and time 2. Sent From Sender, From Sender 3. Recipient 4. Subject 5. Email Headers 6. Rule triggered – log of policies along with actual values including but not limited to DNS records, Phish Campaign identifier, and Domain URL	Log Packet Capture Email attachments	MEDIUM
Content filtering policy updates	Log	MED
SPAM dictionary modifications	Log	MED
IP and Domain reputation (as indicated by mail server connection)	Log	LOW

Table A-4 Anti-Virus and Behaviour-based Malware Protection

Recommended Data	Format	Priority
1. Date and time 2. Source hostname, IP and Port 3. Destination hostname, IP and Port 4. Description of malicious code or action and severity	Log Attachments	MED

5. Identity or (hash) identifier of the file(s) 6. Description of the action taken – clean, quarantine, delete 7. Signature updates		
Indication of the host that connected to a specific URL. <ul style="list-style-type: none"> IP and Domain reputation URL Categorization 	Log	HIGH

Table A-5 Data Loss Prevention

Recommended Data	Format	Priority
1. Date and time 2. Source hostname, IP and Port 3. Destination hostname, IP and Port 4. Description of malicious code or action and severity 5. Identity or identifier of the file(s) 6. Description of the action taken – clean, quarantine, delete 7. Signature updates	Log Attachments	LOW

Table A-6 Network Device Infrastructure

Network Device Infrastructure would include DNS, DHCP, and WiFi.

Recommended Data	Format	Priority
DHCP Lease Information including MAC, IP	Log Packet Capture	LOW to MEDIUM
DNS - Source IP and Port, Destination IP and Port <ul style="list-style-type: none"> Content of Query, Response, and Errors – all record types Zone transfers request and response (audit log) Zone transfers request and response (content) 	Packet Capture preferred, otherwise log.	HIGH for DNS analytics, protection against DNS attacks, protection against exfiltration, and mitigation against malicious domains.
<ul style="list-style-type: none"> WiFi Supporting Infrastructure logs including security logs at INFO level WiFi IDS / IPS events WiFi IDS / IPS alarms Device authentication logs with User Agent URL browsing logs + HTTP methods (e.g., POST, GET, etc.) User authentication logs DHCP Lease Information including MAC, IP Firewall logs showing NAT IP address Roaming Logs Timestamps 	Log Packet capture SNMP data including WALK, GET, TRAP	HIGH
Static Network Address Translation Table mapping as well	Log	HIGHEST

as port forwards.	Database query	
1. Protocol	Script	
2. Port	File	
3. Inside local and global IP and port	Config	
4. Outside local and global IP and port		
5. Timestamps	SNMP	

Table A-7 Network Device Infrastructure

Other network device Infrastructure would include routers, switches, proxies, firewalls, IDS / IPS, VPN gateway devices.

For devices with multiple interfaces, it is desirable to get the interface MAC – if it can be correlated to the de-NAT IP address.

Recommended Data	Format	Priority
Routers and Switches : <ul style="list-style-type: none"> Routing Tables Routing Changes (logging all CLI commands , BGP) IP addressing schema and implementation 	Script File Config	MEDIUM
Hash of the binary / binaries running on the device	Script	HIGH
Firewalls All events from firewall. At the very least, if access control lists (ACL) are enabled and the device is filtering traffic: <ol style="list-style-type: none"> Action Permit, Teardowns, Closes, Denies, and Drops Interface Source hostname, IP address and port, MAC Destination hostname, IP address and port, MAC Protocol type Rule name and number triggered URL if applicable, associated user and User Agent 	Log	HIGH
All IDS / IPS alerts and events <ol style="list-style-type: none"> Source hostname, IP address and port, MAC Destination hostname, IP address and port, MAC Signature triggered and associated details including signature, anomaly, rate threshold Device Name Type of event and category In the case of Fortinet network IPS, attack context (Web / Device) User agent if available 	Log Packet Capture	HIGH
VPN Gateway – all events At the very least, for accepts, teardowns, closes, denies, and drops: <ol style="list-style-type: none"> Date and Time Source hostname, IP address and port, MAC 	Log	HIGH

3. Destination hostname, IP address and port, MAC 4. Source IP address and port, MAC (inside tunnel) 5. Destination IP address and port, MAC (inside tunnel) 6. Authentication information – success or failure with user name and device with user agent 7. Change in status of connections / tunnel status 8. VPN certificate status validation		
Proxies and Web Content Filters Provides NAT, User, and gateway IP address to provide enhanced reporting of malicious domains and IP addresses. In the case of web, w3c format. <ol style="list-style-type: none"> 1. Date and Time 2. Source hostname, IP address and port, MAC 3. Destination hostname, IP address and port, MAC 4. Web URL methods / User agent / Decoded Headers 5. URL categories 6. URL 7. Permitted, Restricted 	Log Packet Capture	HIGHEST
Proxies and Web Content Filters <ol style="list-style-type: none"> 1. Policy updates 2. Software Updates 	Log	HIGHEST

Table A- 8 GC PKI Infrastructure

Recommended Data	Format	Priority
All events related to: <ul style="list-style-type: none"> • Generation; • Revocation; • Access; • Update; • Expiry; • Recover; • Authentication success; • Authentication fail • LDAP logs 	Log	HIGH

Table A-9 Vulnerability Assessments

Recommended Data	Format	Priority
<ol style="list-style-type: none"> 1. Date and Time 2. Hostname, IP address and OS version 3. Open ports 4. Installed applications 5. Vulnerabilities listed in installed applications 6. Source of vulnerability and severity 	Log	MED to HIGH Correlate to packet capture for cyber defence and situational awareness

Table A-10 Operating Systems

Recommended Data	Format	Priority
<p>Windows Infrastructure and Operating Systems</p> <ul style="list-style-type: none">Microsoft’s Best Practices for Securing Active Directory 5 6NSA’s Spotting the Adversary with Windows Event Log Monitoring (Aug 2015) 4National Cyber Security Centre’s Introduction to Logging for Security Purposes 7Windows Event Logging and Forwarding 9 <ol style="list-style-type: none">User and administrator access to OS components and applications:<ol style="list-style-type: none">File and object accessAudit log access (success and failure)System access (failure)System performance and operational characteristics:<ol style="list-style-type: none">Resource utilization, process statusSystem eventsService status changes (e.g. started, stopped)Service failures and restartsSystem configuration:<ol style="list-style-type: none">Changes to security configuration (success and failure)Audit log clearedChanges to accountsUser or group managementFile access:<ol style="list-style-type: none">transfer of data to external mediaPowershell execution commands	Log	HIGH

Table A-11 Database Level

Recommended Data	Format	Priority
<ol style="list-style-type: none">Addition of new users, especially privileged usersQuery, Response, and traceback<ol style="list-style-type: none">methodcomments or variablesmultiple embedded queriesdatabase alerts or failuresAttempts to elevate privileges - successful or unsuccessfulChanges to the database structureChanges to user roles or database permissionsDatabase administrator actionsDatabase logons and logoffs, failed logonsUse of executable commandsCLI commands against the data base.Database configuration and versionAccess to sensitive information within the database such as keys, passwords, privacy related data	Log	HIGH

Table A-12 Application Level

Recommended Data	Format	Priority
Web applications <ul style="list-style-type: none"> • URL • Headers • HTTP Methods - Request with body of data • HTTP Response with body of data 	Log Packet Capture Unencrypted	HIGH
Web application data base queries and responses	Log	HIGH
Web application crashes - processes or applications	Log	HIGH
Web applications configuration and version, middleware configuration and version	Log	HIGH
Commercial Off The Shelf and Custom Applications <ol style="list-style-type: none"> 1. User authentication (success and failure) 2. User and administrator application use: <ol style="list-style-type: none"> a. File and object access b. Audit log access (success and failure) c. System access (failure) d. Application transactions (web page hits, email sent/received, file transfers completed) 3. Transaction logs 4. System performance and operational characteristics: <ol style="list-style-type: none"> a. Resource utilization b. Process status c. Errors (input validation, dis-allowed operations) d. System events e. Service status changes (e.g. started, stopped) 5. Application configuration and version 	Log Application Monitoring Dashboards	MEDIUM
<ol style="list-style-type: none"> 1. User authentication (success and failure) 2. User access of application components: <ol style="list-style-type: none"> a. File and object access b. Audit log access (success and failure) c. System access (failure) d. Application transactions 3. Transaction logs 4. System performance and operational characteristics: <ol style="list-style-type: none"> a. Resource utilization b. Errors (input validation, dis-allowed operations) and exit codes c. Process status d. Service status changes (e.g. started, stopped) 5. Application configuration and version, middleware configuration and version 6. Usage information, if applicable 7. User request and response events, if applicable 	Log	MEDIUM

Table A-13 Virtualization System

Recommended Data	Format	Priority
<ol style="list-style-type: none"> 1. User authentication: <ol style="list-style-type: none"> a. Logon (success and failure) b. Attempts to obtain privileged access (success and failure) 2. User and administrator/root access and actions of components and applications: <ol style="list-style-type: none"> a. File and object access b. Audit log access (success and failure) c. System access (failure) 3. System performance and operational characteristics: <ol style="list-style-type: none"> a. Resource utilization, process status b. System events c. Service status changes (e.g. started, stopped) 4. System configuration: <ol style="list-style-type: none"> a. Changes to security configuration (success and failure) b. Changes to hypervisor c. Changes to VMs d. Changes made within VMs e. Audit log cleared 5. Creation and deployment of VMs 6. Migration of VMs (e.g., source and target systems, time, authorization) 7. Creation and deletion of system-level objects 	Log	MEDIUM

Table A-14 Cloud Environments

Recommended Data	Format	Priority
<p>Nearly all successful attacks on cloud services resulted from customer misconfigurations. With that in mind, the logging and monitoring focus should be on:</p> <ol style="list-style-type: none"> 1. Any activity on Breakglass account(s) (which should never have to be used) 2. Conditional access policy changes 3. Changes to environment policies (e.g., Azure subscription, AWS services, Google solutions, etc.) in management logs 4. Privileged role changes 5. Virtual network (vnet) changes 6. Deletions of Delete Locks 7. Changes to logging policies 8. Privileged Identity Management (PIM) and identity protection changes 9. Changes to alert rules (audit the auditor) 10. Key vault/key management changes 11. API logs 12. Storage file access logs, file, file hashes 13. Baseline deviations for Prod App tiers 14. Baseline deviations for Prod Data Tiers 	Log	HIGHEST

Date modified: 2020-08-07

Contact us

Departments and agencies

Public service and military

News

Treaties, laws and regulations

Government-wide reporting

Prime Minister


About government

Open government



- [Social media](#)
- [Mobile applications](#)
- [About Canada.ca](#)

- [Terms and conditions](#)
- [Privacy](#)

Top of page 

Canada 