# Logging and Monitoring

## Objective

Enable logging for the cloud environment and for cloud-based workloads.

## Key Considerations

* [ ] Implement adequate level of logging and reporting, including a security audit log function in all information systems.
* [ ] Identify the events within the solution that must be audited in accordance with [GC Event Logging](https://www.gcpedia.gc.ca/gcwiki/images/e/e3/GC_Event_Logging_Strategy.pdf).

**Note:** You may need to configure your solution to send the audit log records to a centralized logging facility, if one is available, where existing auditing mechanisms will be applied.

* [ ] Configure alerts and notifications to be sent to the appropriate contact/team in the organization.
* [ ] Configure or use an authoritative time source for the time-stamp of the audit records generated by your solution components.
* [ ] Continuously monitor system events and performance.

## Validation

* [ ] Confirm policy for event logging is implemented.
* [ ] Confirm event logs are being generated.
* [ ] Confirm that security contact information has been configured to receive alerts and notifications.

## Applicable Service Models

* IaaS, PaaS, SaaS

## References

1. [SPIN 2017-01](https://www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/security-identity-management/direction-secure-use-commercial-cloud-services-spin.html), subsection 6.3.1
2. CSE Top 10 #1, 5, 8
3. Refer to [GC Event Logging Guidance](https://www.gcpedia.gc.ca/gcwiki/images/e/e3/GC_Event_Logging_Strategy.pdf)
4. Related security controls: AU‑2, AU‑3, AU‑6, AU‑8, AU‑9, AU‑9(4), AU‑12, SI-4