E-vote 2011

Use case specification: 5.2 Auditing

Project: E-vote 2011

NORWEGIAN MINISTRY OF LOCAL GOVERNMENT
AND REGIONAL DEVELOPMENT

CONTENT

1. Executive Summary

The system shall provide an 'audit module' with easy access to all audit logs. The audit module must have functionality for:

1. Logging of all events. All logs must be immutable.
2. Accessing, filtering and searching in audit logs
3. Creating audit reports
4. Detecting abnormal behaviour and present warning messages (Monitoring agent)
5. Functionality for configuring monitoring parameters

The auditing of the election system comprises two parts:

1. The audit of the actual election must show exactly what happened and when it happened.
2. A technical audit shall ensure that the election system is set up as agreed, and that only approved and audited software is running on the system.

2. Purpose

The purpose of this use case is to provide an event logging and monitoring system to ensure full audit trail for gaining public confidence in the Election System.

3. Actors

Actor	Description
ES	The Election System
Auditor	Auditors may be members of the Central / Local Election boards, members of the internal auditing team, election observers (national and international) and other individuals responsible for ensuring that elections are performed correctly and according to laws and regulations.

4. Pre-conditions

ID	Description	Comments

5.2.1	The Election System is up and running	

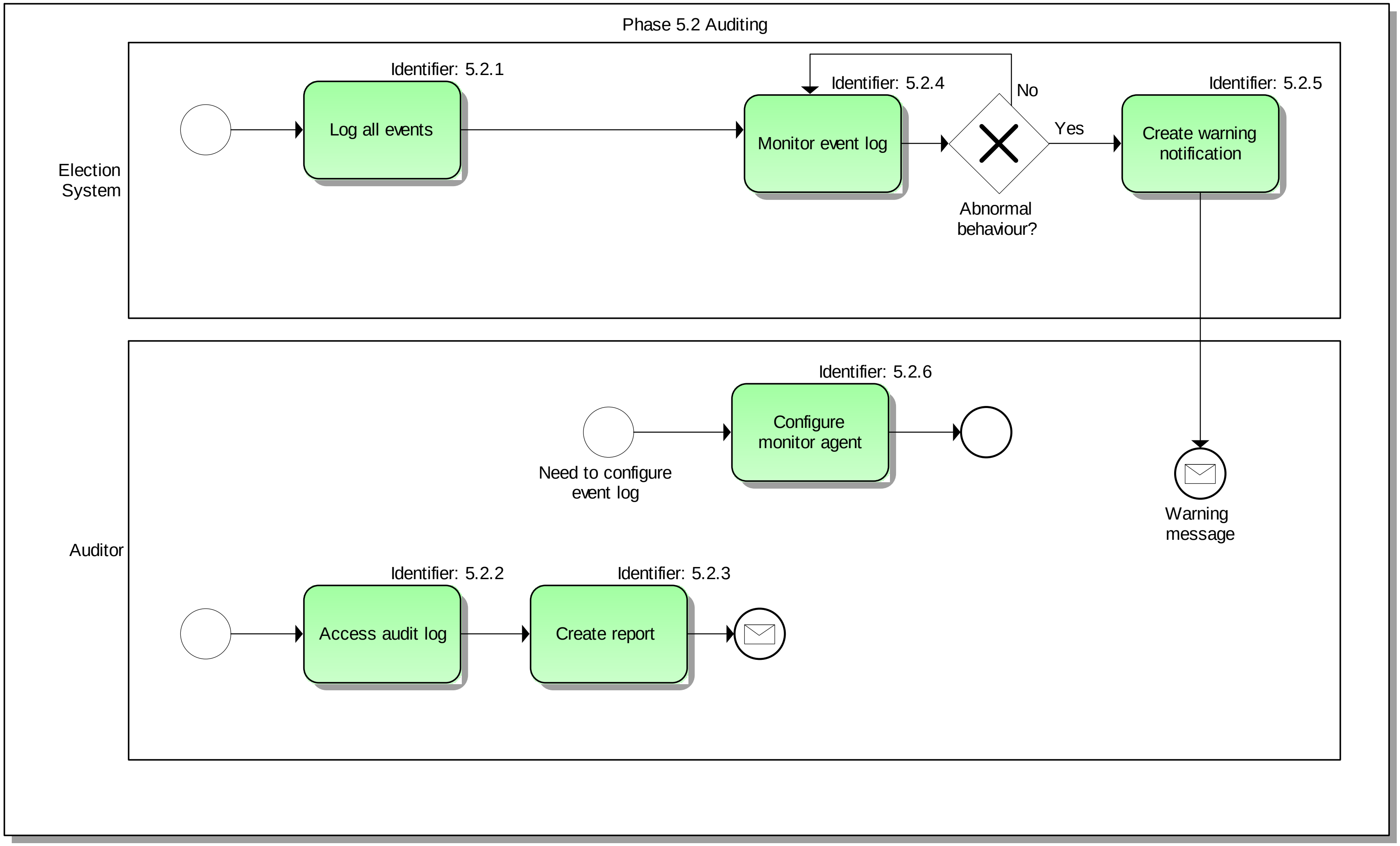
5. Post-conditions

ID	Description	Comments
5.2.2	Configuration of the monitoring agent is stored in the system	
5.2.3	Events are logged in the system	
5.2.4	Reports are produced by the system	

6. Trigger

The need for observing system events.

7. Main Flows - Functional Requirements



7.1. Main flow 1 – Log and monitor events

ID	Actor	Function (Requirement)	Requirement description	Ref
F 5.2.1	ES	Log all events	The system must be able to log all significant events (Record user, time and events). Some of these logs may include: 1. All election transactions 2. Attacks on the operation of the election system and its communications infrastructure 3. System failures, malfunctions and other threats to the system 4. Log of events at all levels of the Election System (including e.g. the system operating system level) 5. Etc. The audit logs shall be protected against unauthorized modification.	
F 5.2.4	ES	Monitor event log	The monitoring agent shall run in the background, continuously monitoring the event log detecting abnormal behaviour.	A1

7.1. Main flow 2 – Configure monitor agent

ID	Actor	Function (Requirement)	Requirement description	Ref
F 5.2.6	Auditor	Configure monitor agent	The auditor must be able to configure parameters for detecting abnormal behaviour in the system.	

7.2. Main flow 3 – Access audit log

ID	Actor	Function (Requirement)	Requirement description	Ref
F 5.2.2	Auditor	Access audit log	The auditor must be able to access, filter and search through all audit logs	
F 5.2.3	Auditor	Create report	The auditor must be able to create reports. See use case 5.1 ‘Reports’ for reporting functionality.	

7.3. Alternate flow 1 – Monitoring agent (A1)

ID	Actor	Function (Requirement)	Requirement description
F 5.2.5	ES	Create warning	The system shall create warning and notify the auditor(s)

8. Non-functional Requirements

8.1. Accessibility & Usability

ID	Requirement description	Ref
5.2.5	See ‘Accessibility and usability requirements’	8.1

8.2. Security

ID	Requirement description	Ref
OS0.15	The election system shall maintain reliable synchronised time sources. The accuracy of the time source shall be sufficient to maintain time marks for audit trails and observation data, as well as for maintaining the time limits for registration, nomination, voting, or counting.	
OS3.6	The audit system shall maintain voter anonymity at all times.	
OS13.2	At any time during an election the election officers shall be able to perform a self-test of the election system, assuring the integrity of the security functions and the user and system data. Any failure that may endanger the proper operation of the system shall be reported.	
OS13.3	The election systems shall generate reliable and sufficiently detailed observation data so that election observation can be carried out. The time at which an event generated observation data shall be reliably determinable. The authenticity, availability and integrity of the data shall be maintained.	
OS13.4	The audit system shall be designed and implemented as part of the election system. Audit facilities shall be present on different levels of the system: logical, technical and application.	
OS13.5	Audit functions of the election system shall include recording, providing monitoring facilities and providing verification facilities.	
OS13.6	The audit system shall be open and comprehensive, and actively report on potential issues and threats.	

OS13.8	The audit system shall provide the ability to oversee the election or referendum and to verify that the results and procedures are in accordance with the applicable legal provisions.	
OS13.9	The audit system shall provide the ability to cross-check and verify the correct operation of the election system and the accuracy of the result, to detect voter fraud and to prove that all counted votes are authentic and that all valid votes have been counted.	
OS13.10	The audit functions of the election system shall provide the ability to verify that an recording of e-votes and counting of e-votes and p-votes has complied with the applicable legal provisions, and that the election results are an accurate representation of the authentic votes.	
OS13.11	The audit system shall be protected against attacks which may corrupt, alter or lose records in the audit system.	
OS13.12	The fact that a vote has been cast within the prescribed time limits shall be ascertainable.	
OS14.4	All system components of the election system shall be independently verifiable i.e. it shall be possible to certify that all system components act accordingly to their specifications.	

8.3. Rules & Regulations

ID	Requirement description	Ref
5.2.6	This use case refers to regulations described in the Representation of the People Act (the Election Act). http://www.regjeringen.no/upload/KRD/Kampanjer/valgportal/Regelverk/Representation_of_the_People_Act170609.pdf	
5.2.7	This use case refers to regulations relating to parliamentary and local government elections (Representation of the People Regulations) http://www.regjeringen.no/upload/KRD/Kampanjer/valgportal/Regelverk/Regulations_2003_EN_170609.pdf	
5.2.8	This use case also refer to the Council of Europe e-vote Recommendation Rec(2004) 11. http://www.coe.int/t/dgap/democracy/activities/GGIS/E-voting/Key_Documents/Rec(2004)11_Eng_Evoting_and_Expl_Memo_en.pdf	

8.4. Performance (Frequency)

ID	Requirement description	Ref
P 5.2.1	The use of audit functions and searching in audit logs, performed during the polling phase of the election, shall have no impact on the voting system capacity or on response times experienced by voters.	
P 5.2.2	Response times when using the audit system shall normally be less than 1 second. In the case of complicated and 'heavy'	

	search operations longer response times may be acceptable. Response time requirements shall be agreed upon during the system design phase.	