CLAIMS

1. A system for automatically monitoring efficacy of security controls relating to access control in a computer network, comprising:

a probe engine configurable with at least one set of rules relating to access permissions to data in said computer network;

at least one security probe forming part of said probe engine and operative to automatically:

place, at at least one storage location within said computer network, simulated data corresponding to said data in said computer network, said simulated data having associated therewith access permissions defining allowed access to said simulated data, said access permissions associated with said simulated data being non-compliant with said at least one set of rules; and

attempt to access said simulated data following the placement thereof, using access privileges satisfying said non-compliant access permissions associated with said simulated data, but not satisfying said at least one set of rules, and

a security monitoring and reporting module operative to provide a user sensible output indicating at least whether said attempt to access said simulated data was successful and, responsive to said attempt to access said simulated data being successful, reporting mitigating activities by said security controls in response to said successful attempt.

2. A system according to claim 1, wherein said at least one set of rules comprises at least one of a general compliance regime and an organization-specific compliance regime.

3. A system according to claim 2, and also comprising a data generator forming part of said probe engine and operative to automatically generate said simulated data.

4. A system according to claim 3, wherein said data generator is operative to:

automatically generate said simulated data based on at least one of said compliance regime and machine learning based on training data pre-classified in accordance with said compliance regime; and

automatically update said simulated data responsive to changes in said compliance regime.

5. A system according to claim 1, wherein said security probe is operative to place said simulated data at said storage location using a first user credential representing a first user within said organization and to access said simulated data using at least a second user credential representing at least a second user within said organization.

6. A system according to claim 5, wherein said non-compliant access permissions comprise access permissions to at least one access group within said organization, said second user belonging to said at least one access group.

7. A system according to claim 5, wherein said at least one second user credential comprises a plurality of user credentials representing a corresponding plurality of second users within said organization, said second users belonging to mutually different access groups.

8. A system according to claim 1, wherein said security monitoring and reporting module is operative to report a lapse of time between said successful attempt and performance of said mitigating activities and to rank different ones of said mitigating activities based on said lapse of time.

9. A system according to claim 1, wherein said security monitoring and reporting module is operative to rank a severity of different ones of said successful attempts to access simulated data, based on a relative sensitivity of the simulated data that was successfully accessed in said different attempts.

10. A system according to claim 8, and also comprising an automatic mitigation module, operative to automatically perform a mitigating action in response to said successful attempt, in the absence of a report of said mitigating activities by said security monitoring and reporting module.

11. A system according to claim 10, wherein said mitigating action by said automatic mitigation module comprises removing permission to access to said storage location.

12. A method for automatically monitoring efficacy of security controls relating to access control in a computer network, comprising:

configuring a probe engine with at least one set of rules relating to access permissions to data in said computer network;

automatically placing, at at least one storage location within said computer network, simulated data corresponding to said data in said computer network, said simulated data having associated therewith access permissions defining allowed access to said simulated data, said access permissions associated with said simulated data being non-compliant with said at least one set of rules associated with said simulated data;

attempting to access said simulated data following the placement thereof, using access privileges satisfying said non-compliant access permissions associated with said simulated data but not satisfying said at least one set of rules, and

providing a user sensible output indicating at least whether said attempt to access said simulated data was successful and, responsive to said attempt to access said simulated data being successful, reporting mitigating activities by said security controls in response to said successful attempt.

13. A method according to claim 12, and also comprising:

automatically generating said simulated data based on at least one of said compliance regime and machine learning based on training data pre-classified in accordance with said compliance regime; and

automatically updating said simulated data responsive to changes in said compliance regime.