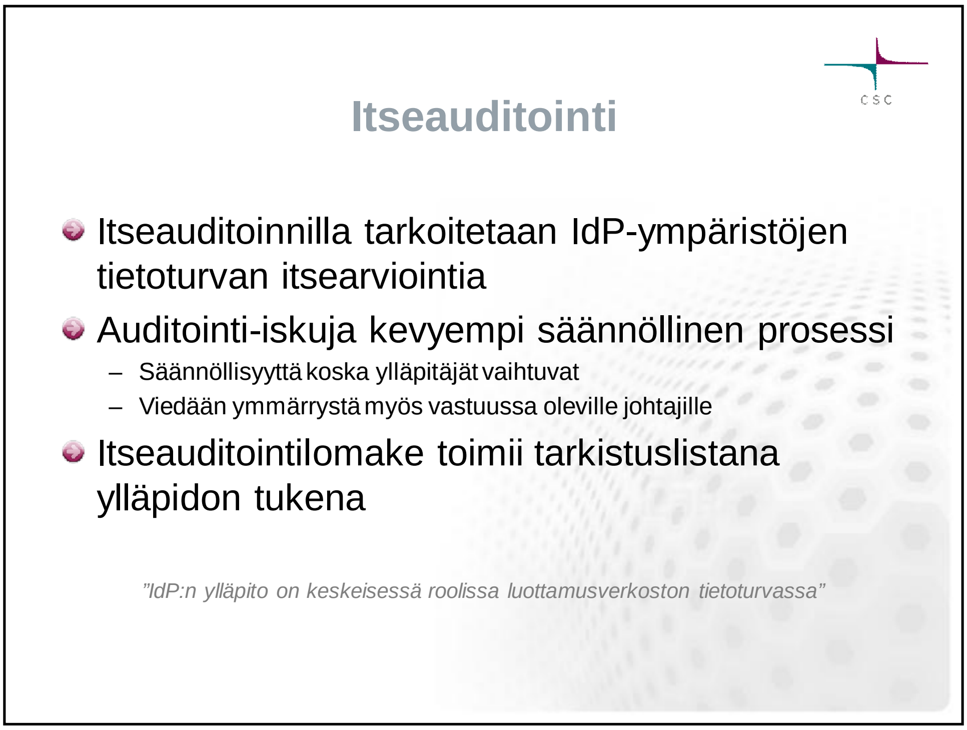
Tietoturvakartoitus- ja itseauditointilomake

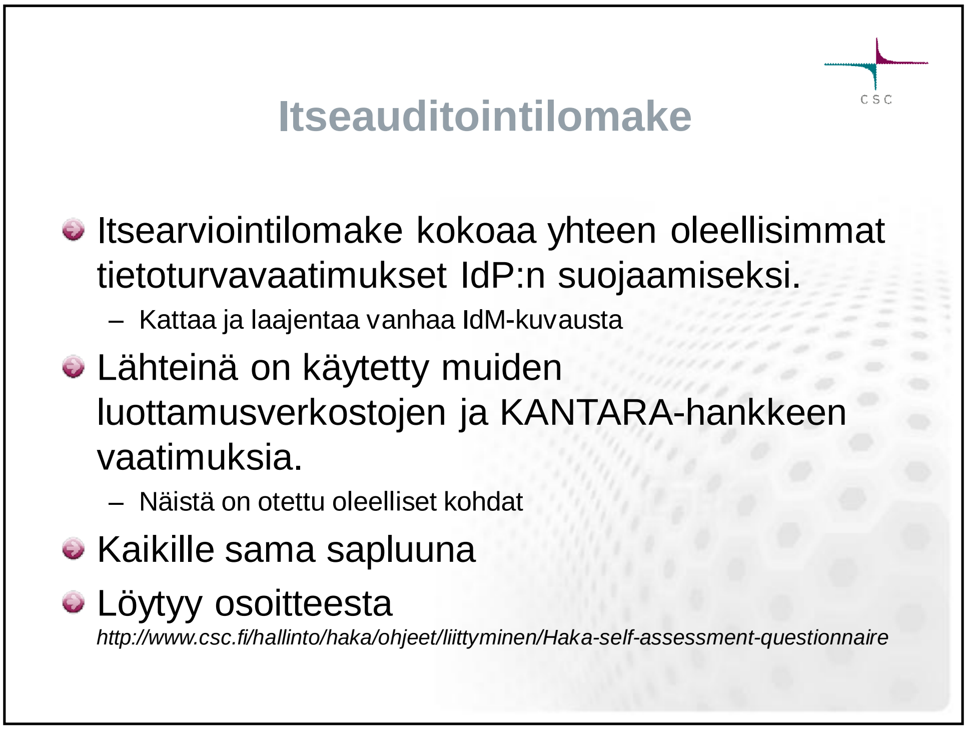
- 14.02.2013
- Sami Silén, sami.silen@csc.fi



Itseauditointi

- Itseauditoinnilla tarkoitetaan IdP-ympäristöjen tietoturvan itsearviointia
- Auditointi-iskuja kevyempi säännöllinen prosessi
  - Säännöllisyyttä koska ylläpitäjät vaihtuvat
  - Viedään ymmärrystä myös vastuussa oleville johtajille
- Itseauditointilomake toimii tarkistuslistana ylläpidon tukena

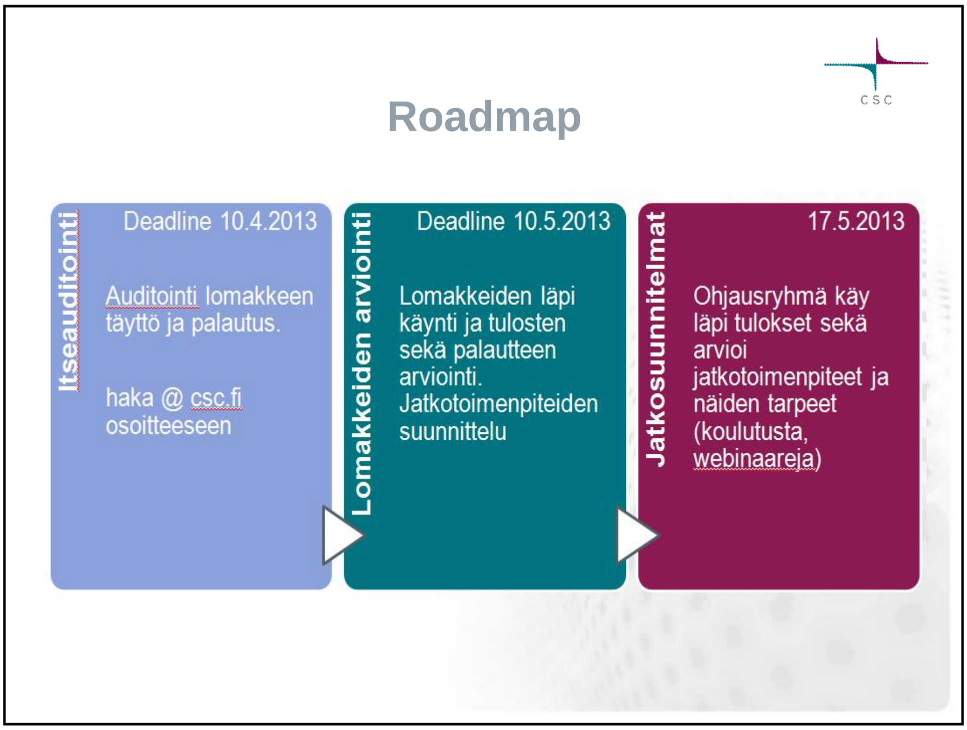
”IdP:n ylläpito on keskeisessä roolissa luottamusverkoston tietoturvassa”



Itseauditointilomake

- Itsearviointilomake kokoaa yhteen oleellisimmat tietoturvavaatimukset IdP:n suojaamiseksi.
  - Kattaa ja laajentaa vanhaa IdM-kuvausta
- Lähteinä on käytetty muiden luottamusverkostojen ja KANTARA-hankkeen vaatimuksia.
  - Näistä on otettu oleelliset kohdat
- Kaikille sama sapluuna
- Löytyy osoitteesta

http://www.csc.fi/hallinto/haka/ohjeet/liittyminen/Haka-self-assessment-questionnaire



Roadmap

Itseauditointi

Deadline 10.4.2013

Auditointi lomakkeen täyttö ja palautus.

haka @ csc.fi osoitteeseen

Lomakkeiden arviointi

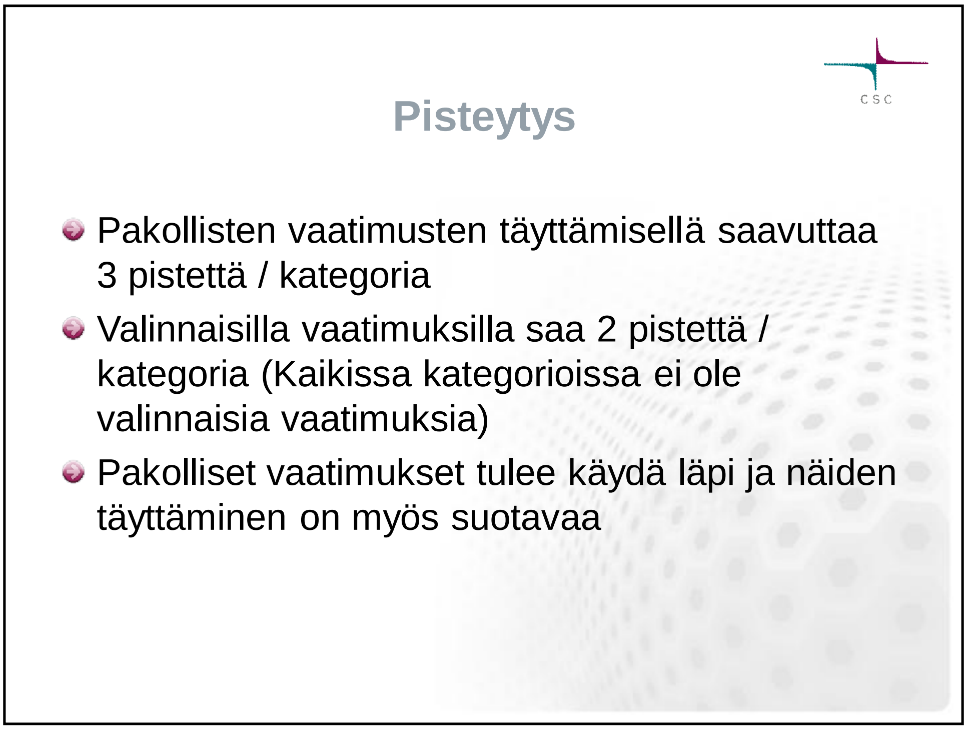
Deadline 10.5.2013

Lomakkeiden läpi käynti ja tulosten sekä palautteen arviointi. Jatkotoimenpiteiden suunnittelu

Jatkosuunnitelmat

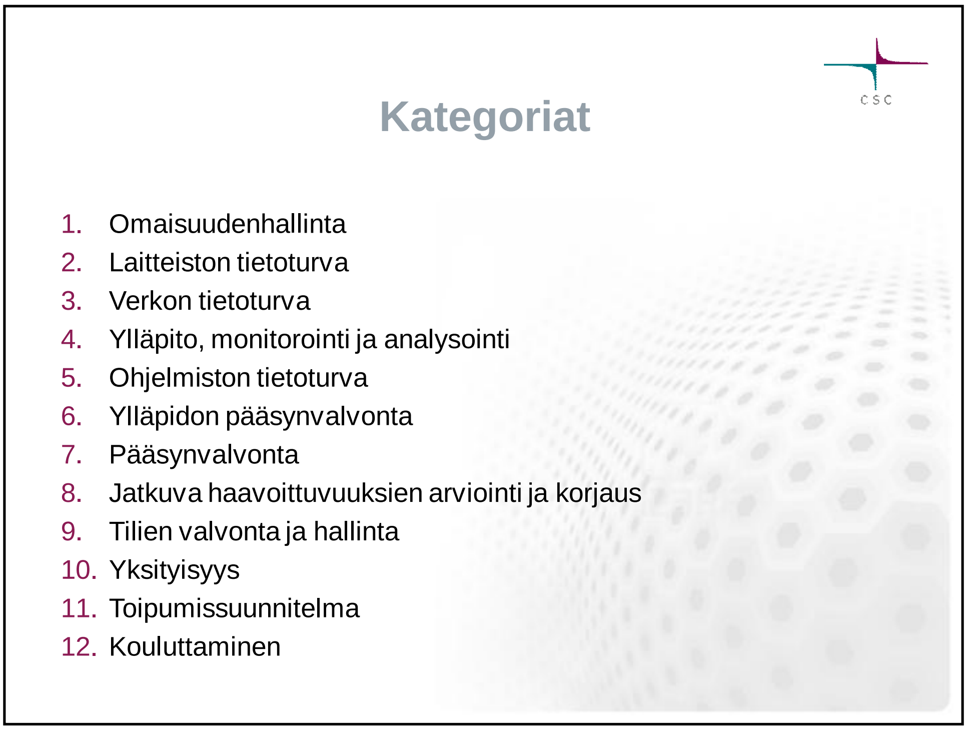
17.5.2013

Ohjausryhmä käy läpi tulokset sekä arvioi jatkotoimenpiteet ja näiden tarpeet (koulutusta, webinaareja)



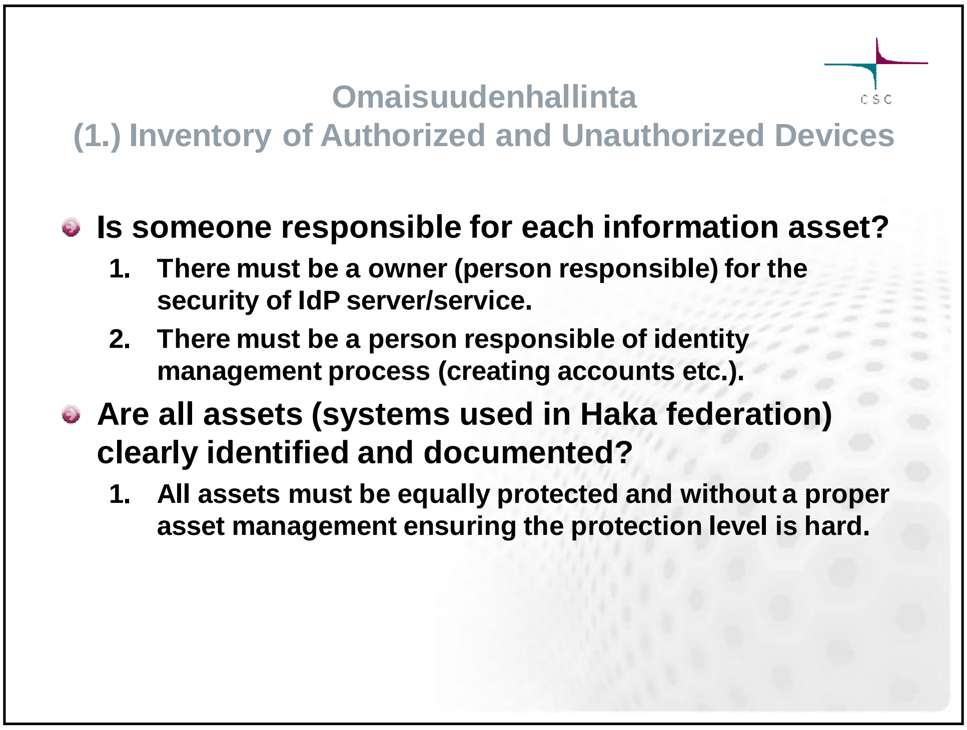
Pisteytys

- Pakollisten vaatimusten täyttämisellä saavuttaa 3 pistettä / kategoria
- Valinnaisilla vaatimuksilla saa 2 pistettä / kategoria (Kaikissa kategorioissa ei ole valinnaisia vaatimuksia)
- Pakolliset vaatimukset tulee käydä läpi ja näiden täyttäminen on myös suotavaa



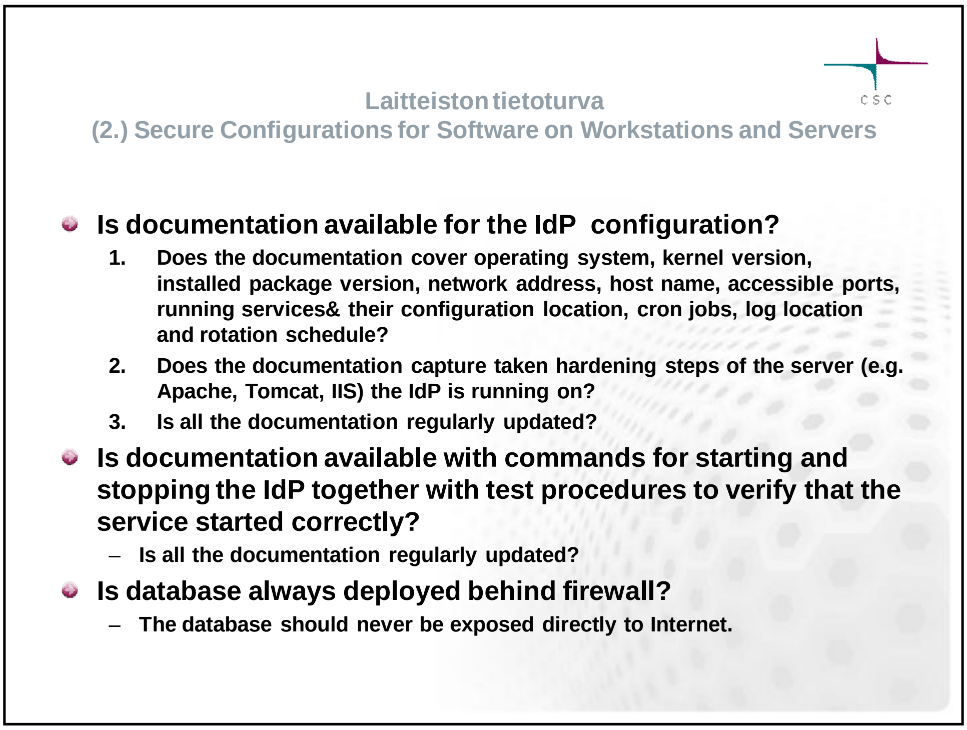
Kategoriat

1. Omaisuudenhallinta
2. Laitteiston tietoturva
3. Verkon tietoturva
4. Ylläpito, monitorointi ja analysointi
5. Ohjelmiston tietoturva
6. Ylläpidon pääsynvalvonta
7. Pääsynvalvonta
8. Jatkuva haavoittuvuuksien arviointi ja korjaus
9. Tilien valvonta ja hallinta
10. Yksityisyys
11. Toipumissuunnitelma
12. Kouluttaminen



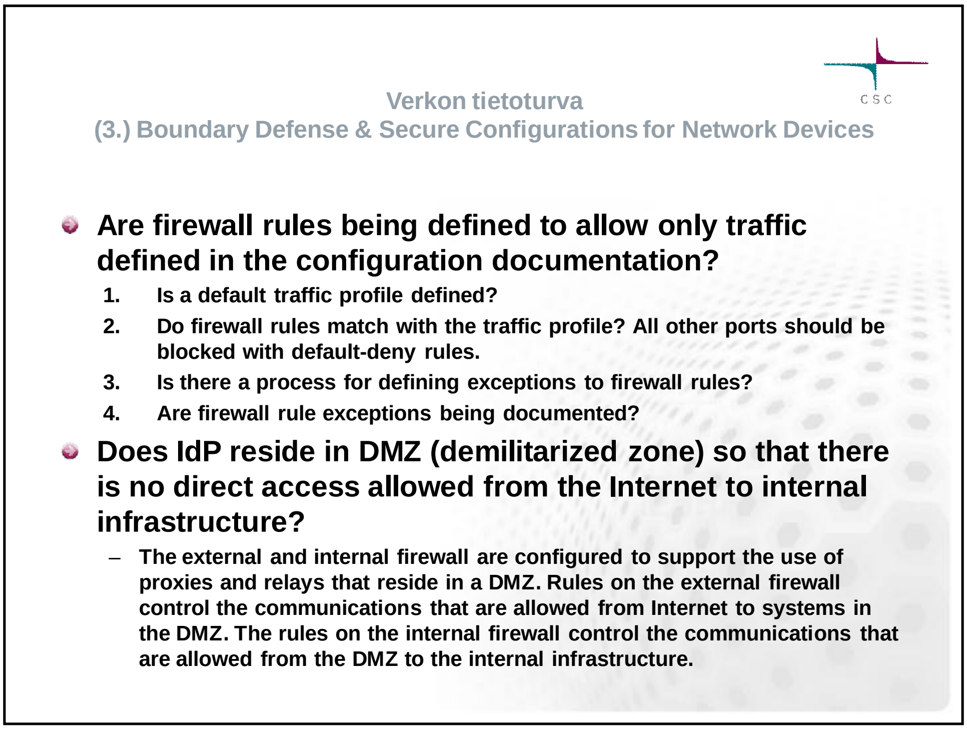
Omaisuudenhallinta
(1.) Inventory of Authorized and Unauthorized Devices

- Is someone responsible for each information asset?
  1. There must be a owner (person responsible) for the security of IdP server/service.
  2. There must be a person responsible of identity management process (creating accounts etc.).
- Are all assets (systems used in Haka federation) clearly identified and documented?
  1. All assets must be equally protected and without a proper asset management ensuring the protection level is hard.



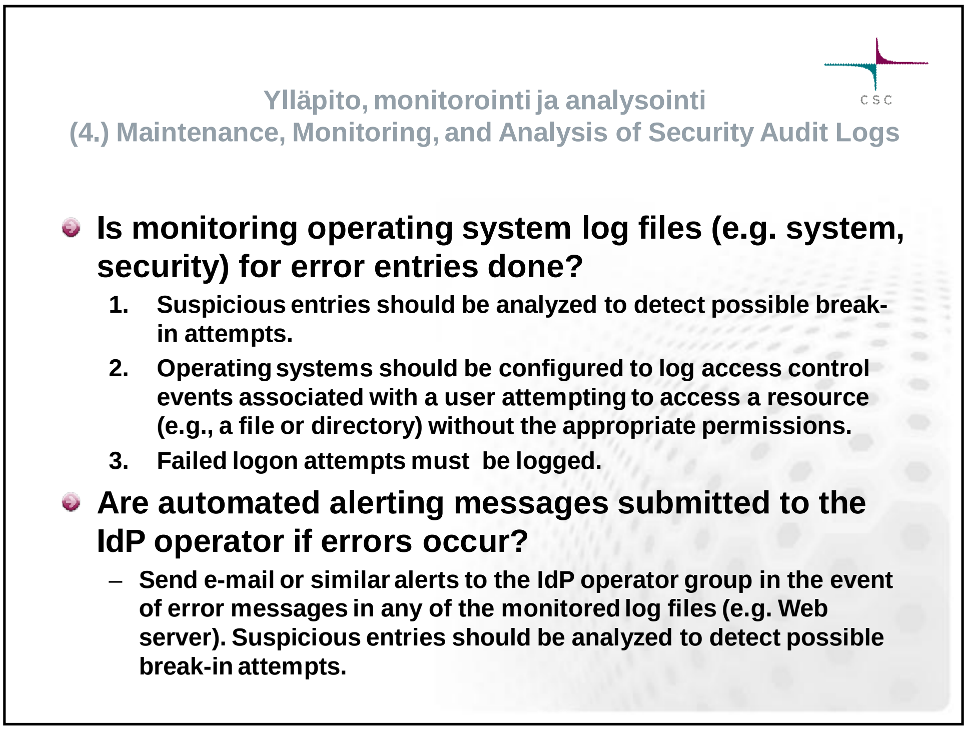
Laitteiston tietoturva
(2.) Secure Configurations for Software on Workstations and Servers

- Is documentation available for the IdP configuration?
  1. Does the documentation cover operating system, kernel version, installed package version, network address, host name, accessible ports, running services& their configuration location, cron jobs, log location and rotation schedule?
  2. Does the documentation capture taken hardening steps of the server (e.g. Apache, Tomcat, IIS) the IdP is running on?
  3. Is all the documentation regularly updated?
- Is documentation available with commands for starting and stopping the IdP together with test procedures to verify that the service started correctly?
  - Is all the documentation regularly updated?
- Is database always deployed behind firewall?
  - The database should never be exposed directly to Internet.



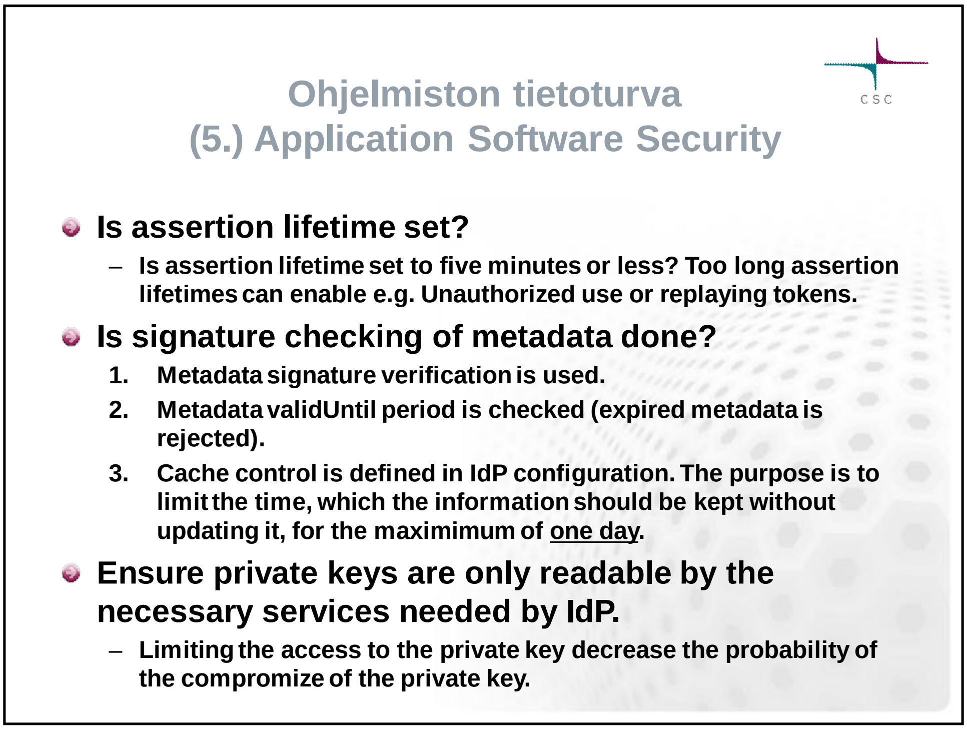
Verkon tietoturva
(3.) Boundary Defense & Secure Configurations for Network Devices

- **Are firewall rules being defined to allow only traffic defined in the configuration documentation?**
  1. Is a default traffic profile defined?
  2. Do firewall rules match with the traffic profile? All other ports should be blocked with default-deny rules.
  3. Is there a process for defining exceptions to firewall rules?
  4. Are firewall rule exceptions being documented?
- **Does IdP reside in DMZ (demilitarized zone) so that there is no direct access allowed from the Internet to internal infrastructure?**
  – The external and internal firewall are configured to support the use of proxies and relays that reside in a DMZ. Rules on the external firewall control the communications that are allowed from Internet to systems in the DMZ. The rules on the internal firewall control the communications that are allowed from the DMZ to the internal infrastructure.



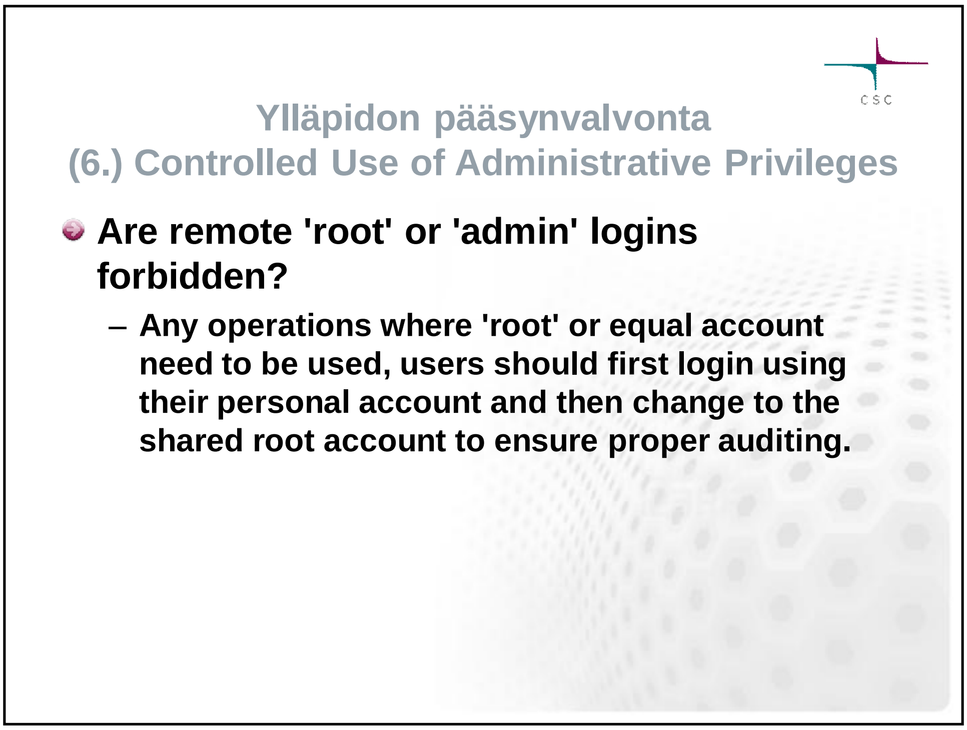
Ylläpito, monitorointi ja analysointi
(4.) Maintenance, Monitoring, and Analysis of Security Audit Logs

- **Is monitoring operating system log files (e.g. system, security) for error entries done?**
  1. Suspicious entries should be analyzed to detect possible break-in attempts.
  2. Operating systems should be configured to log access control events associated with a user attempting to access a resource (e.g., a file or directory) without the appropriate permissions.
  3. Failed logon attempts must be logged.
- **Are automated alerting messages submitted to the IdP operator if errors occur?**
  – Send e-mail or similar alerts to the IdP operator group in the event of error messages in any of the monitored log files (e.g. Web server). Suspicious entries should be analyzed to detect possible break-in attempts.



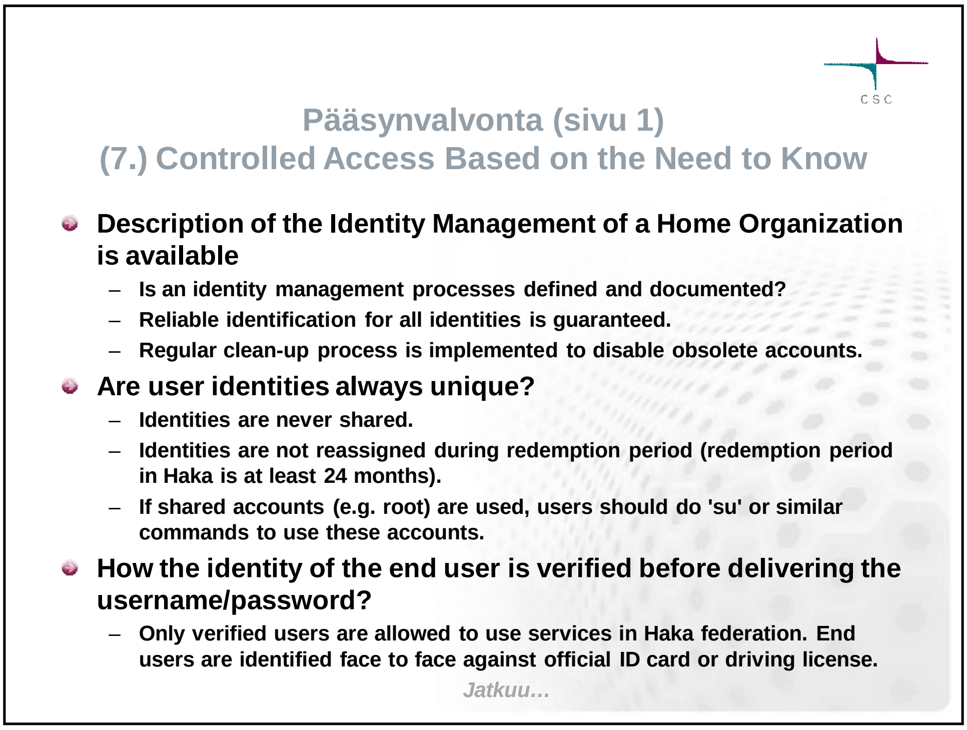
Ohjelmiston tietoturva
(5.) Application Software Security

- Is assertion lifetime set?
  - Is assertion lifetime set to five minutes or less? Too long assertion lifetimes can enable e.g. Unauthorized use or replaying tokens.
- Is signature checking of metadata done?
  1. Metadata signature verification is used.
  2. Metadata validUntil period is checked (expired metadata is rejected).
  3. Cache control is defined in IdP configuration. The purpose is to limit the time, which the information should be kept without updating it, for the maximimum of one day.
- Ensure private keys are only readable by the necessary services needed by IdP.
  - Limiting the access to the private key decrease the probability of the compromize of the private key.



Ylläpidon pääsynvalvonta
(6.) Controlled Use of Administrative Privileges

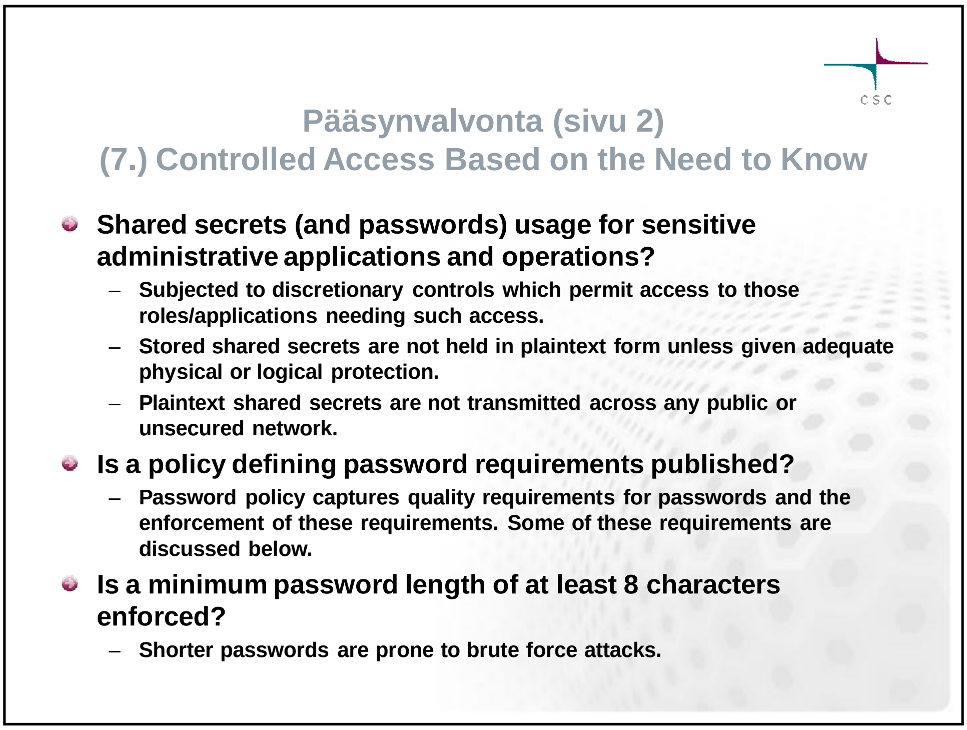
- Are remote 'root' or 'admin' logins forbidden?
  - Any operations where 'root' or equal account need to be used, users should first login using their personal account and then change to the shared root account to ensure proper auditing.



Pääsynvalvonta (sivu 1)
(7.) Controlled Access Based on the Need to Know

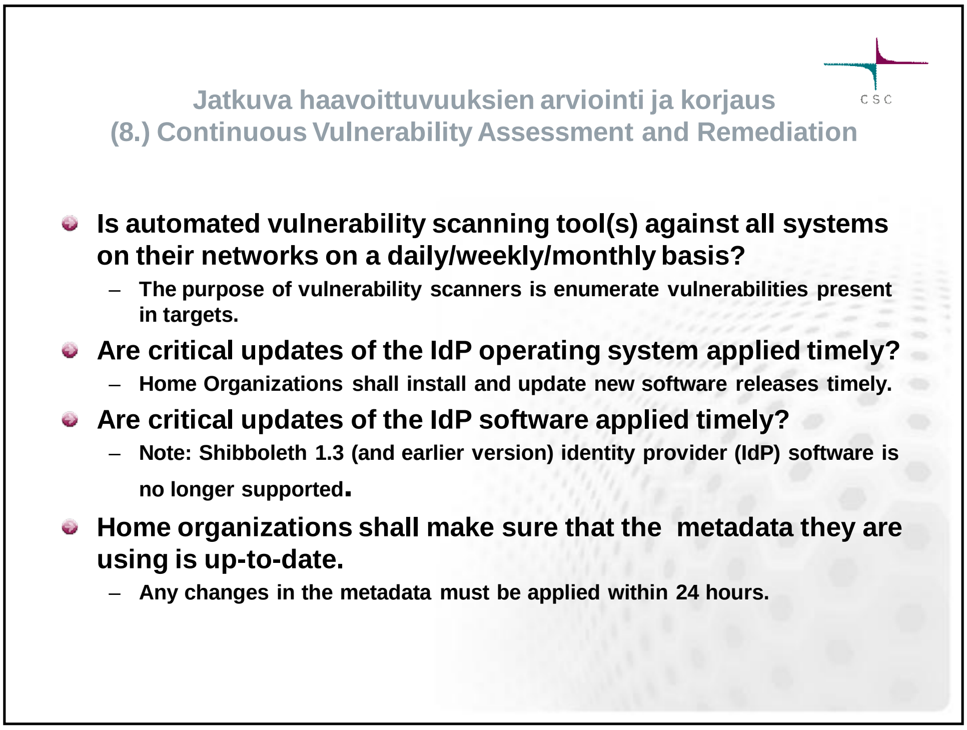
- **Description of the Identity Management of a Home Organization is available**
  - Is an identity management processes defined and documented?
  - Reliable identification for all identities is guaranteed.
  - Regular clean-up process is implemented to disable obsolete accounts.
- **Are user identities always unique?**
  - Identities are never shared.
  - Identities are not reassigned during redemption period (redemption period in Haka is at least 24 months).
  - If shared accounts (e.g. root) are used, users should do 'su' or similar commands to use these accounts.
- **How the identity of the end user is verified before delivering the username/password?**
  - Only verified users are allowed to use services in Haka federation. End users are identified face to face against official ID card or driving license.

Jatkuu…



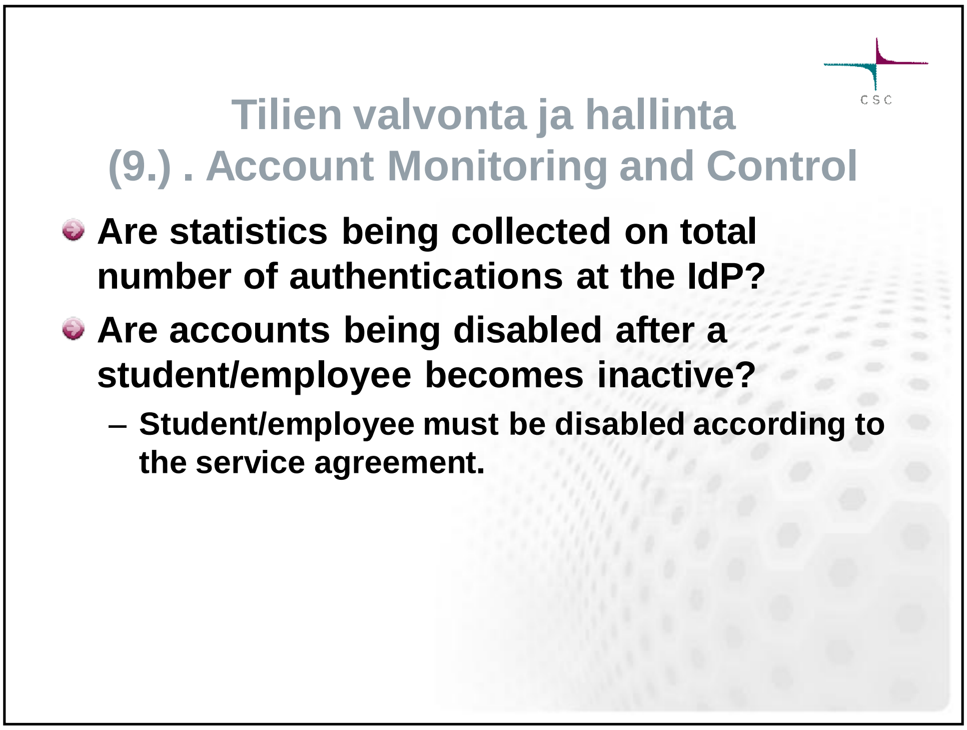
Pääsynvalvonta (sivu 2)
(7.) Controlled Access Based on the Need to Know

- **Shared secrets (and passwords) usage for sensitive administrative applications and operations?**
  - Subjected to discretionary controls which permit access to those roles/applications needing such access.
  - Stored shared secrets are not held in plaintext form unless given adequate physical or logical protection.
  - Plaintext shared secrets are not transmitted across any public or unsecured network.
- **Is a policy defining password requirements published?**
  - Password policy captures quality requirements for passwords and the enforcement of these requirements. Some of these requirements are discussed below.
- **Is a minimum password length of at least 8 characters enforced?**
  - Shorter passwords are prone to brute force attacks.



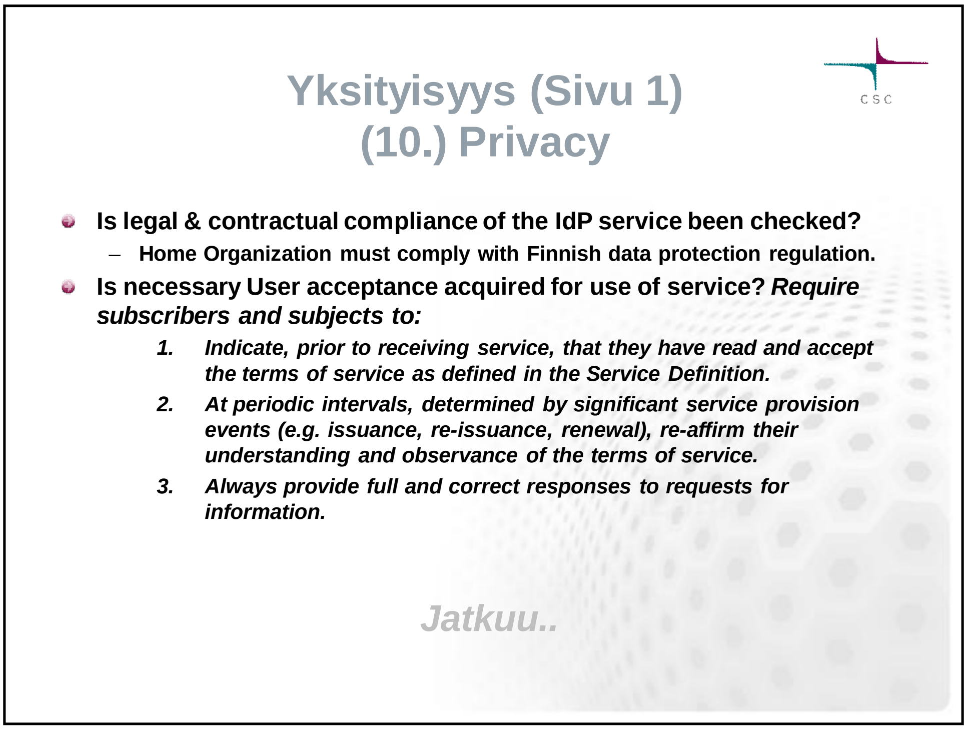
Jatkuva haavoittuvuuksien arviointi ja korjaus (8.) Continuous Vulnerability Assessment and Remediation

- Is automated vulnerability scanning tool(s) against all systems on their networks on a daily/weekly/monthly basis?
  - The purpose of vulnerability scanners is enumerate vulnerabilities present in targets.
- Are critical updates of the IdP operating system applied timely?
  - Home Organizations shall install and update new software releases timely.
- Are critical updates of the IdP software applied timely?
  - Note: Shibboleth 1.3 (and earlier version) identity provider (IdP) software is no longer supported.
- Home organizations shall make sure that the metadata they are using is up-to-date.
  - Any changes in the metadata must be applied within 24 hours.



Tilien valvonta ja hallinta (9.) . Account Monitoring and Control

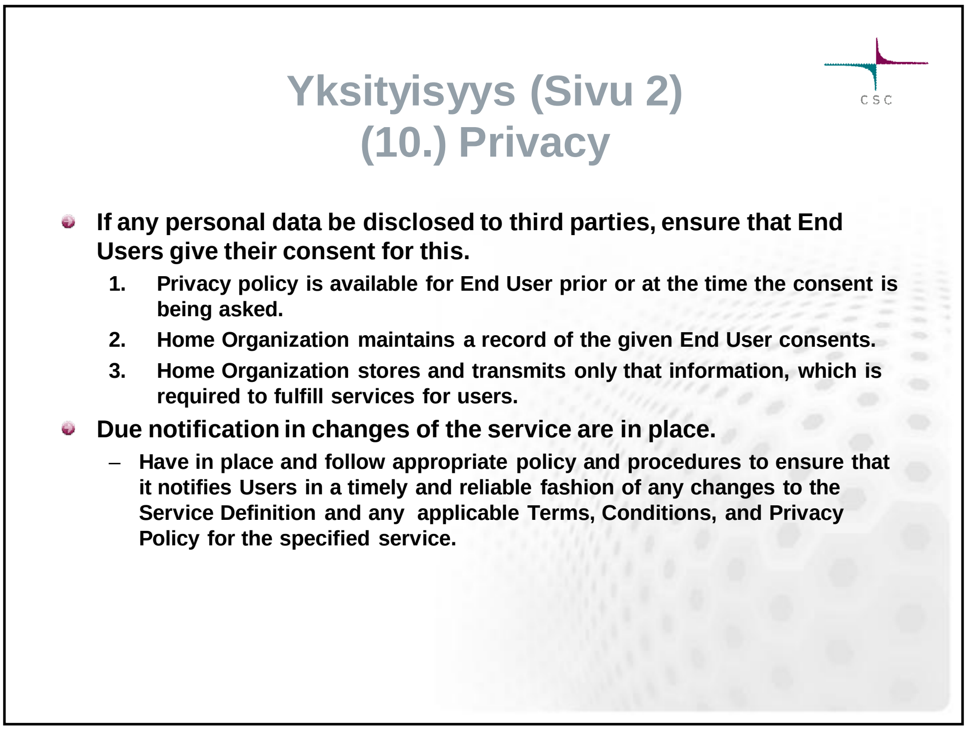
- Are statistics being collected on total number of authentications at the IdP?
- Are accounts being disabled after a student/employee becomes inactive?
  - Student/employee must be disabled according to the service agreement.



Yksityisyys (Sivu 1)
(10.) Privacy

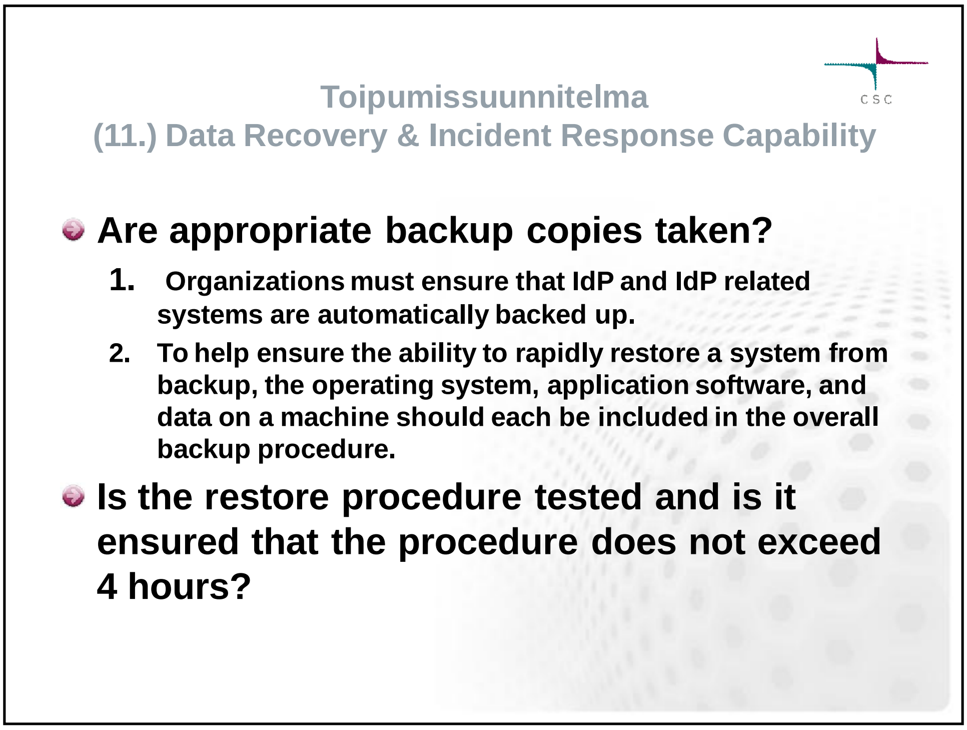
- Is legal & contractual compliance of the IdP service been checked?
  - Home Organization must comply with Finnish data protection regulation.
- Is necessary User acceptance acquired for use of service? *Require subscribers and subjects to:*
  1. *Indicate, prior to receiving service, that they have read and accept the terms of service as defined in the Service Definition.*
  2. *At periodic intervals, determined by significant service provision events (e.g. issuance, re-issuance, renewal), re-affirm their understanding and observance of the terms of service.*
  3. *Always provide full and correct responses to requests for information.*

Jatkuu..



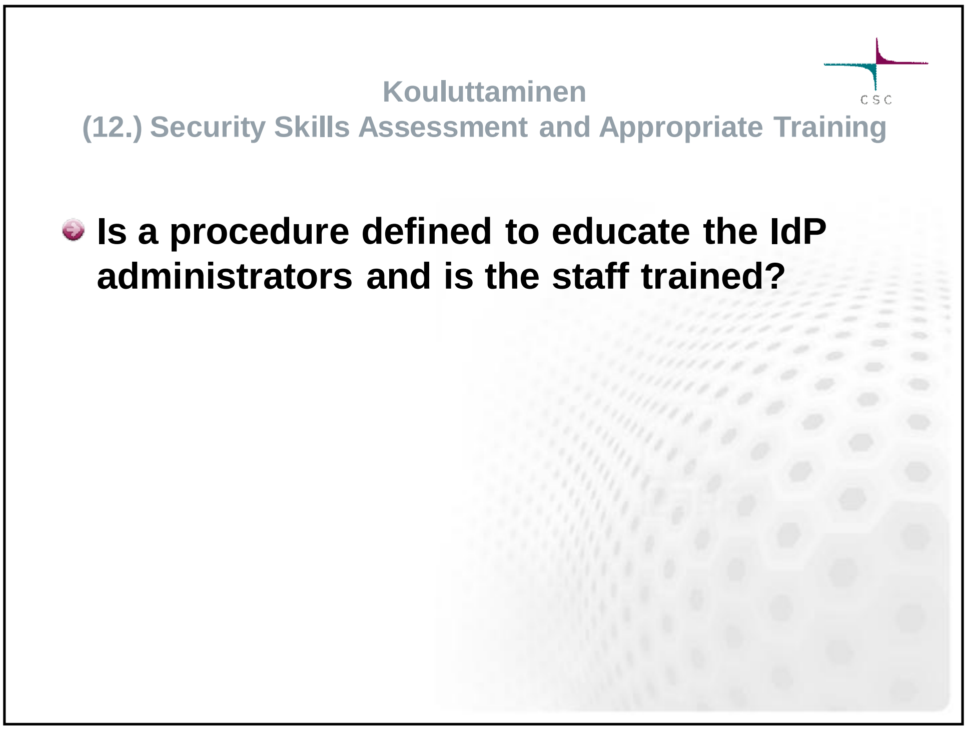
Yksityisyys (Sivu 2)
(10.) Privacy

- If any personal data be disclosed to third parties, ensure that End Users give their consent for this.
  1. Privacy policy is available for End User prior or at the time the consent is being asked.
  2. Home Organization maintains a record of the given End User consents.
  3. Home Organization stores and transmits only that information, which is required to fulfill services for users.
- Due notification in changes of the service are in place.
  - Have in place and follow appropriate policy and procedures to ensure that it notifies Users in a timely and reliable fashion of any changes to the Service Definition and any applicable Terms, Conditions, and Privacy Policy for the specified service.



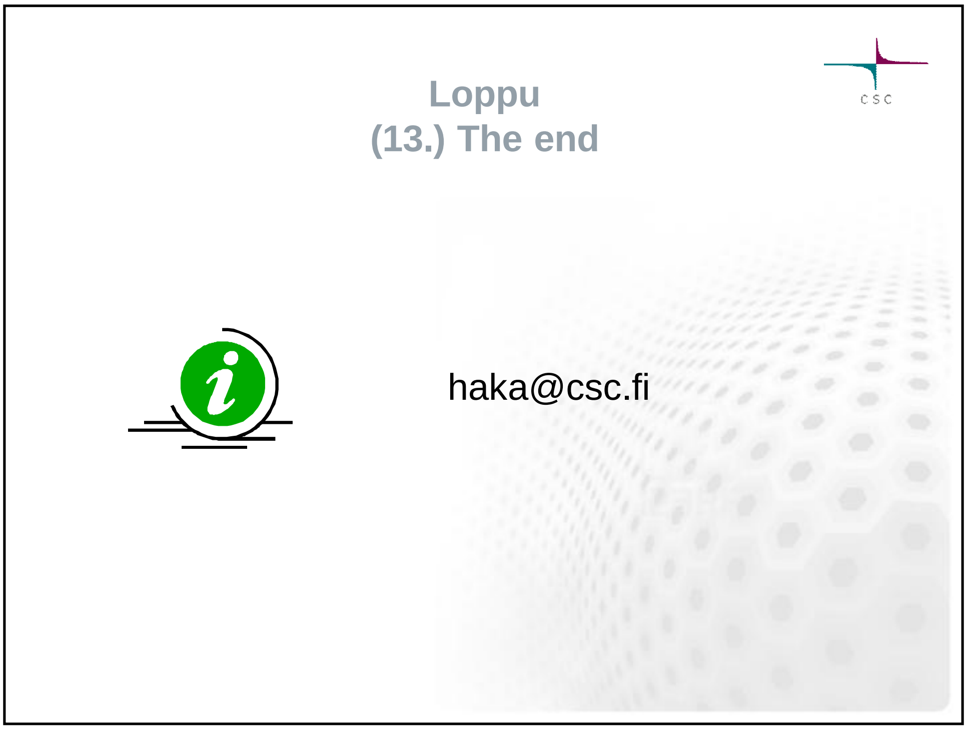
Toipumissuunnitelma
(11.) Data Recovery & Incident Response Capability

- **Are appropriate backup copies taken?**
  1. **Organizations must ensure that IdP and IdP related systems are automatically backed up.**
  2. **To help ensure the ability to rapidly restore a system from backup, the operating system, application software, and data on a machine should each be included in the overall backup procedure.**
- **Is the restore procedure tested and is it ensured that the procedure does not exceed 4 hours?**



Kouluttaminen
(12.) Security Skills Assessment and Appropriate Training

- **Is a procedure defined to educate the IdP administrators and is the staff trained?**



Loppu
(13.) The end

haka@csc.fi