Risk analysis for EMREX

All new systems connected to the EMREX network should be subject to a risk analysis.
This should be performed by the unit responsible for the system.
Below, you will find some risks that could be considered doing this analysis.

Risk	Probability	Impact	Actions	Comments
New HTTPS vulnerabilities are discovered. A hacker can replace NCP-list data being downloaded from EMREG. This makes it possible to set up a fake NCP server and produce fraudulant diplomas.	4	5	Use correct server security configuration. Use cryptographic signatures on data, in addition to HTTPS	Several critical SSL /TLS vulnerabilities have been found in recent years.
CA certificate leaked or abused	3	5	Use signature on data in addition to HTTPS or use custom list of custom Cas (trust store)	Comodo, diginotar, Chinese CA
EMREG is hacked. SMP is communicating with correct server but recieving false data.	2	5	Pen-testing regularly and before major releases to secure application.Patch OS and third party software. Log changes made by user in application.	
NCP is hacked. Places false data in EMREG	2	5	Responsibility of each NCP but login solution (yubikey etc) can make abuse of EMREG more difficult	
EMREG is DDOSed for several days during diploma deadline.	2	2	Anti DDOS measures and Caching	EMREG data can be cached. EMREG downtime may not matter much as long as cached data can be used
NCP is DDOSed. Unable to retrieve foreign diplomas from attacked country during attack.	2	4	Anti DDOS measures	Caching all diplomas is not an option
Rogue employees	1	5	Good practices	
EMREG downtime	2	2	Redundancy and alerts	
NCP or Result service downtime	2	4	Redundancy and alerts	
Hostile code injected in SMP binaries (jar--file)	2	5	Reproducible/determenistic builds	
Hostile code injected in mobility plugin source code. Enabling forging diplomas and hacking systems using SMP	2	5	Good practice, open source, code--review	
NCP sends data against user's wish	3	5	NCP must ask for concent and make it very clear which data will be sent and where it will be sent. A white list of approved URLs for diploma delivery could be used to prevent fake web sites from receiving diplomas. Whitelisting might not be an option if EMREX is to be used by recruiting agencies etc.	
Open source. Makes it easy for hacker s to find vulnerabilities.	2	4	Bug bounty program.	

Min. probability value 1 - Very low (never occured)
Max. probability value 5 Very high (daily/always)
Min. impact value 1 - Can be ignored
Max. impact value 5 - Very high/catastrophic