CERT.LV

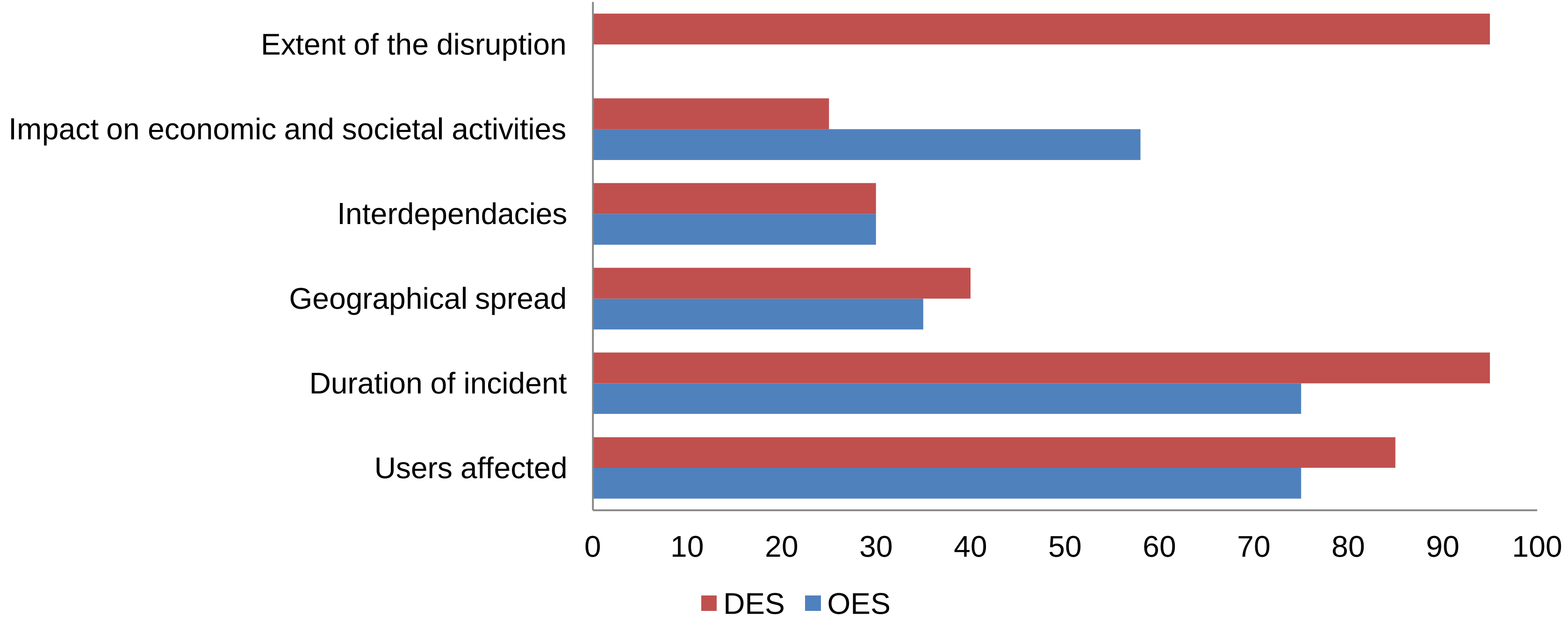
Informācijas tehnoloģiju
drošības incidentu
novēršanas institūcija

Incident reporting and security requirements

05.10.2017. – Riga, Latvia

<table>
<tr><th>Operators of essential services</th><th>Digital service providers</th></tr>
<tr><td colspan="2">SHOULD REPORT INCIDENT AFFECTING THE AVAILABILITY, AUTHENTICITY, INTEGRITY OR CONFIDENTIALITY OF</td></tr>
<tr><td>networks and information systems used in the provision of the essential services</td><td>data stored, transmitted or processed by a DSP through network and information systems</td></tr>
<tr><td colspan="2">WHICH HAS A</td></tr>
<tr><td>significant</td><td>substantial</td></tr>
<tr><td colspan="2">IMPACT</td></tr>
<tr><td>the continuity of the essential services</td><td>on the provision of the digital service offered</td></tr>
</table>

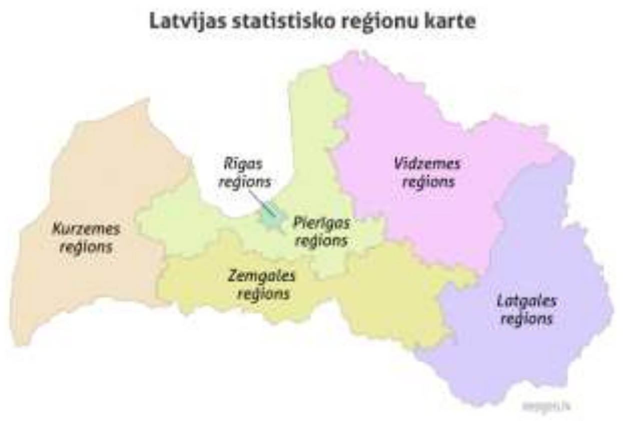
Criteria for reporting



Source: voluntary questioners of private sector players by ENISA

Criteria for reporting [LV]

	1 – 2h	2 - 4h	4 – 6h	6 – 8h	>8h
1 – 2%					🟥
2 – 5%				🟥	🟥
5 – 10%			🟥	🟥	🟥
10 – 15%		🟥	🟥	🟥	🟥
>15%	🟥	🟥	🟥	🟥	🟥


Latvijas statistisko reģionu karte

Only for DES - losses

<table>
<tr><td>Operators of essential services</td><td>Digital service providers identify and</td></tr>
<tr><td colspan="2">TAKE APPROPRIATE AND PROPORTIONATE TECHNICAL AND ORGANISATIONAL MEASURES TO MANAGE THE RISKS POSED TO THE SECURITY OF NETWORK AND INFORMATION SYSTEMS WHICH THEY USE</td></tr>
<tr><td>in their operations.</td><td>in the context of offering services referred to in Annex III within the Union.</td></tr>
<tr><td colspan="2">HAVING REGARD TO THE STATE OF THE ART, THOSE MEASURES SHALL ENSURE A LEVEL OF SECURITY OF NETWORK AND INFORMATION SYSTEMS APPROPRIATE TO THE RISK POSED</td></tr>
<tr><td></td><td>and shall take into account the following elements:
(a) the security of systems and facilities;
(b) incident handling;
(c) business continuity management;
(d) monitoring, auditing and testing;
(e) compliance with international standards.</td></tr>
</table>

Security requirements [LV]

	Existing legal framework	NIS requirements
A.5: Information security policies	✓	
A.6: Organization of information security	✓	
A.7: Human resource security	✓	
A.8: Asset management	✓	✓
A.9: Access control	✓	✓
A.10: Cryptography		
A.11: Physical and environmental security	✓	✓
A.12: Operations security		
A.13: Communications security	✓	
A.14: System acquisition, development and maintenance	✓	
A.15: Supplier relationships	✓	
A.16: Information security incident management	✓	✓
A.17: Information security aspects of business continuity management	✓	✓
A.18: Compliance		✓

(Illustrated by control groups from ISO/IEC 27001:2013)