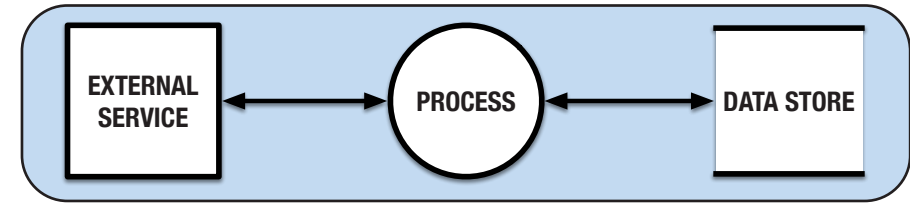


<b>S</b> poofing	Authentication	Fraudulent Data Impersonating legitimate Users Pretending to be something it isn't
<b>T</b> ampering	Integrity	Unauthorised changes to Data Man-In-The-Middle (MITM) Interfering with Data Integrity
<b>R</b> epudiation	Non-Repudiation	Is there an Audit Trail? Can an Attacker hide their activity? Prevented logging of user actions
<b>I</b> nformation	Confidentiality	Data transmitted un-encrypted Leaking of Personal Data (PII) Inadequate Access Control List (ACL)
<b>D</b> enial	Availability	Inaccessbile products or services Resource exhaustion Reduced performance
<b>E</b> levation	Authorisation	Bugs, exploits and misconfiguration increas- ing a user's access level Users being able to access services or resources which they shouldn't

<div>Low 3</div> <div>Medium 6</div> <div>High 8</div> <div>Critical 10</div>		
<b>D</b> amage	How much damage would this vulnerability cause if exploited?	How bad would an attack be? From the Business and Service perspectives
<b>R</b> eproducability	How difficult is it to reproduce this vulnerability?	How easy is it to reproduce? Is it predictable or unpredictable? Are there other factors required?
<b>E</b> xploitability	How easy is it to exploit?	How easy is it to exploit? Is exploiting simple or complex? Requires multiple vulnerabilities?
<b>A</b> ffected	Who is affected?	How many users will it impact? Does it affect only service users?
<b>D</b> iscoverability	How difficult is it to discover this vulnerability?	How easy is it to discover the vulnerability? Exposed configuration information



<b>S</b> poofing	Authentication	Fraudulent Data Impersonating legitimate Users Pretending to be something it isn't
<b>T</b> ampering	Integrity	Unauthorised changes to Data Man-In-The-Middle (MITM) Interfering with Data Integrity
<b>R</b> epudiation	Non-Repudiation	Is there an Audit Trail? Can an Attacker hide their activity? Prevented logging of user actions
<b>I</b> nformation	Confidentiality	Data transmitted un-encrypted Leaking of Personal Data (PII) Inadequate Access Control List (ACL)
<b>D</b> enial	Availability	Inaccessbile products or services Resource exhaustion Reduced performance
<b>E</b> levation	Authorisation	Bugs, exploits and misconfiguration increas- ing a user's access level Users being able to access services or resources which they shouldn't

<div>Low 3</div> <div>Medium 6</div> <div>High 8</div> <div>Critical 10</div>		
<b>D</b> amage	How much damage would this vulnerability cause if exploited?	How bad would an attack be? From the Business and Service perspectives
<b>R</b> eproducability	How difficult is it to reproduce this vulnerability?	How easy is it to reproduce? Is it predictable or unpredictable? Are there other factors required?
<b>E</b> xploitability	How easy is it to exploit?	How easy is it to exploit? Is exploiting simple or complex? Requires multiple vulnerabilities?
<b>A</b> ffected	Who is affected?	How many users will it impact? Does it affect only service users?
<b>D</b> iscoverability	How difficult is it to discover this vulnerability?	How easy is it to discover the vulnerability? Exposed configuration information