Self assessment

Algemeen:

- Zijn er REFs/explains voor dit systeem aanwezig? Zo ja, welke?
- Wordt de omgeving intern binnen het UWV netwerk of extern gehost?

Soort applicatie:

- Is de te testen omgeving een webapplicatie of een SOAP/RESTFUL API?
  - Wordt er **consistent** gebruik gemaakt van een web framework voor de webapplicatie?
    - Bv: ASP.NET, PHP Laravel, Python Django, RESTful API, MVC
    - In het geval van:
      - GEEN MVC (Model View Controller) applicatie of een MVC framework dat geen gebruik maakt van ORM (Object Relational Mapping),
      - De applicatie niet consequent gebruik maakt het MVC framework met ORM: stuur een stukje broncode mee waar en hoe met de database wordt gecommuniceerd
  - Is er door de leverancier/ontwikkelaar een **installatie/ontwerp/configuratie handleiding** meegeleverd waar configuratie en hardening van de webserver wordt beschreven?
    - Deze bevat informatie over benodigde openstaande poorten, te accepteren HTTP methods en headers.
    - Zo ja, graag de handleiding meesturen
    - Wordt er gebruik gemaakt van hardening richtlijnen op de webservers zoals CIS of STIG? Zo ja, geef aan welke richtlijnen gevolgd worden of voeg (een verwijzing naar) de richtlijn toe.

Authenticatie & Autorisatie:

- Is er een proces voor het bijhouden van gebruikers en rechten? Hoe is dit bv. als een gebruiker uit dienst gaat?
- Wordt er gebruik gemaakt van een autorisatiematrix en/of gegroepeerde rechten?
  - Lever een autorisatiematrix op als bewijs.
- In het geval van een interne applicatie:
  - Indien er geen gebruik gemaakt wordt van gebruikers uit de Active Directory/ SSO (Single Sign On), waarom niet?

Gevoelige data:

- Worden gevoelige transacties/data verwerkt door de applicatie?
  - Is er een BBN/BIV/RAL classificatie?
  - Is er een GEB of risico analyse voor de omgeving gedaan?
  - Zo ja: hoe wordt omgegaan met traceerbaarheid en onweerlegbaarheid (a.d.h.v. logging van transacties gekoppeld aan gebruiker die het heeft uitgevoerd)
  - Wordt er gebruik gemaakt van encryptie om gevoelige data te beveiligen? (Bijvoorbeeld encryptie van gedeeltelijke of volledige berichtinhoud, digitale handtekeningen) Zo ja, licht toe hoe precies en maak hierbij onderscheid tussen data-in-transit en data-at-rest.
- In het geval van een interne applicatie:
  - Is de applicatie kritiek in de keten?
    - Zo ja, wat voor overige maatregelen zijn er genomen om deze te beschermen?
      - Graag een HLD document meesturen.

Database informatie:

- Wordt er gebruik gemaakt van geparametriseerde queries?
  - Lever bewijs in de vorm van gebruikte queries/code.

Stack:

- Welke soft- en middelware gebruikt de applicatie:
  - 1. Stuur een overzicht van de gebruikte server software + versies (webservice versie, php/asp versie, sql versie).
    - Bv HLD, Confipedia, SBoM.
  - 2. Optioneel kan ook een Directory listing van de webroot worden meegestuurd, hierdoor hoeven wij minder scans op de server te doen en hebben we een beter beeld van de applicatie.
- Interne apps: Wijkt de gebruikte onderliggende software (stack) af van de UWV ondersteunde applicatielijst?

Logging en detectie/monitoring:

- Wat voor events worden er **gelogd**? Bv: succesvolle/niet succesvolle authenticaties
  - Is er een bewuste keuze gemaakt voor wat voor security/privacy events van de applicatie er **gelogd** worde

        - Wordt er **gemonitord** op deze events, zo ja welke en hoe?
- Logt de applicatie naar een **centrale logging server**
    - **Bv:** (R)syslog, Windows Event Viewer, SNMP database- en applicatielogging
- Interne applicatie?
    - Monitort het UWV SOC op specifieke dreigingen m.b.t. deze applicatie? Zijn er use cases afgestemd?

Patch en lifecycle management

- Indien extern gehoste applicaties/SaaS oplossingen:
    - Is er patch**beleid** binnen de organisatie beschikbaar? Zo ja, geef aan wat dit beleid inhoudt.
- Is er een patchbeleid en **proces** voor de hele applicatie stack? Zo ja, voeg hieronder een korte beschrijving van het beleid/proces toe.
- Hoe wordt zicht gehouden op kwetsbaarheden bij gebruikte server software, componenten of libraries (bv Apache, PHP, Jquery)
    - Bv d.m.v.:
        - Software Component Analysis (SCA) van Third-Party Components (TPC) mbv Software Bill of Materials (SBoM)
        - OWASP Dependency Check in CI/CD pipeline
- Via welke route kunnen beheerders op de omgeving aanmelden voor het updaten van de software? (Is er bijvoorbeeld een aparte opgang of interface beschikbaar voor het uitvoeren van beheerwerkzaamheden?)

Netwerk:

- Wordt er host isolatie, (micro)netwerksegmentatie (bijvoorbeeld een DMZ) of whitelisting toegepast op de front/backend services? Zo ja, licht toe wat er wordt toegepast?
- Hoe is de authenticatie ingeregeld van het frontend systeem naar het backend systeem?
- Wordt de applicatie en het netwerkverkeer beschermd door middel van detectie- en protectiemechanismen? (Denk hierbij aan een WAF of een IDS/IPS) Zo ja, geef aan wat er is ingericht.