Hartelijk welkom!

1. Wie is DNV GL?

2. Certificering van managementsystemen

Geboren uit …

DNV·GL

DNV

GL Group

KEMA

NOBLE DENTON

GARRAD HASSAN

ADVANTICA

Sinds 1864 uitgegroeid naar wereldwijde TIC dienstverlener

155
years

400
offices

100
countries

14,500
employees

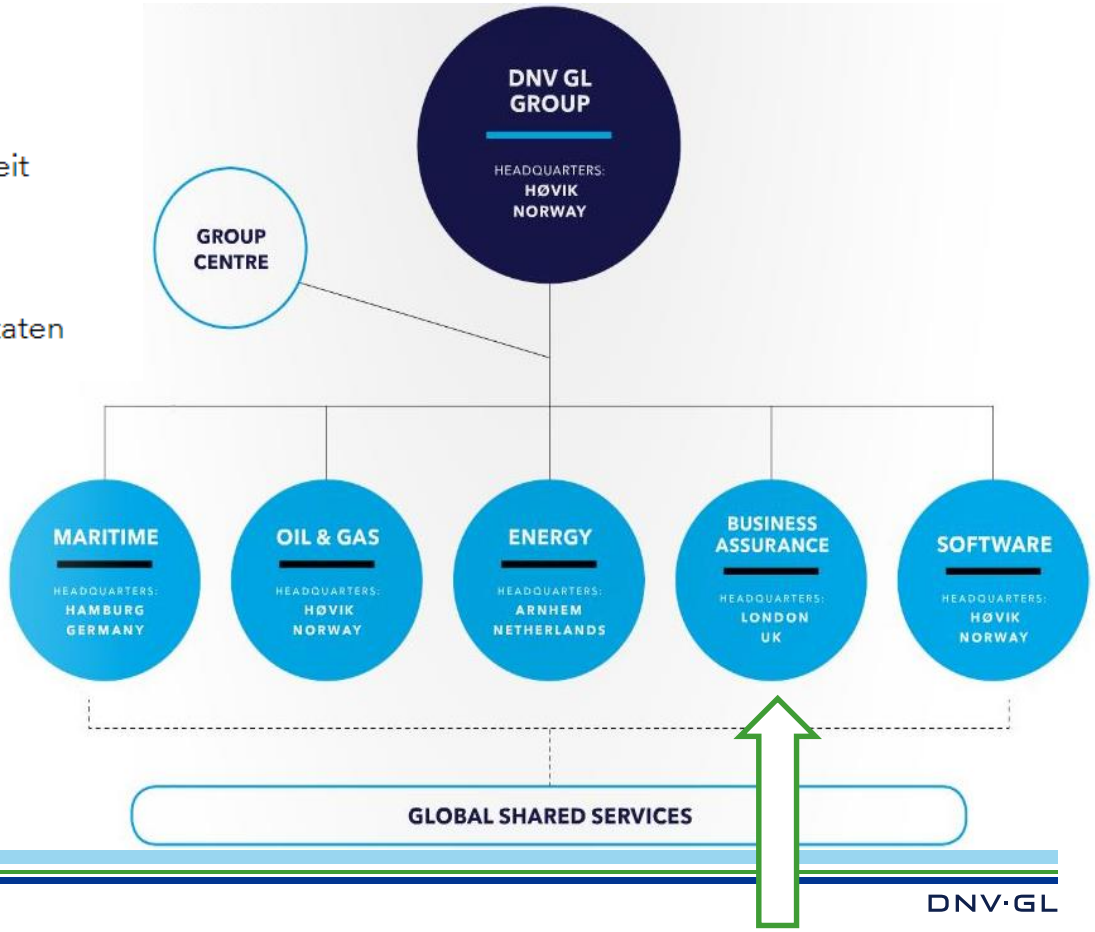
Dit is DNV GL

Doelstelling:
Het beschermen van leven, eigendommen en het milieu

Visie:
Wereldwijd bijdragen aan een veilige en duurzame toekomst

Waarden:

- We bouwen aan betrouwbaarheid en vertrouwen
- We doen geen concessies aan kwaliteit of integriteit
- We hechten belang aan teamwerk en innovatie
- We zorgen voor onze klanten en voor elkaar
- We staan open voor verandering en leveren resultaten



DNV GL Business Assurance

- Eén van 's werelds meest vooraanstaande certificerende instellingen en actief in:

Managementsysteemcertificatie	Product Certificatie	Persoonscertificatie
Training	Assessments	Consulting

- Meer dan 90.000 uitgegeven certificaten wereldwijd.
- Veel ervaring en een goede reputatie in alle sectoren.
- Alle vereiste erkenningen en accreditaties.
- Duurzaam, innovatief en vaak betrokken bij de ontwikkeling van nieuwe initiatieven.
- Unieke klantgerichte werkwijze "Risk Based Certification" → De klant bepaalt de focus.

Managementsysteem certificering

Wat is een managementsysteem?

Systeem – Verzameling gerelateerde of op elkaar inwerkende elementen

Systematisch werken – Om effectief te zijn, moeten de zaken op een passende/praktische manier zijn georganiseerd en in een bepaalde volgorde worden uitgevoerd

Managementsysteem – Verzameling gerelateerde of op elkaar inwerkende elementen van een organisatie voor het opstellen van beleid en doelstellingen en van processen voor het realiseren van deze doelstellingen

Managementsysteem certificering

Ook wel "*ISO Certificering*" genoemd.

- ISO normen:
  - Voorzien in eisen (criteria) voor het vaststellen, implementeren, bijhouden en continu verbeteren van een managementsysteem.
  - Een systematische benadering ter verandering en continue verbetering (PDCA).
  - Internationaal vastgestelde en erkende normen geschikt voor certificering.
  - Op het gebied van kwaliteit, veiligheid, continuïteit en milieu.
- Een ISO norm bevat eisen waar een organisatie aantoonbaar aan moet voldoen.
- Het managementsysteem beschrijft hoe de organisatie aan de eisen voldoet.
- Certificering kan na een volledige implementatie van het managementsysteem.

Het certificatieproces

<u>Optioneel:</u>
Nulmeting, proefaudits of positiebepaling

<u>Fase 1:</u>
Kennismaking en documentatie-beoordeling

<u>Fase 2:</u>
Certificeringsaudit

Periodieke audit

Periodieke audit

Hercertificerings audit

Certificaat 3 jaar geldig

Tot zover vragen?

www.dnvgl.com

SAFER, SMARTER, GREENER

3. De audit van een managementsysteem

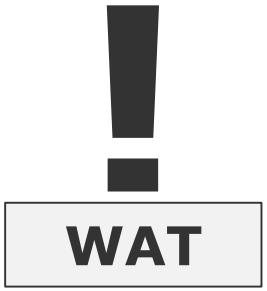
Managementsysteem: High Level Structure

Inleiding	4. Context van de organisatie	5. Leiderschap	6. Planning	7. Ondersteuning	8. Uitvoering	9. Evaluatie van de prestaties	10. Verbetering
1. Onderwerp en toepassingsgebied	4.1 Inzicht verkrijgen in de organisatie en haar context	5.1 Leiderschap en betrokkenheid	6.1 Maatregelen om risico's te beperken en kansen te benutten	7.1 Middelen	8.1 Operationele planning en beheersing	9.1 Monitoren, meten, analyseren en evalueren	10.1 Afwijkingen en corrigerende maatregelen
2. Normatieve verwijzingen	4.2 Inzicht verkrijgen in de behoeften en verwachtingen van belanghebbenden	5.2 Beleid	6.2 XXX doelstellingen en de planning om ze te bereiken	7.2 Competentie	8.2 Risicobeoordeling van informatie-beveiliging	9.2 Interne audit	10.2 Continue verbetering
3. Termen en definities	4.3 Het toepassings-gebied van het management-systeem voor XXX vaststellen	5.3 Rollen, verantwoordelijk-heden en bevoegd-heden binnen de organisatie		7.3 Bewustzijn	8.3 Informatie-beveiligingsrisico's behandelen	9.3 Directie-beoordeling	
	4.4 XXX management system			7.4 Communicatie			
				7.5 Gedocumenteerde informatie			

ISO 27001:2013 - Information security management systems

ANNEX A Referentiebeheers-doelstellingen en –maatregelen

ISO 27001:2013 Annex A.



A.5 Informatiebeveiligingsbeleid		
A.6 Organiseren van informatiebeveiliging	A.7 Veilig personeel	A.8 Beheer van bedrijfsmiddelen
A.9 Toegangsbeveiliging	A.10 Cryptografie	A.11 Fysieke beveiliging en beveiliging van de omgeving
A.12 Beveiliging bedrijfsvoering	A.13 Communicatiebeveiliging	A.14 Acquisitie, ontwikkeling en onderhoud van informatiesystemen
A.15 Leveranciersrelaties	A.16 Beheer van informatiebeveiligings-incidenten	A.17 Informatiebeveiligings-aspecten van bedrijfs-continuïteitsbeheer
A.18 Naleving		

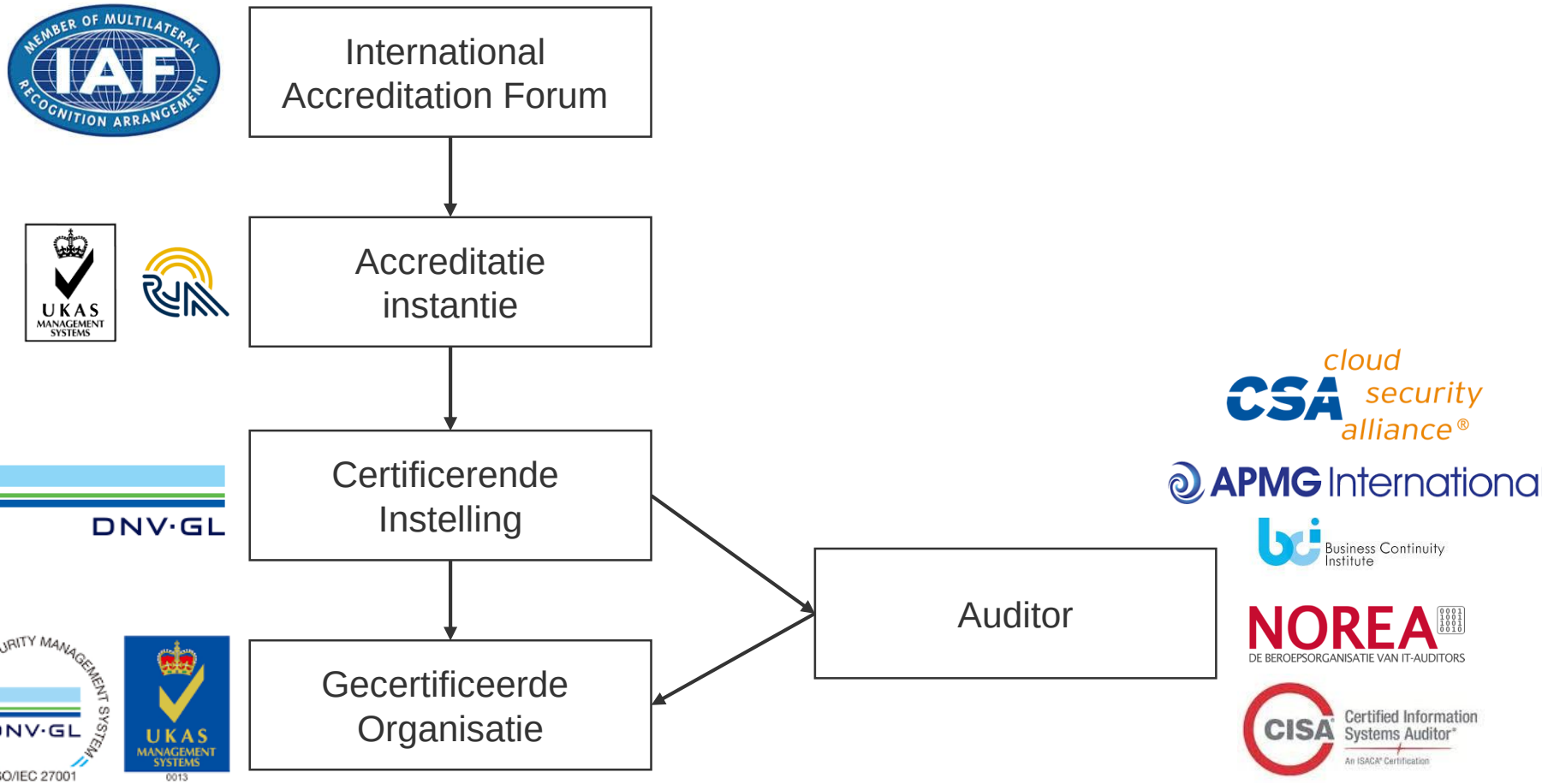
Onze andere normen / standaarden

- **ISO 27001** - Information security management systems
- **NEN 7510** - Informatiebeveiliging in de zorg
- **ISO 20000-1** - Service management system
- **ISO 22301** - Business continuity management systems

- **CSA STAR** - Cloud Security Alliance Security Trust Assurance and Risk registry
- **ISO 27017** - Code of practice for information security controls based on ISO 27002 for cloud services
- **ISO 27018** – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

- **ISO 28000** – Specification security management systems for the supply chain

Geaccrediteerde certificering



De audit van een managementsysteem

NEN-EN-ISO 19011 (nl)
Richtlijnen voor het uitvoeren van audits van managementsystemen

Nederlandse norm
Vervangt NEN-EN-ISO 19011:2011 (nl)
ICS 03.100.70; 03.120.10; 03.120.20; 13.020.10
Juli 2018

INTERNATIONAL STANDARD **ISO/IEC 17021-1**

First edition
2015-06-15

Conformity assessment — Requirements for bodies providing audit and certification of management systems —

Part 1:
Requirements

Évaluation de la conformité — Exigences pour les organismes procédant à l'audit et à la certification des systèmes de management — Partie 1: Exigences

Reference number
ISO/IEC 17021-1:2015(E)

© ISO/IEC 2015

Auditor (3.8) -
persoon die een audit (3.1) uitvoert

De audit (ISO 19011)

- **Audit (3.1)** - Systematisch, onafhankelijk en gedocumenteerd proces voor het verkrijgen van **auditbewijsmateriaal** (3.3) en het objectief beoordelen daarvan om vast te stellen in welke mate aan de **auditcriteria** (3.2) is voldaan

- **Auditbevindingen (3.10) -** Resultaten van de beoordeling van het verzamelde auditbewijsmateriaal (3.3) aan de hand van auditcriteria (3.2)
- *OPMERKING: Auditbevindingen geven conformiteit aan of wijzen op afwijkingen.*

- **Auditconclusie (3.5) -** resultaat van een audit (3.1), na overweging van de auditdoelstellingen en alle auditbevindingen (3.4)

De audit en de auditor

Auditcriteria
- ISO 27001
- Beleid
- Procedures
- Wet- en regelgeving
- Contractuele eisen

Auditbewijsmateriaal
- Interviews
- Observaties
- Registraties
- Rapportages
- Test resultaten

Vereiste situatie

Feitelijke situatie

Audit bevindingen

✓ **conformiteit**

× **afwijking**

Audit conclusie

Hoe wordt je ISO 27001 auditor (DNV)

- **Werkervaring** - minstens 4 jaar praktische werkervaring in ICT, waarvan minstens 2 jaar in een rol of functie gerelateerd aan informatiebeveiliging
- **Training** - met succes een 5-daagse training gevolgd met daarin de onderwerpen ISMS auditen en audit management
- **Audit ervaring** – Ervaring opgebouwd met ISMS audits door minstens 4 certificering audits (bij voorkeur volledige audits) uitgevoerd, totaal minstens 20 dagen onder supervisie van een gekwalificeerde ISO 27001 Lead Auditor.
- **Technical areas (sectoren)**
  - ICT
  - Aanvullende competentie eisen voor sectoren zoals:
    - Telecom
    - Banken en Financiele dienstverlening
    - Overheid en onderwijs
    - Zorg

Hoe wordt je ISO 27001 auditor (DNV)

Het verkorte traject van vanavond bestaat uit 4 vragen om u te kunnen kwalificeren als "ISO 27001 LEAD AUDITOR".

De audit case

Auditcriteria
- ISO 27001
- Beleid
- Procedures
- Wet- en regelgeving
- Contractuele eisen

Auditbewijsmateriaal
- Interviews
- Observaties
- Registraties
- Rapportages
- Test resultaten

Vereiste situatie

Feitelijke situatie

Audit bevindingen

✓ **conformiteit**

× **afwijking**

Audit conclusie

The Bitter-Brew Case

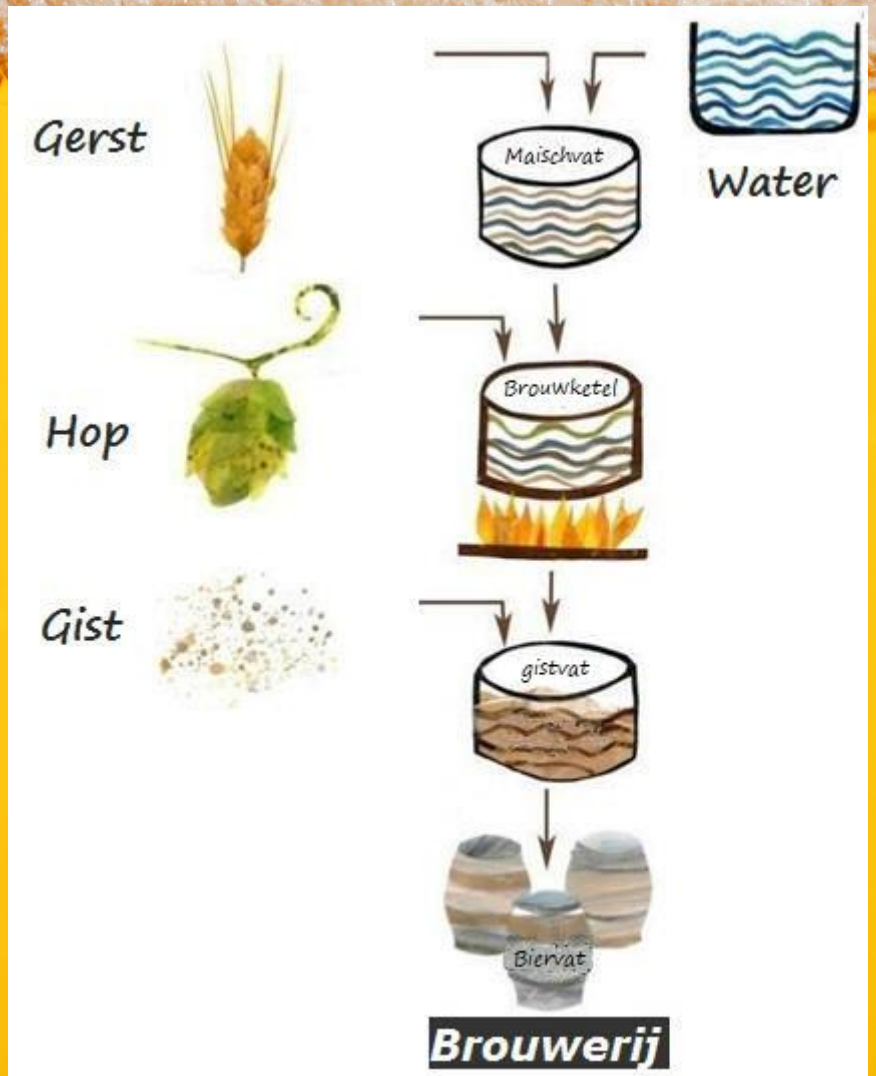
- De **Bitter-Brew** brouwerij mag haar bieren leveren aan het Holland House tijdens de Olympische Spelen in Tokyo (2020), Beijing (2022), Parijs (2024) & Los Angeles (2028).

Voorwaarde

- Bitter-Brew moet met een ISO 27001 certificaat kunnen aantonen, dat ze de beveiliging van alle informatie t.b.v. het leveren van deze bieren in het Holland House op orde hebben.

De audit bij Bitter-Brew

Inkoop



Brouwerij

Interne audit

De Inkoper

- De inkoper heeft alle contracten over de inkopen van ingrediënten op zijn laptop staan.
- Het IT beleid zegt dat alle laptops voorzien moeten zijn van BitLocker disk encryptie software.
- De inkoper gebruikt een eigen laptop en zegt dat disk encryptie software daar niet op staat.
- Hij heeft als alternatief een ZIP file met alle contracten, die hij heeft beveiligd met een wachtwoord.

Audit bevindingen

- **AUDITCRITERIA:**
  - Conform IT beleid moeten alle laptops voorzien zijn van BitLocker disk encryptie.
- **BEVINDING:**
  - De laptop van de inkoper heeft geen BitLocker disk encryptie.
- **AUDITBEWIJS:**
  - Inspectie van de laptop van de inkoper.

De Brouwmeester

- De Brouwmeester van de brouwerij laat zien dat hij informatie over geproduceerde hoeveelheden bier in zijn kluis bewaart.
- Hij zegt dat hij volgens het classificatie-beleid van Bitter-Brew, alle informatie over het brouwproces als “vertrouwelijk” moet labelen en in de kluis moet bewaren.
- Tijdens de inspectie van de brouwerij wordt door de auditor nergens anders “vertrouwelijke” informatie aangetroffen.

Audit bevindingen

- **AUDITCRITERIA:**
  - Informatie over het brouwproces moet “vertrouwelijk” gelabeld zijn en opgeslagen in de kluis.
- **BEVINDING:**
  - De brouwmeester bewaart vertrouwelijk gelabelde informatie over het brouwproces in de kluis.
- **AUDITBEWIJS:**
  - Rondgang door de brouwerij en inspectie van de kluis.

De Interne Auditor

- De Interne Auditor van Bitter-Brew geeft aan dat er afgelopen 12 maanden geen enkele interne audit is gehouden conform de planning.
- Hij weet dat ISO 27001 dat wel als eis stelt, maar hij heeft al zijn tijd nodig gehad voor de voorbereidingen op de Olympische Spelen.
- Hij laat het laatste interne audit rapport van 01/02/2018 zien.

Audit bevindingen

- **AUDITCRITERIA:**
  - De organisatie dient conform audit plan interne audits uit te voeren.
- **BEVINDING:**
  - De organisatie heeft sinds 01/02/2018 geen interne audits uitgevoerd conform audit plan.
- **AUDITBEWIJS:**
  - Interview interne auditor, laatste audit rapport 01/02/2018.

De audit conclusie

Audit bevindingen

- ✓ **conformiteit**
- × **afwijkingen**

Audit conclusie

- **Major NC (cat-1)**
- **Minor NC (cat-2)**


DNV·GL

MANAGEMENT SYSTEEM CERTIFICAAT

Bitter-Brew

ISO/IEC 27001:2013

Cat-1 of cat-2

✓ Plan voor correctie en de correctieve maatregel(en) is beoordeeld en geaccepteerd.

+

Cat-1

✓ De correctie en de correctieve maatregel(en) is beoordeeld

De certificering

1. *Corrective Action Plan*

Laptop encryptie

Correctie:
Oorzaak:
Corrigerende maatregel:

✓

Corrective Action Plan

Uitvoeren Interne audits

Correctie:
Oorzaak:
Corrigerende maatregel:

✓

2. *Corrective Action Plan*

Uitvoeren Interne audits

Correctie:
Oorzaak:
Corrigerende maatregel:

✓

DNV·GL

MANAGEMENT SYSTEEM CERTIFICAAT

Bitter-Brew
Nederland

voldoet aan de eisen gesteld in de Informatiebeveiliging Managementsysteem norm:
ISO/IEC 27001:2013

De certificaat is geldig voor de volgende scope:
Informatiebeveiliging gerelateerd aan het produceren van bier, in overeenstemming met de Verklaring van Toepasselijkheid v3.0, d.d. 01-01-2019.

Hartelijk dank!

Vragen

Opmerkingen

Suggesties