ONDERZOEKSRAPPORT

Saxion, Datacadabra

SCRIPTIE

Verbeteren van informatiebeveiliging gebaseerd op het model van ISO27001

Rita Simon, 475795

Versie	Datum	Beschrijving	Bewerker
0.1	08-10-2023	Aanmaken document	Rita Simon
0.2	10-10-2023	Document met voorwoord en inleiding aanvullen	Rita Simon
0.3	15-10-2023	Begrippenlijst toegevoegd	Rita Simon
0.4	18-10-2023	Theoretisch kader	Rita Simon
0.5	20-10-2023	Theoretisch kader	Rita Simon
0.6	22-10-2023	Deelvraag 1	Rita Simon
0.7	30-10-2023	Deelvraag 2	Rita Simon
0.8	31-10-2023	Feedback aanpassen	Rita Simon
0.9	01-11-2023 t/m 02-11-2023	TK helemaal opnieuw aanpassen	Rita Simon
1.0	09-11-2023	Deelvraag 1 en 2	Rita Simon
1.1	12-11-2023	TK aanvullen	Rita Simon
1.2	21-11-2023	1. Aanvullen de deelvragen 2. De TK verbeteren 3. BPMN toevoegen	Rita Simon
1.3	27-11-2023	Deelvraag 3 toegevoegd	Rita Simon
1.4	01-12-2023 tot 06-12-2023	Deelvraag 4 en 5 toegevoegd	Rita Simon
1.5	08-12-2023 t/m 10-12-2023	Deelvraag 4	Rita Simon
1.6	11 en 12 december 2023	Tabellen en figurenlijst toegevoegd	Rita Simon
1.7	13 december	Verbetering deelvraag 1 tot 3 en toevoeging feedback van Hans	Rita Simon
1.8	14 december	Bijlage met verwijzing toegevoegd en deelvraag 4 verbeterd	Rita Simon
1.9	23 t/m 28 december	Feedback Hans verwerken	Rita Simon
2.0	29 december 2023	Hans feedback resultaten verwerken	Rita Simon

2.1	16 t/m 21 januari	Feedback hans en Ronald verwerken	Rita Simon

Voorwoord

In dit onderzoeksrapport wordt de belangrijke rol van informatiebeveiliging in het bedrijfsleven van Datacadabra onderzocht. In dit onderzoek wordt onderzocht hoe digitale verandering en veel datagebruik de noodzaak voor een sterke informatiebeveiligingsmaatregelen onderstrepen. Door de huidige informatiebeveiligingsstrategieën van Datacadabra B.V. te analyseren en te vergelijken met in dit geval de ISO 27001 en best practices, streeft dit onderzoek ernaar om passende oplossingen en strategieën te bieden voor het versterken van de informatiebeveiliging binnen de organisatie. Hierbij wordt specifiek aandacht besteed aan het verbinden van theoretische inzichten met praktische toepassingen, om zo de gap tussen theorie en praktijk te overbruggen.

Inhoudsopgave

Managementsamenvatting

Het doel is om de huidige risicobeheerstrategieën en -processen bij Datacadabra te evalueren en te verbeteren, met bijzondere aandacht voor het naleven van het ISO 27001-model. Deze inzet voor verbetering werd aangedreven door de noodzaak om inzichten en feedback te verzamelen van zowel interne als externe belanghebbenden, waarbij de nadruk lag op het identificeren van tekortkomingen in de informatiebeveiliging van Datacadabra. Dit omvatte een gedetailleerde analyse van de interne beveiligingsprotocollen en de mate van betrokkenheid van belanghebbenden. De centrale onderzoeksvraag richtte zich op het versterken van de informatiebeveiliging binnen Datacadabra, specifiek door te onderzoeken hoe de implementatie van ISO 27001 kan bijdragen aan deze verbetering.

Voor het verkrijgen van een diepgaand inzicht in de bestaande situatie en potentiële verbeterpunten, werd een gecombineerde onderzoeksmethode toegepast. Deze bestond uit kwantitatieve data-analyse en kwalitatieve technieken zoals interviews en casestudies. Deze aanpak stelde ons in staat een grondige analyse te verrichten van de huidige beveiligingsprotocollen en de betrokkenheid van stakeholders bij Datacadabra.

De onderzoeksresultaten bij Datacadabra onthullen een complex beeld van informatiebeveiliging. De sterke punten omvatten innovatie, technologische capaciteiten, en kennis. Echter, er zijn aanzienlijke zwakheden, zoals het ontbreken van een sterke beveiligingsinfrastructuur en onvoldoende bewustzijn en training in informatiebeveiliging. Belangrijke bedreigingen zijn datalekken, gegevensverlies, en reputatieschade, naast de financiële en juridische uitdagingen van nalevingskosten. Deze bevindingen wijzen op een noodzaak voor Datacadabra om zowel interne kwetsbaarheden aan te pakken als zich te wapenen tegen externe bedreigingen om hun informatiebeveiliging te versterken.

De hoofdconclusie van dit onderzoek is dat Datacadabra significante stappen vooruit kan zetten in de informatiebeveiliging door de implementatie van de ISO 27001-normen. De implementatie hiervan zou niet alleen interne beveiligingsprocessen versterken, maar ook bijdragen aan een cultuur van veiligheidsbewustzijn binnen de organisatie. Daarnaast is duidelijk geworden dat deze veranderingen niet alleen interne voordelen bieden, maar Datacadabra ook positioneren als een organisatie in de sector voor effectief beveiligingsbeheer.

De analyse onthulde dat Datacadabra aanzienlijke verbeteringen kan realiseren door het herzien van de huidige beveiligingsprotocollen en het verhogen van het veiligheidsbewustzijn onder medewerkers en stakeholders. Een belangrijke bevinding was dat de implementatie van ISO 27001 kan leiden tot meer gestandaardiseerde en sterke beveiligingspraktijken.

Het onderzoek benadrukt het belang van standaardisatie in informatiebeveiliging en de actieve betrokkenheid van stakeholders. Een beperking van de studie is de noodzaak van een langdurige evaluatie van de geïmplementeerde veranderingen. Aanbevolen wordt om in toekomstig onderzoek de lange termijn impact van ISO 27001 in diverse organisatorische contexten te onderzoeken. Deze inzichten kunnen essentieel zijn voor zowel Datacadabra als andere organisaties die streven naar een verbeterde informatiebeveiliging

Figuren- en tabellenlijst

Figuur 8	Subproces	Deze ‘BPMN’ weergeeft in een groot geheel welke processen gedetailleerd
Figuur 9	IT-Department	Dit is cruciaal voor het identificeren van kritieke punten waarin informatiebeveiliging moet worden geïntegreerd, met als doel het verminderen van risico's en het verbeteren van de vertrouwelijkheid, integriteit en beschikbaarheid van informatie
Figuur 10	Build process	Biedt een systematische weergave van de fasen van de ontwikkeling en implementatie van de diensten.
Figuur 11	Quality Control	Biedt een systematisch weergave van de kwaliteitscontroles binnen verschillende fasen tijdens de ontwikkeling
Figuur 12	Release fase	is essentieel omdat het de laatste stap is in het systeemtest- en bugfixingproces, waarbij het productteam zorgt voor uitgebreide veiligheids- en functietests, gevolgd door regressietests door de engineeringafdeling
Figuur 13	CRM	Hierin wordt verkoopcyclus van Datacadabra weergegeven.
Figuur 14	Timeline	Hierin staat het implementatieplan in timeline weergegeven.

Begrippenlijst

1. **Informatiebeveiliging:** Het proces van het beschermen van gegevens tegen ongeautoriseerde toegang, openbaarmaking, vernietiging of wijziging om de vertrouwelijkheid, integriteit en beschikbaarheid van informatie te waarborgen. (Surelock - IT Security Services, 2024)
2. **Digitalisering:** De overgang van analoge informatie naar digitale vorm, waarbij gegevens worden omgezet in elektronische formaten. (*Van Dale NEDERLAND*, z.d.)
3. **Integriteit van gegevens:** De kwaliteit van gegevens die aangeeft dat ze volledig, accuraat en ongewijzigd zijn. (*Data integriteit, vertrouw je op je eigen data?*, z.d.)
4. **Datalek:** Het ongeoorloofd vrijkomen van gegevens naar een onbevoegde partij, wat kan leiden tot privacy- en beveiligingsproblemen. (*Wat is een datalek?*, z.d.)
5. **Beveiligingsincident:** Een gebeurtenis waarbij de informatiebeveiliging van een organisatie wordt geschonden, zoals een datalek of een cyberaanval. (*Wat is een beveiligingsincident? - Lumen Group*, 2020)
6. **Best Practices:** Geaccepteerde en bewezen methoden of procedures die worden beschouwd als de meest effectieve manieren om beveiligingsdoelen te bereiken. . (*Van Dale NEDERLAND*, z.d.)
7. **Multifactorauthenticatie (MFA):** Een beveiligingsmethode waarbij gebruikers zich moeten aanmelden met meer dan één vorm van identificatie, zoals een wachtwoord en een sms-code, om toegang te krijgen tot systemen of gegevens. (Copaco Nederland, 2020)
8. **Informatiebeveiligingskader:** Een set van beleidsregels, procedures en technologieën die worden gebruikt om informatiebeveiliging binnen een organisatie te beheren. (*Informatiebeveiliging & IT Security*, 2023)
9. **Gegevensintegriteit:** De nauwkeurigheid en betrouwbaarheid van gegevens gedurende hele levenscyclus, inclusief het voorkomen van ongeoorloofde wijzigingen. (*Van Dale NEDERLAND*, z.d.)
10. **Reputatieschade:** De schade die een organisatie kan oplopen aan haar imago en reputatie als gevolg van beveiligingsincidenten of andere negatieve gebeurtenissen. (*Van Dale NEDERLAND*, z.d.)
11. **Operationele risico's:** Risico's die verband houden met de dagelijkse bedrijfsvoering van een organisatie, waaronder beveiligingsrisico's die de operationele prestaties kunnen beïnvloeden. (*S9 - Operationeel risico standaardmodel*, 2024)
12. **ISO 27001:** Binnen het kader van ISO 27001 wordt de Risk Impact Scale gebruikt tijdens het risicobeoordelingsproces. Na het identificeren van potentiële risico's, worden deze beoordeeld op basis van impact en waarschijnlijkheid. (*Informatiebeveiliging & IT Security*, 2023b)
13. **Risk impact scale:** De Risk Impact Scale is een hulpmiddel dat wordt gebruikt om de potentiële impact van geïdentificeerde risico's op een organisatie te beoordelen. Deze schaal kan variëren van laag, middelmatig, tot hoog, of kan zelfs meer gedetailleerde niveaus bevatten, afhankelijk van de behoeften van de organisatie. (*Risk Assessment Matrix: Overview and guide | AuditBoard*, z.d.)

1. Inleiding

Datacadabra is een vooraanstaand bedrijf gespecialiseerd in data science en kunstmatige intelligentie, gericht op het ondersteunen van geautomatiseerde processen en het verlichten van werkdruk. Ze bieden geavanceerde technologische diensten waarbij ze informatiebeveiliging hooghouden, essentieel voor de bescherming van bedrijfsdata en andere bedrijfsmiddelen. Datacadabra heeft een sterke focus op het aanpakken van risico's gerelateerd aan cyberaanvallen en gegevenslekken, en werkt aan het versterken van de samenwerking tussen IT- en andere afdelingen voor een effectievere implementatie van informatiebeveiligingsstrategieën.

Het doel van dit onderzoek is om maatregelen en best practices te vinden om de gevolgen van". Het tekort aan informatiebeveiliging te verminderen. Dit omvat het verminderen van risico's, zoals datalekken, financiële verliezen en reputatieschade en het versterken van de weerbaarheid tegen informatiebeveiligingsincidenten binnen de organisatie. Door de informatiebeveiliging te verbeteren door de maatregelen en strategieën te implementeren, kan het bedrijf vertrouwen van de klanten opbouwen en groeien als organisatie.

1.1. Aanleiding

Dit onderzoek is tot stand gekomen nadat duidelijk werd dat onvoldoende informatiebeveiliging en het ontbreken van een erkend certificaat leidden tot klantenverlies. Dit is tevens bevestigd in een gesprek met de managing director op 13 november 2023, zie hiervoor bijlage 10.6. Gesprekken met belangrijke stakeholders en incidenten zoals datalekken en phishingaanvallen hebben de urgentie van dit probleem bevestigd, wat Datacadabra motiveerde om risico's te voorkomen en haar informatiebeveiliging te versterken.

Datacadabra's huidige en potentiële afnemers zijn bedrijven die op zoek zijn naar geavanceerde technologische oplossingen. Door onvoldoende informatiebeveiliging en het gebrek aan een erkend certificaat ervaart Datacadabra dat er minder potentiële klanten zijn en klantenverlies, dit wordt in een meeting op 25 augustus 2023 vastgelegd, zie hiervoor bijlage 10.1 interview 0. Klanten van Datacadabra benutten hun diensten en producten voor een scala aan technologische toepassingen. Deze diensten omvatten data science en AI-gebaseerde oplossingen voor procesautomatisering en efficiëntieverbetering. Op de website van Datacadabra, vermeld in de bronnenlijst, staan diverse recent ontwikkelde oplossingen. Voor een gedetailleerd overzicht van deze diensten en hun toepassingen, verwijs ik naar de website van Datacadabra (Datacadabra, z.d.). Betrouwbaarheid en veiligheid van die diensten zijn belangrijke aspecten in de organisatie. Momenteel worden de diensten en producten vooral in Nederland verkocht en uitbesteed, toekomstperspectief is wel om uit te breiden binnen heel EU. Afname van de diensten vindt continue plaats, hierbij zijn bedrijven afhankelijk van de constante beschikbaarheid en veiligheid van Datacadabra's oplossingen. De afnemers kiezen voor Datacadabra vanwege haar innovatieve technologische oplossingen, maar doordat er bij deze ontwikkelingen data erg belangrijk is, is het voor Datacadabra cruciaal om de informatiebeveiliging te verbeteren. Potentiële afnemers kunnen terughoudend zijn om Datacadabra's diensten af te nemen vanwege zorgen over informatiebeveiliging en het ontbreken van een erkend certificaat, zie hiervoor bijlage 10.6 interview met de managing director.

1.2. Probleemstelling

Datacadabra wordt geconfronteerd met een merkbaar gebrek aan bewustzijn en focus op informatiebeveiliging. De potentiële risico's binnen de informatiebeveiliging heeft ernstige gevolgen voor de organisatie en kan leiden tot risico's voor de integriteit van gegevens, financiële instabiliteit en schade aan de bedrijfsreputatie. Voor deze interpretatie is gebruik gemaakt van het document 'Cybersecurity Quick Scan Report', in verband met veiligheid en vertrouwelijke informatie, is het niet mogelijk om het als bijlage toe te voegen aan dit rapport.

1.3. Doelstelling

Het hoofddoel van dit onderzoek is om effectieve maatregelen en best practices te vinden en aan te bevelen voor Datacadabra om haar informatiebeveiliging te verbeteren en op lange termijn te waarborgen in de bedrijfsactiviteiten. Dit omvat het identificeren en aanpakken van specifieke risico's die bijdragen aan het tekort aan informatiebeveiliging, het integreren van informatietechnologie in bedrijfsprocessen, het bevorderen van samenwerking tussen afdelingen, en het zorgen voor blijvende verbeteringen in informatiebeveiliging.

2. Theoretisch kader

In dit hoofdstuk wordt het theoretisch kader toegelicht; een belangrijke basis voor het begrijpen en analyseren van de complexe vraagstukken die spelen bij Datacadabra. Dit kader biedt de lens waardoor er naar de organisatie en haar uitdagingen gekeken wordt, door gevestigde theorieën en concepten te verbinden met de specifieke context van Datacadabra. Het stelt de organisatie in staat om de structuren en dynamieken te begrijpen die lijden aan de problemen die onderzocht wordt en biedt een gestructureerde manier om naar oplossingen te zoeken.

2.1. Freemans theorie

Freeman staat voornamelijk bekend om zijn stakeholdertheorie en stelt dat organisaties rekening moeten houden met de belangen van al haar stakeholders bij het nemen van beslissingen die betrekking hebben op het veranderen van een bepaald bedrijfsproces. (Boom Management, 2023)

Stakeholdertheorie van Freeman

1. Definitie en belang van stakeholders: Freeman definieert stakeholders als elke groep of elk individu dat beïnvloed kan worden door of invloed kan uitoefenen op de doelstellingen van een organisatie. Het vernieuwende van Freemans benadering is dat hij adviseert om niet alleen aandeelhouders te beschouwen, maar ook werknemers, klanten, leveranciers, de lokale gemeenschap en andere betrokken partijen.

2. Wederzijdse afhankelijkheid: volgens Freeman is een bedrijf diepgaand verbonden met zijn stakeholders. Er bestaat een wederzijdse afhankelijkheid: het bedrijf heeft de stakeholders nodig voor resources en support, terwijl de stakeholders afhankelijk zijn van het bedrijf voor werkgelegenheid, producten, diensten of economische groei.

3. Waardecreatie en evenwicht: Freeman benadrukt het belang van waarde creatie voor alle stakeholders. Het idee is dat bedrijven moeten streven naar evenwicht, waarbij de belangen van alle stakeholders worden meegenomen en gerespecteerd. Dit betekent dat besluitvorming is gebaseerd op overweging van de impact op alle relevante partijen en niet enkel op winstmaximalisatie voor aandeelhouders.

4. Management en ethiek: de stakeholdertheorie draagt ook bij aan de ethische fundamenten van bedrijfsvoering. Freeman stelt dat ethisch management en het in overweging nemen van stakeholderbelangen hand in hand gaan. Managers moeten transparant, eerlijk en integer zijn in de interacties met alle stakeholders.
(MindTools, sd)

Toepassing op informatiebeveiliging binnen Datacadabra

Wanneer we deze theorie toepassen op de context van informatiebeveiliging binnen Datacadabra, wordt duidelijk dat:

1. Alle stakeholders zijn betrokken: informatiebeveiliging is niet alleen de verantwoordelijkheid van de IT-afdeling, maar raakt aan alle onderdelen van de organisatie en alle stakeholders. Medewerkers, klanten, leveranciers en zelfs de bredere gemeenschap hebben belang bij het waarborgen van informatiebeveiliging.

2. Wederzijdse verantwoordelijkheid: Datacadabra heeft de verantwoordelijkheid om de persoonlijke en gevoelige gegevens van haar stakeholders te beschermen, terwijl stakeholders verantwoordelijk zijn voor het naleven van beveiligingsprotocollen en -praktijken.

3. Waardecreatie door beveiliging: een robuuste informatiebeveiligingsaanpak creëert waarde voor alle stakeholders door het beschermen van assets, het voorkomen van datalekken en het handhaven van vertrouwen.
4. Ethische benadering: het ethisch omgaan met informatie en het beschermen van de privacy van stakeholders is een cruciaal onderdeel van informatiebeveiliging en is in lijn met de principes van Freemans stakeholdertheorie.

Door de stakeholdertheorie van Freeman toe te passen op informatiebeveiliging, erkent Datacadabra de wederzijdse afhankelijkheid tussen het bedrijf en haar stakeholders, streeft het naar waarde creatie voor alle betrokkenen en benadert het de informatiebeveiliging vanuit een ethisch verantwoord perspectief.

2.2. Root cause analysis

Een root cause analysis (RCA) is een methodologie die wordt gebruikt om de fundamentele oorzaak van problemen of incidenten te identificeren, te begrijpen en te adresseren. Het doel is niet om symptomen te behandelen, maar om de bron van een probleem aan te pakken om toekomstige incidenten te voorkomen. Hieronder volgt een theoretische onderbouwing van deze methode. (MindTools, sd)

Proces:

1. Probleemdefinitie;
2. Data-analyse;
3. Identificatie van mogelijke oorzaken;
4. Oorzaak-gevolganalyse;
5. Identificatie van fundamentele oorzaak;
6. Ontwikkeling van oplossing.

RCA vereist een gestructureerde en systematische aanpak om effectief te zijn. Het is belangrijk om alle mogelijke oorzaken in overweging te nemen en om de analyse op feiten en gegevens te baseren. Dit zorgt voor een objectieve benadering en vermindert de kans op het trekken van verkeerde conclusies. (MindTools, sd)

Een RCA is een krachtige methodologie voor probleemoplossing die zich richt op het identificeren en aanpakken van de onderliggende oorzaken van problemen of incidenten. Door een gestructureerde en systematische aanpak te hanteren, worden organisaties geholpen om effectieve oplossingen te ontwikkelen die toekomstige problemen voorkomen en bijdragen aan continue verbetering. (MindTools, sd)

2.3. Competing values framework

Het competing values framework (CVF) is een instrument dat inzicht biedt in organisatieculturen en de manier waarop deze de dynamiek en prestaties binnen een organisatie beïnvloeden. Binnen het CVF worden vier cultuurtypen onderscheiden: clan, adhocracy, market en hierarchy. Voor Datacadabra, een klein en dynamisch bedrijf met een informele sfeer en sterke nadruk op samenwerking, zijn vooral de clan- en adhocracycultuur relevant (ToolSHero, 2019)

1. **Clancultuur**: deze cultuur is als een uitgebreide familie waarin iedereen samenwerkt aan een gemeenschappelijk doel. Het is gebaseerd op waarden als participatie,

samenwerking en loyaliteit. Voor Datacadabra, waar de teamgrootte beperkt is en de onderlinge relaties sterk zijn, biedt een clancultuur de nodige sociale cohesie en een gevoel van saamhorigheid. Medewerkers kunnen rekenen op ondersteuning van de directe collega's en leiders, wat bijdraagt aan een positieve werkomgeving en het gevoel dat iedereen ertoe doet. Deze cultuur moedigt open communicatie en participatie aan, wat cruciaal is in een klein bedrijf waarin iedereens bijdrage telt. (ToolSHero, 2019)

2. **Adhocracycultuur**: deze cultuur stimuleert innovatie, creativiteit en bereidheid om risico's te nemen. Ze is gericht op flexibiliteit en een externe oriëntatie, met de nadruk op verandering en aanpassingsvermogen. Voor Datacadabra, dat opereert in de snel veranderende wereld van data-analyse en -oplossingen, is het essentieel om flexibel en adaptief te zijn. Een adhocracycultuur moedigt medewerkers aan om proactief te zijn, nieuwe ideeën in te brengen en te experimenteren. Dit draagt bij aan de innovatieve kracht van het bedrijf en stelt het in staat om snel in te spelen op nieuwe kansen en uitdagingen. (ToolSHero, 2019)

Binnen Datacadabra is merkbaar dat er te maken is met twee culturele typen en dat biedt een gebalanceerde mix van stabiliteit en flexibiliteit voor de organisatie. Bij clancultuur heeft men te maken met sterke interne cohesie en een ondersteunende werkomgeving, wat terug te zien is binnen Datacadabra. Daarentegen bevordert de adhocracycultuur de innovatieve en adaptieve houding die nodig is om in de voorhoede van de industrie te blijven. De combinatie zorgt ervoor dat de medewerkers zich gewaardeerd en onderdeel van een team voelen, terwijl zij tegelijkertijd worden aangemoedigd om mee te denken en buiten de gebaande paden te treden. Deze unieke combinatie van culturele elementen maakt Datacadabra een krachtige, cohesieve en innovatieve organisatie die klaar is om de uitdagingen en kansen van de hedendaagse, data gedreven wereld aan te gaan.

2.4. ISO 27001

Uit de interviews en meetings met de werkgever van Datacadabra bleek dat Datacadabra geneigd zijn om ISO 27001 te implementeren.
ISO 27001 is een internationale standaard voor informatiebeveiliging die organisaties voorziet van een raamwerk voor het beheren van de beveiliging van activa (DXfferent BV, 22), zoals financiële informatie, intellectueel eigendom, werknemersgegevens of informatie die is toevertrouwd aan derden. Bij het implementeren van ISO 27001 binnen Datacadabra, of een vergelijkbare organisatie, voor het verbeteren van informatiebeveiliging, zijn de volgende theoretische kaders relevant:

1. **Risicobeheer:** centraal in ISO 27001 staat het identificeren, analyseren en beheren van informatiebeveiligingsrisico's. Dit houdt in dat Datacadabra risico's systematisch moet beoordelen en passende maatregelen moet treffen om ze te beheersen of verminderen.
2. **Beveiligingsbeleid:** dit beleid vormt de basis voor het opstellen van beveiligingsnormen en -procedures. Het helpt Datacadabra bij het definiëren van haar algemene aanpak van informatiebeveiliging en het stellen van doelen.
3. **Organisatorische structuur:** ISO 27001 vereist dat organisaties een duidelijke organisatorische structuur hebben met gedefinieerde rollen en verantwoordelijkheden voor informatiebeveiliging. Dit waarborgt dat alle

werknemers weten wat van hen wordt verwacht in termen van het beschermen van gegevens.

4. **Controlemaatregelen en -procedures:** dit zijn de specifieke technieken en processen die Datacadabra gebruikt om haar beveiligingsrisico's te beheersen. Dit omvat zaken als toegangscontrole, crypto grafische maatregelen en fysieke beveiliging.
5. **Voortdurende verbetering:** ISO 27001 benadrukt het belang van voortdurende evaluatie en verbetering van het informatiebeveiligingsmanagementsysteem (ISMS). Dit betekent dat Datacadabra regelmatig haar processen en beleid moet herzien om ervoor te zorgen dat die effectief blijven.
6. **Betrokkenheid van het management:** voor effectieve implementatie van ISO 27001 is actieve betrokkenheid en ondersteuning van het hoger management vereist. Dit zorgt ervoor dat informatiebeveiliging op hoog niveau wordt erkend en ondersteund binnen de organisatie.
7. **Interne audits en beoordelingen:** regelmatige interne audits en beoordelingen zijn essentieel om de effectiviteit van het ISMS te controleren en om gebieden voor verbetering te identificeren.

(NEN, sd)

Deze voorkeur werd onderbouwd door de erkenning van de internationale status en de grondigheid van deze standaard. Datacadabra waarderen vooral het raamwerk dat ISO 27001 biedt, omdat het verder gaat dan technische maatregelen en ook is gericht op organisatorische en procesmatige aspecten van informatiebeveiliging. Bovendien benadrukten de stakeholders van Datacadabra tijdens deze gesprekken het belang van het naleven van wereldwijde regelgevingsvereisten en het versterken van het vertrouwen van klanten en stakeholders, iets wat wordt gezien als een direct resultaat van het volgen van een consistent en bewezen kader voor informatiebeveiliging, zoals ISO 27001. Deze aspecten, in combinatie met de huidige behoefte aan een meer gestructureerde aanpak van informatiebeveiliging, maakten ISO 27001 de voor de hand liggende keuze voor de organisatie (Dijkman, 2023).

2.5. GDPR

De Europese Algemene verordening gegevensbescherming (GDPR) heeft tot doel de wetgeving inzake gegevensbescherming op de Europese interne markt te stroomlijnen en individuen zeggenschap te geven over hun persoonsgegevens (GDRP, sd). De GDPR heeft gegevensbescherming hoger op de bedrijfsagenda geplaatst, waardoor organisaties zoals Datacadabra, die met persoonsgegevens van EU-burgers omgaan, verplicht zijn deze te beschermen en de privacy van betrokkenen te waarborgen.

Dit is relevant voor Datacadabra, omdat het als IT-bedrijf dat mogelijk met persoonsgegevens werkt, moet voldoen aan de GDPR-vereisten. Dit omvat het implementeren van adequate beveiligingsmaatregelen om persoonsgegevens te beschermen, het waarborgen van de rechten van betrokkenen en het naleven van de regels voor gegevensverwerking en -overdracht. Het niet naleven van GDPR kan leiden tot aanzienlijke boetes en reputatieschade, waardoor het belangrijk is voor Datacadabra om deze verordening serieus te nemen in haar informatiebeveiligingsstrategie. (GDRP, sd)

2.6. Multifactorauthenticatie

Wat is het?

Multifactorauthenticatie (MFA) is een beveiligingsmethode waarmee twee of meer authenticatievormen vereist zijn om toegang te krijgen tot een applicatie of systeem. Dit biedt een extra beveiliging laag boven op de normale gebruikersnaam en wachtwoord. MFA is relevant voor het onderzoek, omdat die een belangrijke oplossing biedt voor beveiligingsrisico's. Een van de voornaamste oplossingen voor deze risico's is namelijk het gebruik van MFA, waarbij de authenticatie van gebruikers beter beveiligd wordt door meerdere verificatielagen te vereisen (Meervoudige verificatie (MFA) | Microsoft Beveiliging, Z.D.).

Hoe werkt het?

MFA combineert twee of meer van de volgende authenticatievormen:

1. Iets wat de gebruiker weet, bijvoorbeeld een wachtwoord of pincode.
2. Iets wat de gebruiker heeft, bijvoorbeeld een smartphone met een authenticatieapp of een hardware token.
3. Iets wat de gebruiker is, bijvoorbeeld biometrische gegevens, zoals vingerafdrukken of gezichtsherkenning.

Toepassing bij Datacadabra

Voor Datacadabra kan MFA worden gebruikt om de toegang tot gevoelige data en systemen te beveiligen. Bijvoorbeeld, werknemers die toegang moeten hebben tot klantgegevens of interne netwerken, kunnen verplicht worden om MFA te gebruiken, waardoor de kans op ongeautoriseerde toegang wordt verkleind. Deze toepassing bij Datacadabra sluit aan bij de theoretische onderbouwing, waarbij MFA wordt gezien als een effectieve strategie om risico's in de digitale beveiliging te verkleinen.

2.7. End-to-end-encryptie

Wat is het?

End-to-end-encryptie (E2EE) is een methode waarbij gegevens versleuteld worden verzonden van de ene partij naar de andere en alleen de verzender en ontvanger de sleutel hebben om de gegevens te ontcijferen. In dit onderzoek staat E2EE centraal als een cruciale oplossing voor privacy- en beveiligingsrisico's. Het biedt een sterke beveiliging, doordat alleen de communicerende partijen toegang hebben tot de ontsleutelde informatie (Lutkevich & Bacon, 2021).

Hoe werkt het?

Bij E2EE worden gegevens aan de kant van de verzender versleuteld en pas ontcijferd aan de kant van de ontvanger. Dit betekent dat zelfs als de data onderschept worden tijdens de overdracht, deze onleesbaar blijven voor iedereen behalve de bedoelde ontvanger. Dit mechanisme zorgt ervoor dat de data tijdens de gehele transmissie beveiligd blijven tegen onderschepping of manipulatie.

Toepassing bij Datacadabra

Datacadabra kan E2EE gebruiken om de communicatie tussen haar servers en klanten te beveiligen. Dit is bijzonder belangrijk voor een bedrijf dat zich bezighoudt met data en AI, omdat de vertrouwelijkheid en integriteit van klantgegevens van belang zijn. Het gebruik van E2EE zorgt ervoor dat klantgegevens beschermd zijn tegen afluisteren en toegang door

onbevoegden. De implementatie van E2EE binnen Datacadabra past binnen het theoretisch kader, dat stelt dat geavanceerde encryptietechnieken van belang zijn voor de bescherming van gevoelige data in een digitale wereld.

2.8. Annex A

Annex A van ISO 27001 is een essentieel onderdeel van de internationaal erkende norm voor informatiebeveiligingsbeheer. Het biedt een uitgebreide set van beveiligingscontroles, die organisaties kunnen gebruiken om de risico's voor hun informatiebeveiliging te beheren en minimaliseren. (DXfferent, 2015)

1. Overzicht van Annex A

Annex A van ISO 27001 bestaat uit 14 domeinen, 35 controlecategorieën en 114 controles. Deze domeinen omvatten diverse aspecten van informatiebeveiliging, zoals informatiebeveiligingsbeleid, organisatie van informatiebeveiliging, beheer van bedrijfsmiddelen, beveiliging van menselijke hulpbronnen, fysieke en omgevingsbeveiliging, communicatiebeveiliging, acquisitie, ontwikkeling en onderhoud van informatiesystemen, leveranciersrelaties en informatiebeveiliging incidentbeheer en -naleving. Elk van deze domeinen bevat specifieke controles en richtlijnen om de beveiliging van informatie te waarborgen. (DXfferent, 2015)

2. Toepassing van Annex A bij Datacadabra

Bij Datacadabra kan Annex A worden ingezet als raamwerk om de huidige informatiebeveiligingsstrategieën te evalueren en verbeteren. Dit raamwerk biedt een gestandaardiseerde benadering voor het identificeren en beoordelen van beveiligingsrisico's en het implementeren van de benodigde beveiligingscontroles. Door de controles van Annex A toe te passen, kan Datacadabra de volgende stappen ondernemen:

- **Beoordelen van risico's**: het uitvoeren van een risicoanalyse op basis van de controles uit Annex A helpt Datacadabra om haar specifieke beveiligingsrisico's te identificeren en prioriteren.
- **Implementatie van controles**: afhankelijk van de resultaten van de risicoanalyse kan Datacadabra passende beveiligingscontroles uit Annex A implementeren. Dit kan variëren van het opstellen van beveiligingsbeleid en het verbeteren van fysieke beveiliging tot het versterken van IT-systemen en het beheren van leveranciersrelaties.
- **Bewaking en review**: de controles bieden ook een basis voor voortdurende monitoring en evaluatie van de effectiviteit van de informatiebeveiligingspraktijken.

3. **Voordelen voor Datacadabra**

Door Annex A te integreren in haar informatiebeveiligingsbeheer, kan Datacadabra profiteren van verbeterde beveiliging, betere naleving van regelgeving en een verhoogd vertrouwen van klanten en partners. Het biedt een systematische benadering die niet alleen helpt bij het beheren van risico's, maar ook bij het proactief identificeren en aanpakken van potentiële toekomstige bedreigingen.

Conclusie

Het gebruik van Annex A van ISO 27001 voor informatiebeveiliging bij Datacadabra biedt een gestructureerde en effectieve aanpak voor het beheer van beveiligingsrisico's. Het stelt Datacadabra in staat om haar beveiligingspraktijken af te stemmen op internationale standaarden, waardoor ze beter is voorbereid op het beschermen tegen en reageren op de dynamische aard van cyberdreigingen in de hedendaagse digitale wereld.

3. Onderzoeksopzet

In dit hoofdstuk wordt de onderzoeksopzet weergegeven die de basis vormt naar het onderzoek in de huidige tekortkomingen in de informatiebeveiliging bij Datacadabra. De onderzoeksvraag en de bijbehorende deelvragen worden toegelicht om een beter inzicht te bieden in de bijdrage van de deelvragen om de hoofdvraag te beantwoorden.

De kern van het onderzoek is de identificatie van de huidige tekortkomingen in de informatiebeveiliging en de ontwikkeling van de strategieën om deze aan te pakken. Hierbij worden, zoals uit de onderstaande deelvragen blijkt, zowel de bedrijfsprocessen als de stakeholders geëvalueerd om de risico's op het gebied van gegevensintegriteit, financiële stabiliteit, operationele efficiëntie en bedrijfsreputatie in kaart te brengen. In dit hoofdstuk vind je de vraagstelling en de deelvragen die erbij horen om de hoofdvraag te beantwoorden. Ook wordt per deelvraag toegelicht hoe het bijdraagt aan het beantwoorden van de hoofdvraag, zie hiervoor 3.2.

Hoofdvraag

Hoe kan Datacadabra haar informatiebeveiliging verbeteren en waarborgen in haar bedrijfsvoering?

Deelvragen

1. Welke specifieke risico's dragen bij aan het gebrek aan informatiebeveiliging binnen Datacadabra?
2. Hoe kunnen de specifieke risico's die bijdragen aan het gebrek van informatiebeveiliging aangepakt worden?
3. Hoe kan Datacadabra informatietechnologie integreren in haar bedrijfsprocessen om de informatiebeveiliging te optimaliseren en te waarborgen?
4. Hoe kan Datacadabra de samenwerking en communicatie tussen afdelingen verbeteren om een geïntegreerde aanpak van informatiebeveiliging te waarborgen?
5. Hoe kan het behoud van verbeterde informatiebeveiliging gewaarborgd worden binnen Datacadabra?

3.1. Probleemanalyse

Aanleiding

Het onderzoek wordt uitgevoerd doordat er urgentie is om de tekortkomingen in de informatiebeveiliging van Datacadabra te identificeren en te verbeteren, zoals blijkt uit gesprekken met belanghebbenden voor meer details zie 'risicoanalyse rapport' H3. Het doel is om risico's zoals datalekken, financiële verliezen en reputatieschade te verminderen. En de zelfbewustheid tegen informatiebeveiligingsincidenten binnen Datacadabra te versterken.

Achtergrond van het vraagstuk

Bij Datacadabra is een tekort aan bewustzijn en focus op informatiebeveiliging vastgesteld, zowel wat betreft de processen als binnen de organisatie (dus de stakeholders). Dit leidt tot risico's voor de integriteit van gegevens, financiële stabiliteit, operationele efficiëntie en bedrijfsreputatie.

Afbakeningen van het vraagstuk

Dit onderzoek binnen Datacadabra zal zich richten op drie specifieke aspecten:

1. Interne veiligheidsprotocollen;

2. Bewustzijnstraining;
3. Coördinatie van informatiebeveiligingsinitiatieven.

Gezien de complexiteit en veelzijdigheid van informatiebeveiliging is het lastig om te bepalen welk percentage van het totale probleem door deze focus wordt aangepakt. De veelzijdigheid van deze facetten kunnen onderverdeeld worden in technologisch, menselijk, wettelijk en organisatorisch. Al deze invloeden zijn nauw met elkaar verworven en evolueren continu. Er wordt geconcentreerd op de belangrijke interne elementen van Datacadabra's informatiebeveiliging, maar vertegenwoordigt slechts een deel van de bredere beveiligingsstrategie van de organisatie.

Deze focus op deze aspecten is belangrijk om verschillende redenen:

1. **Interne Veiligheidsprotocollen**: Het evalueren van de interne veiligheidsprotocollen helpt bij het identificeren van bestaande zwakheden in de beveiligingsinfrastructuur van Datacadabra.
2. **Bewustzijnstraining**: Door het bewustzijn en de training van personeel te beoordelen, wordt het menselijke aspect van informatiebeveiliging aangepakt.
3. **Coördinatie van Informatiebeveiligingsinitiatieven**: Het onderzoeken van de coördinatie van beveiligingsinitiatieven biedt inzicht in hoe goed de organisatie beveiligingsrisico's beheert en reageert op nieuwe dreigingen.

Relevantie van het vraagstuk

De relevantie van dit onderzoek ligt in de cruciale rol van informatiebeveiliging in de data-gedreven wereld, zoals benadrukt door Smith en Jones (2020) in het Journal of Information Security. Tekortkomingen in deze beveiliging, resulterend in gegevenslekken, operationele verstoringen en reputatieschade vormen de risico's. Dit onderzoek is van groot belang voor het verbeteren van Datacadabra's beveiligingsstrategie en biedt tevens inzichten die waardevol zijn voor andere organisaties die met vergelijkbare beveiligingsuitdagingen kampen. (Journal of Information Security and Applications, sd)

3.2. Keuze voor de deelvragen en relevantie ervan

Hieronder worden de deelvragen toegelicht en wordt besproken hoe ze bijdragen aan het beantwoorden van de hoofdvraag.

Deelvraag 1: Welke specifieke risico's dragen bij aan het gebrek aan informatiebeveiliging binnen Datacadabra?

- Door de risico's te identificeren, helpt dit bij het identificeren van de kernrisico's die de huidige informatiebeveiligingsuitdagingen van Datacadabra vormen. Het beantwoorden ervan is de eerste stap in het proces van risicobeheer, omdat het een duidelijk overzicht geeft van wat aangepakt moet worden. Dit legt de basis voor het ontwikkelen van gerichte strategieën om deze risico's te beheren.

Deelvraag 2: Hoe kunnen de specifieke risico's die bijdragen aan het gebrek van informatiebeveiliging aangepakt worden?

- Hierbij wordt het gericht op zowel de detectie als de mitigatie van informatiebeveiligingsrisico's. Het beantwoorden ervan draagt bij aan de hoofdvraag door het bieden van methoden en processen voor zowel het identificeren van de risico's als het implementeren van effectieve maatregelen om ze te beheren. Dit

omvat het evalueren van bestaande beveiligingsprotocollen en het voorstellen van verbeteringen.

Deelvraag 3: Hoe kan Datacadabra informatietechnologie integreren in haar bedrijfsprocessen om de informatiebeveiliging te optimaliseren en te waarborgen?

- Informatietechnologie (IT) wordt beschouwd als een hulpmiddel omdat het specifieke tools, systemen en technologieën omvat waarmee organisaties gegevens kunnen verzamelen, opslaan, verwerken en beheren. IT biedt de mogelijkheid om informatie efficiënter en effectiever te beheren en te beschermen. De deelvraag benadert informatiebeveiliging vanuit een operationeel perspectief en onderzoekt hoe IT kan worden geïntegreerd in bedrijfsprocessen om de informatiebeveiliging te verbeteren. De keuze om zich in deelvraag 3 specifiek op informatietechnologie (IT) te richten, is ingegeven door het belang van IT als kritische component in de operationele structuur van Datacadabra voor informatiebeveiliging. Dit is essentieel voor het ontwikkelen van een holistische en technologisch geavanceerde benadering van informatiebeveiliging.

Deelvraag 4: Hoe kan Datacadabra de samenwerking en communicatie tussen afdelingen verbeteren om een geïntegreerde aanpak van informatiebeveiliging te waarborgen?

- Effectieve informatiebeveiliging binnen een organisatie als Datacadabra hangt niet alleen af van technologische oplossingen, maar vereist ook sterke samenwerking en communicatie binnen de organisatie. Het onderzoeken van deze aspecten is essentieel voor het ontwikkelen van een samenhangende en effectieve informatiebeveiligingsstrategie. Deze aanpak draagt bij aan het creëren van een organisatiebreed bewustzijn en verantwoordelijkheid voor informatiebeveiliging, wat cruciaal is voor het waarborgen van de algehele veiligheid van de organisatie.

Deelvraag 5: Hoe kan het behoud van verbeterde informatiebeveiliging gewaarborgd worden binnen Datacadabra?

- Deze deelvraag is gericht op de langetermijnstrategieën en -processen die nodig zijn om een effectieve informatiebeveiliging te handhaven.

4. Methodiek

Dit hoofdstuk behandelt aanpak van elke deelvraag van het onderzoek. Voor het onderzoek is gebruikgemaakt van diverse methoden, zoals interviews, documentanalyses en SWOT-analyses om de uitdagingen van informatiebeveiliging te begrijpen en effectieve oplossingen te ontwikkelen. Het doel is om Datacadabra te helpen bij het versterken van haar informatiebeveiliging en het bedrijf voor te bereiden op toekomstige cyberdreigingen, door een combinatie van praktische inzichten (van de stakeholders) en theoretisch onderzoek.

4.1. Welke specifieke risico's dragen bij aan het gebrek aan informatiebeveiliging binnen Datacadabra?

Doel:

Het doel van deze deelvraag is om de specifieke risico's die bijdragen aan de tekortkomingen in de informatiebeveiliging bij Datacadabra identificeren en te begrijpen. Deze deelvraag is noodzakelijk om de hoofdvraag te beantwoorden, omdat het een inzicht biedt in de onderliggende oorzaken van de beveiligingsproblemen binnen de organisatie, dit is belangrijk voor het ontwikkelen van oplossingen en strategieën.

Aanpak

Voor de deelvraag over risico's en tekortkomingen in de informatiebeveiliging bij Datacadabra, begint de aanpak met het verkrijgen van inzichten door gesprekken (interviews) met ervaren stakeholders zoals de CTO, MD, en OM, die volledig kennis van de organisatie en de tekortkomingen hebben. Dit wordt aangevuld met deskresearch, bestaande uit analyse van bestaande bedrijfsdocumenten (documentanalyse). Fieldresearch omvat verdere gesprekken met stakeholders, voor opheldering van de functies van de stakeholder, zie hoofdstuk 3 in het 'Risicoanalyse rapport' detaildocument. De data-analyse is kwalitatief en voor de validiteit en betrouwbaarheid van de data wordt triangulatie toegepast, waarbij de resultaten worden gevalideerd door verificatie door organisatie-experts.

Producten

Hieronder staat puntsgewijs hoe de eerste deelvraag is aangepakt:

1. **SWOT-analyse**: analyseren van sterke en zwakke punten, kansen en bedreigingen met betrekking tot informatiebeveiliging (Gertjanschop, 2023), om zowel interne zwakheden als externe risico's, zoals cyberaanvallen en beveiligingsinbreuken, te identificeren, wat cruciaal is om de specifieke risico's die bijdragen aan het gebrek aan informatiebeveiliging binnen Datacadabra te begrijpen.
2. **Stakeholderanalyse**: identificeren van sleutelfiguren binnen Datacadabra, zoals het management, de IT-afdeling en HR, en hun rol en invloed binnen de informatiebeveiligingsstructuur bepalen. In het risicoanalyserapport in hoofdstuk 3 (die wordt als detaildocument bijgevoegd) is een stakeholderanalyse uitgevoerd en is aangegeven met welke stakeholders een interview is gehouden. Dit biedt inzicht in de betrokkenheid van verschillende partijen bij informatiebeveiligingskwesties.
3. **Risicoanalyserapport**: opstellen van een rapport over de huidige risico's die Datacadabra ervaart, inclusief details over specifieke risico's, zoals datalekken en nalevingskosten. Dit draagt bij aan een beter begrip van de urgentie en omvang van deze risico's.
4. **Bijlage met risico's, oorzaken, gevolgen en data**: door de interviews die plaats vinden met de stakeholders hierboven genoemd, wordt er een lijst opgesteld met de risico's

die bijdragen aan tekort aan informatiebeveiliging binnen Datacadabra. Lijst met de risico's draagt bij aan het gedetailleerd documenteren en begrijpen van de specifieke risico's die bijdragen aan het gebrek aan informatiebeveiliging binnen Datacadabra.

4.2. Hoe kunnen de specifieke risico's die bijdragen aan het gebrek van informatiebeveiliging aangepakt worden?

Doel

Het doel is om effectieve strategieën en maatregelen te identificeren die nodig zijn om de geïdentificeerde informatiebeveiligingsrisico's bij Datacadabra aan te pakken, met als uiteindelijk doel het verbeteren en waarborgen van de algehele informatiebeveiliging van het bedrijf.

Aanpak

Voor deze deelvraag ligt de focus op kwalitatieve analyse, met een specifieke nadruk op het begrijpen van de oorzaken achter informatiebeveiligingsrisico's bij Datacadabra door middel van Root Cause Analysis (RCA) zie theoretisch kader 2.2. De dataverzameling voor deze analyse vindt plaats via een combinatie van desk- en fieldresearch, waarbij voornamelijk data uit de eerste deelvraag wordt gebruikt. Deze data helpen bij het in kaart brengen van de risico's en onderzoekt vervolgens de beste manieren van aanpak. Hierbij wordt ook gebruik gemaakt van literatuuronderzoek naar best practices en methodes voor het gestandaardiseerd beheren van risico's en het vinden van effectieve strategieën. De resultaten van deze analyses worden verder versterkt en geverifieerd door gesprekken met experts binnen de organisatie, waarbij RCA wordt toegepast om dieper in te gaan op de fundamentele oorzaken van de geïdentificeerde risico's.

Producten

1. **Toepassen van 'Risk Impact Scale**: Dit instrument wordt ingezet om informatiebeveiligingsrisico's bij Datacadabra te kwantificeren en prioriteren. Het draagt bij aan een systematische beoordeling van risico's, met een focus op het identificeren van de onderliggende oorzaken, in lijn met RCA-principes en ISO 27001.
2. **Implementatie van een Beheer strategie voor Risico's**: Deze strategie richt zich op het ontwikkelen van maatregelen om geïdentificeerde risico's te managen, verminderen of elimineren. Deze aanpak, die in overeenstemming is met RCA-principes, zorgt voor een systematische en effectieve behandeling van elke bedreiging, wat leidt tot een verbeterde beveiligingsinfrastructuur bij Datacadabra.

Samengevat, de combinatie van deze twee producten - de 'Risk Impact Scale' en de beheerstrategie voor risico's - stelt Datacadabra in staat om begrip te ontwikkelen van hun informatiebeveiligingsrisico's en biedt een gestructureerd kader voor het effectief aanpakken en beheren van deze risico's.
Zie hoofdstuk 2.4 voor gedetailleerde uitleg over ISO 27001. In de resultaten van deelvraag 2 wordt de risk impact scale toegelicht.

4.3. Hoe kan Datacadabra informatietechnologie integreren in haar bedrijfsprocessen om de informatiebeveiliging te optimaliseren en te waarborgen?

Doel
Het doel is om systematische methoden en praktijken te identificeren die Datacadabra in staat stellen informatietechnologie effectief te integreren in haar bedrijfsprocessen. Dit met het uiteindelijke doel om de algehele informatiebeveiliging te verbeteren en toekomstige risico's te minimaliseren.

Aanpak
Voor de deelvraag over de integratie van informatietechnologie in de bedrijfsprocessen van Datacadabra wordt een uitgebreide aanpak gehanteerd. Dit omvat het verzamelen en kwalitatief analyseren van relevante documenten over informatiebeveiligingspraktijken en IT-integratie. De aanpak omvat ook een GAP-analyse, geïnspireerd door Vleeshouwers (2023), om verbeteringsgebieden te identificeren en de huidige situatie te begrijpen. Daarnaast wordt documentanalyse uitgevoerd om inzicht te krijgen in bedrijfsprocessen en IT-infrastructuur.
Deze analyses leiden tot visuele diagrammen die de huidige en gewenste situatie weergeven, en dit wordt gevalideerd door MD en CTO van Datacadabra om de betrouwbaarheid te waarborgen. Deze gecombineerde aanpak biedt diepgaand inzicht in hoe IT-integratie kan worden verbeterd voor informatiebeveiliging.

Producten
De onderzoeksmethoden hebben geleid tot twee kernproducten:

1. **Procesmodellen in de vorm van BPMN (Business Process Model Notation):** Deze modellen geven inzicht in de interne werking van Datacadabra door de bedrijfsprocessen van verschillende afdelingen te visualiseren. Hierdoor wordt duidelijk hoe deze afdelingen met elkaar zijn verbonden en hoe informatietechnologie geïntegreerd kan worden om informatiebeveiliging te optimaliseren.
2. **GAP-analyse:** De GAP-analyse documenteert zowel de huidige situatie als de gewenste situatie met betrekking tot informatiebeveiliging en IT-integratie binnen Datacadabra. Hierdoor ontstaat een gedetailleerd overzicht van de verschillen tussen de twee, waardoor het mogelijk wordt om gerichte maatregelen te nemen om deze kloof te overbruggen en de informatiebeveiliging te verbeteren.

Deze methoden en producten bieden een systematische aanpak om de informatiebeveiliging van Datacadabra te verbeteren.

4.4. Hoe kan Datacadabra de samenwerking en communicatie tussen afdelingen verbeteren om een geïntegreerde aanpak van informatiebeveiliging te waarborgen?

Doel
In deze context helpt het om te begrijpen hoe interne samenwerking en communicatie kunnen bijdragen aan een meer geïntegreerde en effectieve beveiligingsaanpak. Dit is essentieel, omdat informatiebeveiliging niet alleen een technisch vraagstuk is, maar ook afhangt van hoe goed verschillende afdelingen samenwerken en informatie delen.
Aanpak
Voor deze deelvraag worden relevante stakeholders, waaronder de Managing Director en de Operationeel Manager, geïdentificeerd. Gesprekken met hen worden gepland om inzichten

te verzamelen over informatiebeveiliging, interne communicatie en samenwerking binnen Datacadabra (fieldresearch). Daarnaast wordt deskresearch uitgevoerd door wetenschappelijke artikelen over informatiebeveiliging en casestudies (zie bronnenlijst) te analyseren op het gebied van bedrijfscommunicatie en informatiebeveiliging. De resultaten van de gesprekken en deskresearch worden geanalyseerd om patronen, uitdagingen en kansen te identificeren en de huidige situatie binnen Datacadabra te begrijpen.

Producten

1. **Communicatieplan:** Dit product is essentieel omdat het een gedetailleerd plan biedt om de interne communicatie en samenwerking binnen Datacadabra te versterken. Het plan is ontworpen met inachtneming van de principes van ISO 27001, wat betekent dat het niet alleen voldoet aan internationale normen, maar ook bijdraagt aan een verbeterde informatiebeveiliging. Door dit plan te ontwikkelen, wordt een praktische strategie geboden om de communicatie tussen afdelingen te verbeteren, wat cruciaal is voor een geïntegreerde aanpak van informatiebeveiliging.
2. **Communicatieanalyse:** De analyse van de interviews met stakeholders biedt diepgaande inzichten in de huidige communicatiedynamiek en -uitdagingen binnen Datacadabra. Deze analyse onthult patronen, uitdagingen en kansen op het gebied van interne communicatie en samenwerking. De resultaten van deze analyse vormen een realistisch beeld van de huidige situatie binnen de organisatie en helpen bij het identificeren van specifieke gebieden die verbeterd kunnen worden. Hierdoor kunnen gerichte aanbevelingen en strategieën worden geformuleerd om de samenwerking tussen afdelingen te versterken en de informatiebeveiliging te waarborgen.

Kortom, het communicatieplan biedt een concrete strategie, terwijl de interviewanalyse diepgaande inzichten levert. Samen helpen deze producten bij het ontwikkelen van aanbevelingen en strategieën om de communicatie en samenwerking tussen afdelingen te verbeteren en zo een geïntegreerde aanpak van informatiebeveiliging te waarborgen binnen Datacadabra.

Zie hoofdstuk 2.1 voor gedetailleerd toelichting over de cultuur binnen de organisatie.

4.5. Hoe kan het behoud van verbeterde informatiebeveiliging gewaarborgd worden binnen Datacadabra?

Doel

Het doel van de deelvraag is om een gestructureerde benadering te ontwikkelen voor het handhaven van verbeterde informatiebeveiligingsstrategieën op de lange termijn binnen Datacadabra. Deze benadering omvat continue verbetering van informatiebeveiligingsprocessen en -systemen, gebaseerd op actuele trends en best practices. Het uiteindelijke doel is om duurzame en toekomstbestendige informatiebeveiligingsstrategieën te implementeren en te behouden binnen de organisatie, zodat Datacadabra effectief kan reageren op huidige en toekomstige beveiligingsuitdagingen.

Aanpak

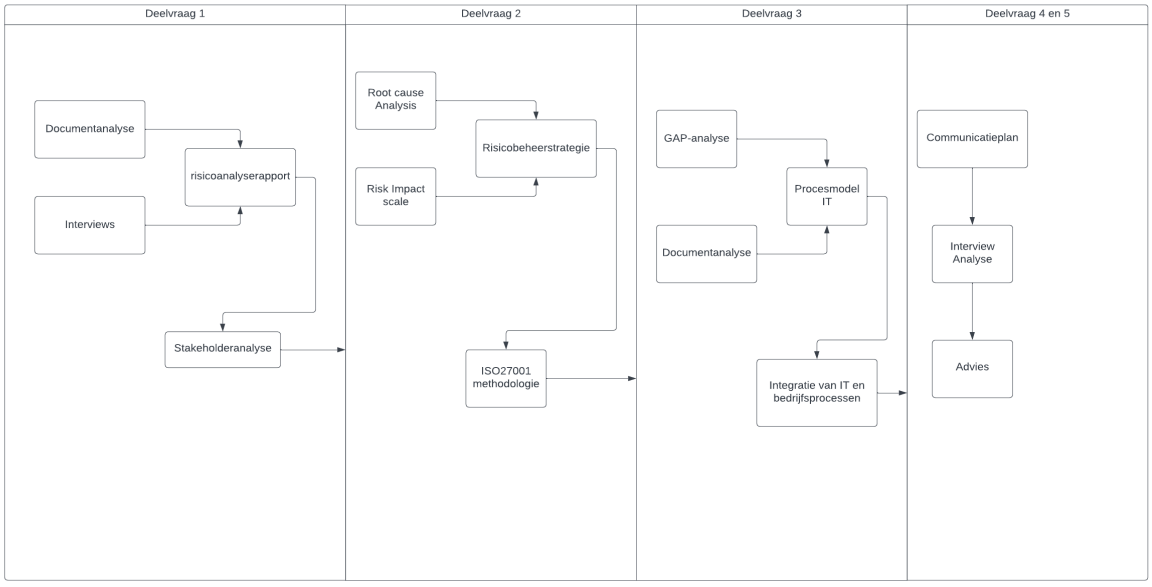
De aanpak voor het behouden van een effectieve implementatie en het behoud van verbeterde informatiebeveiligingsstrategieën op de lange termijn bij Datacadabra integreert methodologieën en producten voor een gestructureerde benadering. Hieronder staat de samenvatting van deze aanpak:

1. **Continuous improvement**: deze methodiek (*Continuous improvement: 6 stages to follow and why it's important*, z.d.) ligt aan de basis van het onderzoek. Ze stelt ons in staat om continue verbeteringen in de informatiebeveiligingsprocessen en -systemen van Datacadabra te identificeren en door te voeren, wat zorgt voor up-to-date en aangepaste beveiligingsprotocollen.
2. **Deskresearch (interview in een meeting vorm)**: hierbij wordt gebruikgemaakt van bronnen, zoals vakliteratuur, online artikelen en interne documenten van Datacadabra. Dit biedt diepgaand inzicht in actuele trends, uitdagingen en best practices op het gebied van informatiebeveiliging.

Producten

1. **Advies met een roadmap van het implementatieplan**: dit rapport bevat een uitgewerkt conceptimplementatieplan en een tijdlijn die bij de implementatie hoort. In het adviesrapport staan ook oplossingen en aanbevelingen die praktisch zijn voor verbetering van de informatiebeveiliging binnen Datacadabra.

De combinatie van continuous improvement en deskresearch biedt een diepgaande benadering van informatiebeveiliging bij Datacadabra. Het adviesrapport dient als routekaart voor continue verbetering. Samen zorgen deze producten ervoor dat Datacadabra in staat is om niet alleen te reageren op huidige beveiligingsuitdagingen, maar ook proactief op toekomstige bedreigingen te anticiperen.



Figuur 1: Onderzoek model

5. Resultaten

Hieronder staan de resultaten van de deelvragen. Voor de resultaten is gebruikgemaakt van detaildocumenten, interviews en literatuuronderzoek.

Strengths	Weaknesses
1. Innovatie en technologie 2. Kennis en expertise	1. Ontbreken van beveiligingsinfrastructuur 2. Bewustzijn en Training Afhankelijkheid van Cruciale Gegevens
Opportunities	**Threats**
1. Regelgeving als Richtlijn 2. Marktvraag	1. Datalekken en Gegevensverlies 2. Reputatieschade 3. Nalevingskosten 4. Aansprakelijkheid 5. Verlies van klantvertrouwen 6. Intellectueel eigendom

Figuur 6: SWOT-analyse

5.1. Analyse van informatiebeveiligingsrisico's

In het proces van het onderzoeken van specifieke risico's die bijdragen aan het gebrek aan informatiebeveiliging binnen Datacadabra, zijn naast interviews en documentanalyses, zoals beschreven in hoofdstuk 4.1, ook andere methoden toegepast. Een van deze methoden is de ontwikkeling van een SWOT-analyse, gebaseerd op de uitkomsten van de interviews, zoals geïllustreerd in figuur 6. Het doel van deze methoden is om een begrip te verkrijgen van zowel de interne als externe factoren die de informatiebeveiliging van Datacadabra beïnvloeden. Deze aanpak heeft geleid tot de identificatie van diverse risico's die de informatiebeveiliging van Datacadabra bedreigen. Deze risico's omvatten zowel interne zwakheden als externe bedreigingen. Interne zwakheden benadrukken het ontbreken van een adequate beveiligingsinfrastructuur, onvoldoende bewustzijn en training van medewerkers, evenals een hoge afhankelijkheid van gegevens. Externe bedreigingen omvatten onder andere cyberaanvallen, beveiligingsinbreuken, datalekken, het verlies van kritieke gegevens en de noodzaak om te voldoen aan regelgeving.
Voor een diepgaander inzicht in de geïdentificeerde risico's en de details van de interviews met stakeholders, verwijs ik naar bijlage 10.1 I(interviews 1 tot 3) en bijlage 10.16 voor meer gedetailleerde informatie over deze specifieke risico's.

Risico	Bijdrage aan Tekort aan Informatiebeveiliging
Datalekken	Leidt tot onbedoelde blootstelling van gevoelige gegevens, privacy inbreuken en juridische problemen.
Gegevensverlies	Resulteert in het verlies van kritieke bedrijfsinformatie en operationele verstoringen.

Risico	Bijdrage aan Tekort aan Informatiebeveiliging
Verlies van Vertrouwen	Schade aan klant- en leveranciersrelaties, wat resulteert in omzetdaling en reputatieschade.
Nalevingskosten	Financiële en juridische consequenties door niet-naleving van regelgeving.
Reputatieschade	Negatieve publieke perceptie die klantverloop en merkschade veroorzaakt.
Operationele Storingen	Verstoring van de normale bedrijfsvoering door technische storingen.
Verlies van Intellectueel Eigendom	Verlies van belangrijke bedrijfsinformatie en innovaties, wat concurrentievoordeel kan verminderen.

Tabel 1: risico's

5.1.1. Methodologie van de risicoanalyse

De aanpak van de risicoanalyse omvat diverse methoden voor een inzicht in de informatiebeveiligingsrisico's bij Datacadabra. Deze zijn: literatuurstudie om een theoretisch kader te vormen, interne beoordelingen voor specifieke risico-identificatie, interviews met stakeholders voor diepgaande inzichten en een vergelijkende analyse met best practices in de industrie. Deze geïntegreerde benadering zorgde voor een veelzijdig en diepgaand begrip van de risico's en hun potentiële impact op de organisatie.

5.1.2. Aanbevolen acties

In mijn advies aan Datacadabra, gebaseerd op de 'Risicoanalyse Rapport', worden er twee essentiële acties onderdrukt om de informatiebeveiliging te verbeteren, in lijn met ISO 27001 en best practices in de beveiligingsindustrie:

1. **Verbeteren van de Beveiligingsinfrastructuur**: Dit is van belang om de organisatie te beschermen tegen externe bedreigingen zoals cyberaanvallen en beveiligingsinbreuken.
2. **Vergroten van het Bewustzijn van de Medewerkers over Informatiebeveiliging**: Het verhogen van het bewustzijn en de competentie van medewerkers in het omgaan met beveiligingsrisico's is essentieel om interne kwetsbaarheden te verminderen.

De keuze voor de bovenstaande acties, met als doel het verbeteren van de beveiligingsinfrastructuur en vergroting van bewustzijn van medewerkers, is gedaan op basis van:

1. **Prioritering van Kritieke Risico's**: Risicoanalyses, waaronder beveiligingsaudits en zwakteanalyses, toonden aan dat zowel externe bedreigingen, zoals cyberaanvallen, als interne zwakheden, zoals een gebrek aan bewustzijn, significant bijdroegen aan de informatiebeveiligingsrisico's. Deze bevindingen, in lijn met ISO 27001-normen, onderstrepen de urgentie van deze acties.
2. **Effectiviteit en Impact**: Deze twee acties werden geïdentificeerd als de effectieve maatregelen om zowel de externe als interne risico's aan te pakken. De geselecteerde maatregelen zijn gekozen vanwege de effectiviteit in het aanpakken van zowel externe als interne risico's. Deze acties bieden een evenwichtige benadering om technologische kwetsbaarheden te verminderen en tegelijkertijd het bewustzijn en de competentie van medewerkers te verbeteren

3. **Stakeholder Input en Best Practices**: De keuzes zijn mede gebaseerd op inzichten verkregen uit interviews met stakeholders en de analyse van best practices in de industrie. Deze input benadrukte het belang van deze twee specifieke acties.

5.2. Risicobeheerproces

In dit hoofdstuk wordt er focus gelegd op het beantwoorden van de deelvraag: "Hoe kunnen de specifieke risico's die bijdragen aan het gebrek van informatiebeveiliging aangepakt worden?" Hierin worden de methoden en strategieën onderzocht die Datacadara kan inzetten om de informatiebeveiliging uitdagingen aan te pakken. De volgende punten geven een overzicht van de kernaspecten die in dit hoofdstuk worden behandeld:

1. Identificatie en evaluatie van informatiebeveiligingsrisico's.
2. Toepassing van RCA en ISO 27001-normen voor risicoanalyse.
3. Gebruik van 'risk impact scale' voor risicoprioritering.
4. Beheerstrategieën voor datalekken en gegevensverlies.
5. Maatregelen voor vertrouwens- en nalevingskostenbeheer.
6. Uitgebreide risicobeheerbenaderingen.

Door de tekortkomingen binnen Datacadabra is er een uitgebreid onderzoek verricht naar het beheer van informatiebeveiligingsrisico's. Hierbij is er een methodologie toegepast die gebaseerd is op best practices, waaronder RCA (Root Cause Analysis) en ISO 27001-normen. Deze benadering bevat het gebruik van de 'risk impact scale' en de Annex A-methode van ISO 27001 voor systematische identificatie, evaluatie en rangschikking van risico's. Deze strategie, die wordt ondersteund door de CTO van Datacadabra (zie bijlage 10.1 interview 4 tot 7), wordt aanbevolen als de basis voor een uitgebreid risicobeheerproces om de algehele informatiebeveiliging te verbeteren. Voor meer gedetailleerde informatie zie bijlage 10.9 voor de beheerstrategie, bijlage 10.9.1, 10.9.2 voor uitwerking en bijlage 10.11 voor de aanpak van risico's.

5.2.1. Toekomstige identificatiemethoden

De risicoanalyse van Datacadabra richt zich op het identificeren en aanpakken van specifieke kwetsbaarheden in de beveiligingspraktijken. Deze focus is gebaseerd op een combinatie van gedetailleerde analyses, interviews met de CTO (bijlagen 10.1, 10.10 t/m 10.12) en literatuurstudie. De identificatie van risico's bestaat uit:

1. **Datalekrisico's**: Door IT-beveiligingsrapporten en incidentlogboeken te analyseren en gesprekken te voeren met IT-medewerkers, kunnen patronen van risico's op datalekken herkend worden. Dit proces helpt bij het ontwikkelen van preventieve maatregelen en biedt inzichten in specifieke dreigingen zoals phishing en e-mailbeveiliging.
2. **Gegevensverliesrisico's**: Het analyseren van gegevensbeheerprocessen en back-upprotocollen is van belang. Interactie met personeel dat betrokken is bij gegevensbeheer en IT-onderhoud helpt bij het identificeren van specifieke risico's, wat leidt tot effectievere risicobeperkingsstrategieën.
3. **Risico's op verlies van vertrouwen**: Het analyseren van klantfeedback en leveranciersbeoordelingen biedt inzicht in hun percepties en verwachtingen. Dit helpt bij het optimaliseren van communicatieprocedures om relaties met klanten en leveranciers te versterken.

4. **Nalevingskostenrisico's**: Een grondige regelgevingsreview en overleg met het juridische team zijn noodzakelijk om nalevingskostenrisico's te identificeren, vooral in relatie tot ISO 27001-normen. Deze aanpak biedt inzicht in compliance-uitdagingen en gerelateerde kosten.

Dit plan, ontwikkeld in samenwerking met de CTO, zie interview 7 en de meeting tussen de CTO en de MD en gebaseerd op grondig onderzoek, stelt Datacadabra in staat om proactief potentiële risico's aan te pakken en de bedrijfsveiligheid en -stabiliteit te waarborgen.

5.2.2. Risk impact scale

De risicobeheermethodiek van Datacadabra, zoals beschreven in het interview met de Managing Director (interview 4), is ontwikkeld in reactie op het belang om de informatiebeveiligingspraktijken te verbeteren en in lijn te brengen met ISO 27001-normen. De aanleiding voor deze gestructureerde aanpak was de identificatie van significante beveiligingsrisico's binnen de organisatie. Door risico's te beoordelen op waarschijnlijkheid en impact met numerieke scores, kan Datacadabra prioriteit geven aan de hoge risico's. Specifieke actieplannen, waaronder beveiligingsmaatregelen en naleving van regelgeving, zijn ontworpen om deze risico's effectief te beheren en de algehele organisatorische veiligheid te verbeteren. Deze methodiek benadrukt een verantwoordelijke en systematische benadering van risicobeheer binnen de organisatie.

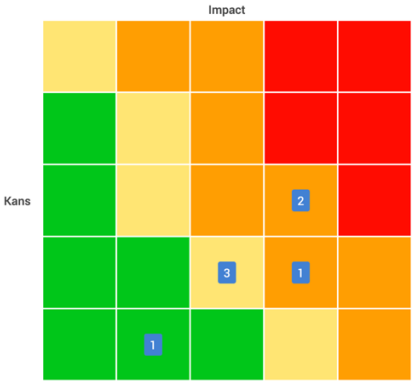
Titel	Eigenaar	Kans	Impact	Risiconiveau	Status	Aanpak
Ongeautoriseerde toegang tot bedrijfs- en persoonsgegevens	Mark Bulthuis	Mogelijk	Groot	Hoog	Nieuw	Beheersen
Niet voldoen aan data- en privacyregelgeving, gebrekkige nalevingsprocedures	Mark Bulthuis	Mogelijk	Groot	Hoog	Nieuw	Beheersen
Risico's verbonden aan het niet voldoen aan data- en privacywetgeving, vooral van belang gezien de aard van de werkzaamheden van Datacadabra	Mark Bulthuis	Zelden	Groot	Hoog	Nieuw	Beheersen
Risico's gerelateerd aan softwarefouten, hardwarestoringen of andere technische problemen die de dienstverlening kunnen verstoren		Zelden	Significant	Normaal	Nieuw	Beheersen
Negatieve media-aandacht, publieke misstappen, schandalen	Mark Bulthuis	Zelden	Significant	Normaal	Nieuw	Beheersen
Juridische claims door foutieve data-analyse, softwarefouten die schade veroorzaken	Mark Bulthuis	Zelden	Significant	Normaal	Nieuw	Beheersen
Stroomuitval, technische storingen, storingen in software of hardware	Mark Bulthuis	Onwaarschijnlijk	Klein	Laag	Nieuw	Accepteren

Tabel2: Tabel berekende risico's

5.2.3. Matrix

Datacadabra's risicobeoordeling, in lijn met ISO 27001, gebruikt waarschijnlijkheids- en impactschalen om risico's te kwantificeren en te prioriteren. Om de prioritering correct uit te voeren, wordt dus de kans * impact berekening uitgevoerd, om te kunnen bepalen waar een risico zich moet bevinden. Voor een gedetailleerd uitwerking van de risico's en de impact scale, zie 'Risicoanalyse rapport' hoofdstuk 6.

De nummers geven aan hoeveel risico's per blok aanwezig zijn, zie tabel 1. Zie voor verdere uitleg en onderbouwing van de risico's het Risicoanalyse rapport" document.



Figuur 2: Risk impact matrix

5.2.4. Beheerproces

De volgende tabel biedt een overzicht van de voorgestelde risicobeheerstrategieën voor Datacadabra, zoals uiteengezet in bijlage 10.9, 10.11 en 10.12 van het rapport. Deze bijlage omvat de secties 10.9.1 tot en met 10.9.3, en beschrijft uitvoerig de geïdentificeerde risico's en de bijbehorende behandelingsplannen. Het is belangrijk op te merken dat, hoewel deze strategieën in detail zijn uitgewerkt en aanbevolen voor implementatie, Datacadabra momenteel nog geen van deze beheer strategieën heeft geïmplementeerd. Het bedrijf overweegt deze plannen zorgvuldig en is in het proces van het beoordelen van de haalbaarheid en relevantie voor de specifieke bedrijfscontext. De tabel hieronder geeft een samenvatting van de voorgestelde aanpakken voor elk risico, zoals beschreven in de genoemde bijlage van het rapport.

Risico	**Risicovermindering**	**Risico-overdracht**	**Risicovermijding en -acceptatie**
Datalek en Gegevensverlies	Implementatie van multifactorauthenticatie, end-to-end-encryptie, en regelmatige cybersecuritytrainingen.	Afsluiten van cyberverzekeringen.	Beperken van toegang tot gevoelige data en gebruik van beveiligde cloudopslag.
Reputatieschade	Ontwikkeling van een crisiscommunicatieplan.	Niet van toepassing.	Accepteren van een bepaald niveau van risico met een plan voor reputatiemanagement.
Nalevingskosten en Aansprakelijkheid	Zorgen voor voortdurende naleving van wet- en regelgeving.	Overwegen van juridische verzekeringen.	Niet van toepassing.
Operationele Storingen	Uitvoeren van regulier onderhoud en updates van systemen, ontwikkeling van bedrijfscontinuïteits- en rampenherstelplannen.	Niet van toepassing.	Accepteren van kleine storingen met snelle responsmechanismen.

Risico	Risicovermindering	Risico-overdracht	Risicovermijding en -acceptatie
Verlies van Intellectueel Eigendom	Implementeren van strikte toegangscontroles en beveiligingsprotocollen.	Gebruik van auteursrechten.	Niet van toepassing.

Tabel 3: Beheerproces

5.2.5. Aanpak

De aanpak voor risicobeheer bij Datacadabra wordt sterk aanbevolen op basis van bevindingen uit het onderzoek en de feedback vanuit interviews, waaruit bleek dat een soortgelijke aanpak binnen Datacadabra gewenst is. Deze aanpak volgt een systematische en geïntegreerde benadering, in overeenstemming met de ISO 27001-normen. Uitgebreide details van deze aanpak zijn beschikbaar in interview 8 in bijlage 10.9 en worden ondersteund door aanvullende informatie in bijlage 10.11 en 10.12.

Deze benadering omvat het identificeren van risico's, het toewijzen van specifieke risico-eigenaren en het implementeren van gerichte actieplannen. Bijzondere aandacht wordt besteed aan twee risico's: datalekken en reputatieschade. Voor het beheer van datalekken hanteert Datacadabra maatregelen zoals multi-factor authenticatie, end-to-end-encryptie en cybersecuritytrainingen. Daarnaast wordt er voor het omgaan met reputatieschade een crisiscommunicatieplan ontwikkeld.

Bij Datacadabra ligt de focus op de aanpak van de twee risico's: datalekken en reputatieschade.

1. **Datalekken**: De aanpak bestaat uit het implementeren van multi factor authenticatie en end-to-end-encryptie, gecombineerd met regelmatige cybersecuritytrainingen. Deze maatregelen zijn essentieel vanwege de hoge impact van datalekken op de veiligheid van klant- en bedrijfsgegevens. Daarnaast wordt het risico van financiële verliezen door datalekken verder beperkt door het afsluiten van cyberverzekeringen.
2. **Reputatieschade**: Hier wordt een crisiscommunicatieplan ontwikkeld voor snelle en effectieve reactie op incidenten die de reputatie kunnen schaden. Dit is belangrijk om het vertrouwen van klanten en stakeholders te behouden en snel te herstellen in geval van incidenten.

Voor een volledig overzicht van de aanpak van alle andere risico's bij Datacadabra, inclusief hun specifieke beheerstrategieën en waarom deze belangrijk zijn, zie bijlage 10.11 en 10.12. Deze gedetailleerde aanpak zorgt voor een systematisch risicobeheer binnen de organisatie.

De focus op datalekken en reputatieschade in het risicobeheer bij Datacadabra komt voort uit de specifieke uitdagingen die deze risico's vormen voor de organisatie. Datalekken vormen een directe bedreiging voor de veiligheid van klant- en bedrijfsgegevens, wat kan leiden tot financiële verliezen en verlies van klantvertrouwen. De maatregelen zoals multi-factor authenticatie en end-to-end-encryptie zijn effectief in het verminderen van het risico op datalekken en worden gecombineerd met regelmatige cybersecuritytrainingen om de algehele veiligheidskennis binnen de organisatie te verbeteren. Deze studie onthult dat de implementatie van MFA uitstekende bescherming biedt, met meer dan 99,99% van MFA-beveiligde accounts die veilig bleven tijdens de onderzoeksperiode. (arxiv, sd)

Reputatieschade daarentegen kan langdurige negatieve gevolgen hebben voor het klantvertrouwen en de marktpositie. De ontwikkeling van een crisiscommunicatieplan zorgt ervoor dat Datacadabra snel en effectief kan reageren op incidenten die de reputatie kunnen schaden, waardoor het vertrouwen van klanten en stakeholders behouden blijft.

5.3. Integratie van de IT-informatiebeveiliging bij Datacadabra

Om de deelvraag 'Hoe kan Datacadabra informatietechnologie integreren in haar bedrijfsprocessen om de informatiebeveiliging te optimaliseren en te waarborgen?' te beantwoorden, is een gerichte aanpak vereist die specifieke technologische upgrades en beleidsmatige verbeteringen integreert, in lijn met ISO 27001 en de AVG/GDPR. Deze strategie focust op het versterken van de beveiliging van gegevens opgeslagen in Google Cloud, met de volgende specifieke stappen:

1. **Analyse van de Huidige versus Gewenste Situatie:** Datacadabra moet beginnen met een grondige analyse van hun huidige beveiligingsinfrastructuur, gericht op het identificeren van kwetsbaarheden in zowel hardware als software. Dit kan een beoordeling inhouden van de huidige firewall-configuraties, encryptiepraktijken, en endpoint securityoplossingen. Een belangrijk aspect hierbij is de beoordeling van hoe data wordt overgedragen en opgeslagen, met aandacht voor de beveiliging van de cloud-omgeving. Deze analyse zou ook de naleving van het huidige beleid ten aanzien van de AVG/GDPR en ISO27001 moeten bevatten.
2. **Bedrijfsprocessen en Integratiestrategieën**: Voor Datacadabra is het essentieel om informatiebeveiliging te integreren in alle bedrijfsprocessen. Dit kan bijvoorbeeld inhouden dat er strengere toegangscontroles worden geïmplementeerd voor gevoelige klantgegevens.
3. **Toekomstige Ontwikkelingen:** De focus ligt op automatisering van beveiligingstaken via AI-gedreven security analytics, en de integratie van privacybescherming in nieuwe productontwikkelingen. Dit omvat het toepassen van privacy by design principes in de ontwikkeling van nieuwe diensten.
4. **Incident Respons Plan (IRP):** Ontwikkeling van een gedetailleerd IRP, inclusief specifieke protocollen voor het snel identificeren en reageren op beveiligingsincidenten. Dit plan bevat duidelijke richtlijnen voor communicatie, herstel van systemen en data, en post-incident evaluatie.

De versterking van het informatiebeveiligingsbeleid en de naleving daarvan, vooral in relatie tot AVG/GDPR-compliance, wordt ondersteund door intern onderzoek en interviews (zie bijlage 10.1, interviews 4 tot 7). Dit omvat een grondige evaluatie van de wijze waarop persoonsgegevens worden verwerkt en beschermd binnen Google Cloud.

Verder is de upgrade van beveiligingstechnologie en -infrastructuur essentieel, waarbij keuzes gebaseerd zijn op grondige evaluaties van functionaliteit, reputatie en bedrijfsspecifieke eisen. Deze keuzes worden onderbouwd door een casestudy over de implementatie van cloud-beveiligingstechnologieën en de integratie van multi-factor authenticatie voor toegangsbeveiliging (zie hoofdstuk 10.7, 10.8 en 10.12 en bijbehorende bronvermelding).

5.3.1. Integratie van de IT-informatiebeveiliging bij Datacadabra

Deze tabel weergeeft de transitie van Datacadabra van een basisniveau van informatiebeveiliging naar een verbeterd niveau die voldoet aan de marktconform eisen. Waarbij volledige compliance en een effectief incidentbeheer centraal staan. Dit proces is gericht op het verminderen van risico's en het verbeteren van de algehele veiligheid en regelgevende naleving van het bedrijf, zoals gedetailleerd beschreven in het 'Risicoanalyse rapport'.

Hier is een tabel die de huidige situatie van Datacadabra met betrekking tot hun risicobeheer afzet tegen de gewenste situatie:

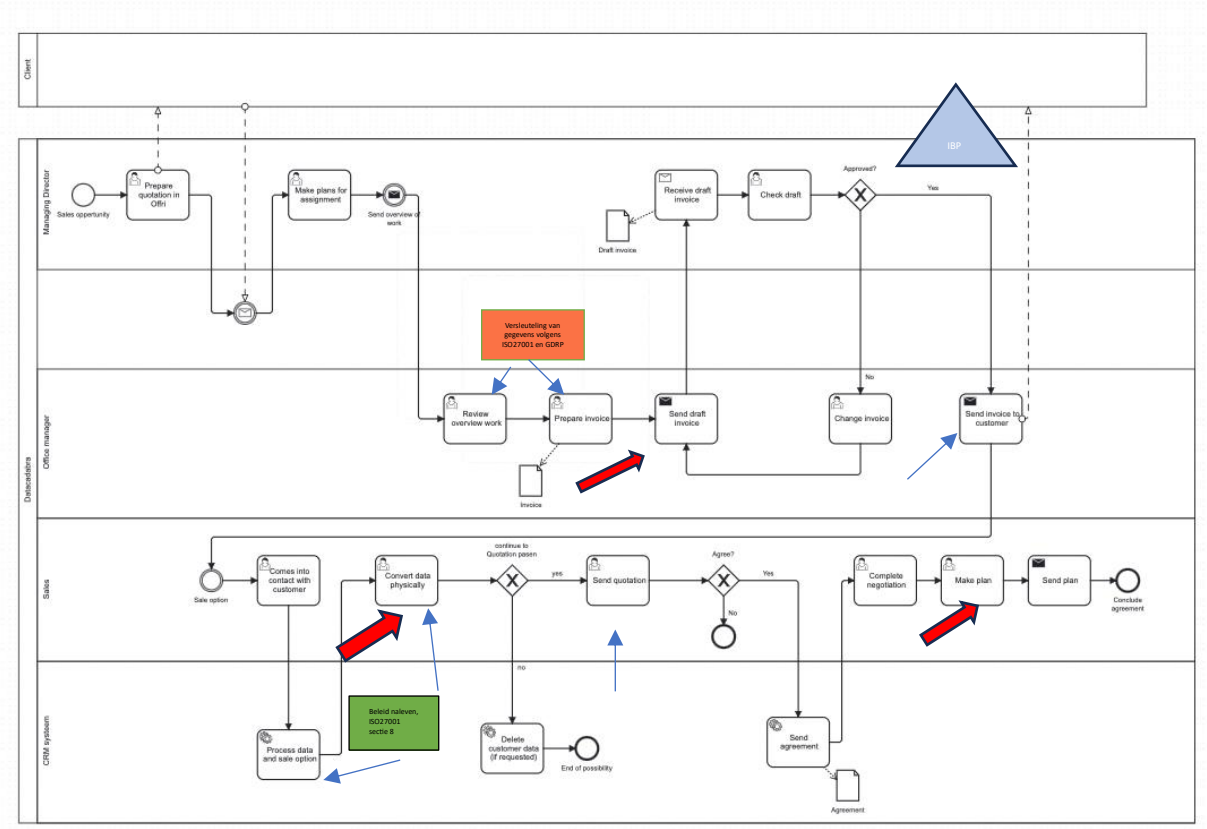
Risico	Huidige Situatie	Gewenste Situatie
Datalek en Gegevensverlies	Basis beveiligingsinfrastructuur; inconsistentie in beleidsnaleving.	Implementatie van multifactorauthenticatie, end-to-end-encryptie, regelmatige cybersecuritytrainingen; volledige naleving van het informatiebeveiligingsbeleid.
Reputatieschade	Geen specifiek crisiscommunicatieplan; reactief beheer.	Ontwikkeling van een proactief crisiscommunicatieplan; effectief reputatiemanagement.
Nalevingskosten en Aansprakelijkheid	Onvoldoende gestructureerde naleving van ISO 27001 en AVG/GDPR.	Strikte naleving van wet- en regelgeving; overwegen van juridische verzekeringen.
Operationele Storingen	Basis onderhoud van systemen zonder volledige rampenherstelplannen.	Regelmatig onderhoud en updates van systemen; ontwikkeling van bedrijfscontinuïteits- en rampenherstelplannen.
Verlies van Intellectueel Eigendom	Onvoldoende beveiliging van intellectueel eigendom.	Implementatie van strikte toegangscontroles en beveiligingsprotocollen; juridische bescherming via patenten en auteursrechten.
Effectief Incidentbeheer	Gebrek aan specifieke protocollen voor incidentbeheer.	Ontwikkeling van specifieke protocollen en procedures voor snel en efficiënt incidentbeheer.

Tabel 4: GAP-Analyse

5.3.2. Bedrijfsprocessen Datacadabra

In het proces van het integreren van IT en informatiebeveiliging bij Datacadabra, is het gebruik van Business Process Model and Notation (BPMN) voor het in kaart brengen van bedrijfsprocessen een waardevolle stap. BPMN biedt een gestructureerde en visuele representatie van de processen, wat essentieel is voor het identificeren van kritieke punten waarin informatiebeveiliging geïntegreerd moet worden. Door het verkoopproces op deze manier te modelleren, kan Datacadabra duidelijk zien waar beveiligingsmaatregelen en -protocollen moeten worden toegepast om de integriteit en vertrouwelijkheid van gevoelige

klantgegevens te waarborgen. Dit helpt niet alleen bij het verbeteren van de beveiliging, maar draagt ook bij aan een betere naleving van ISO 27001 en de AVG/GDPR.

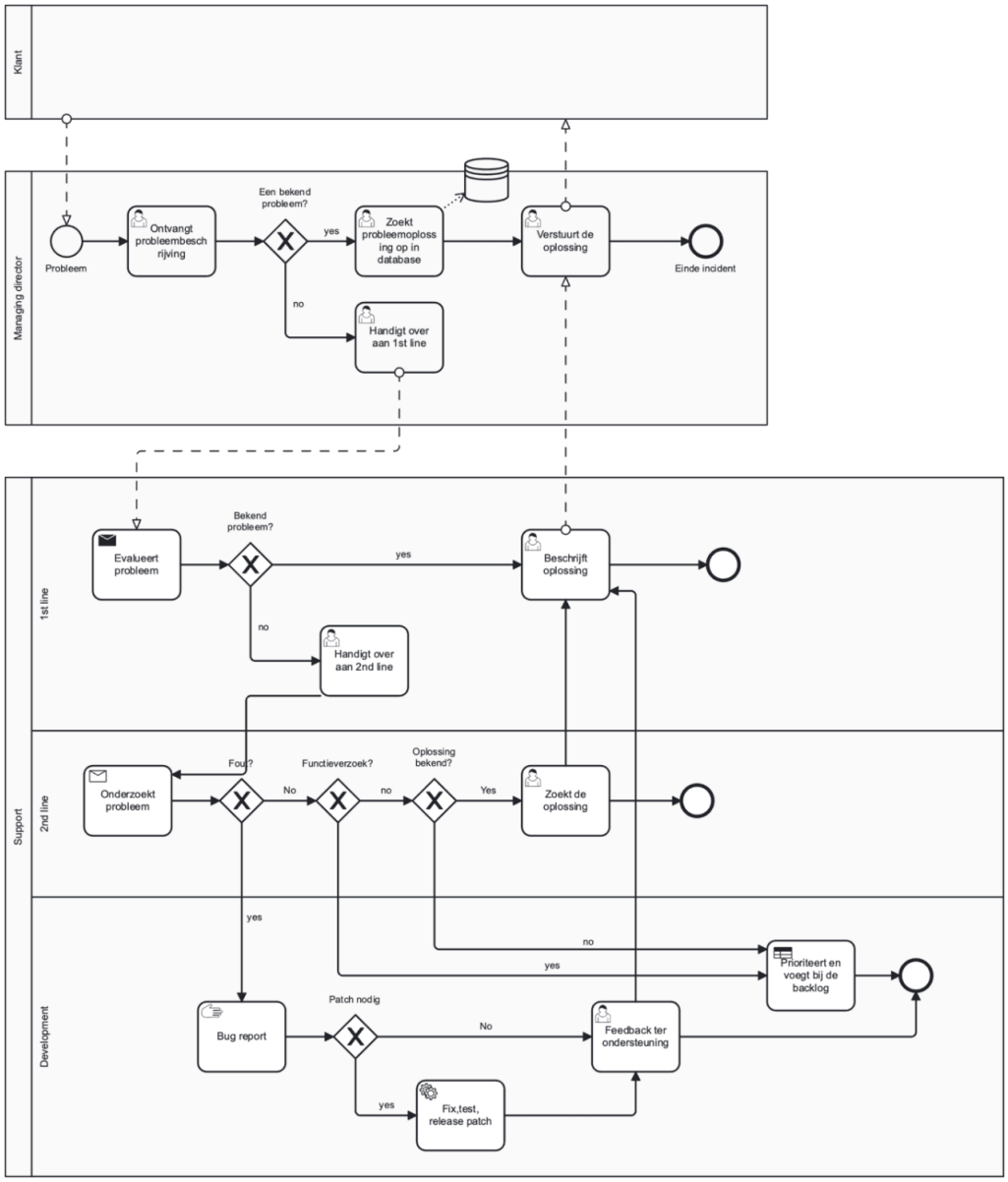


Figuur 3: BPMN-verkoopproces

Het aangepaste BPMN-diagram benadrukt de inzet voor sterke informatiebeveiliging en naleving van de regelgeving. Hiervoor zijn er specifieke stappen gemarkeerd waar beleidsnaleving essentieel is, zoals bij de omzetting van data en het verwerken van transacties, met visuele indicatoren zoals de pijlen en compliance labels, aangevuld met annotaties die verwijzen naar relevante beleidssecties zoals ISO 27001. Verder wordt bij kritieke stappen waar gegevens worden verwerkt en opgeslagen, de volledige naleving van ISO 27001 en AVG/GDPR benadrukt. Het diagram toont ook punten waar effectief incidentbeheer plaatsvindt, zie hiervoor de driehoek.

5.3.3. Incident respons plan

Dit IRP (incident respons plan) is ontwikkeld in overleg met de managing director, om te voldoen aan de ISO 27001-norm. Dit IRP heeft een belangrijke rol in het beschermen van informatie en het behouden en vergroten van klantvertrouwen. Dit IRP is visueel weergegeven in een BPMN, zoals hieronder te zien. De samenwerking tussen de klanten, directie en supportafdeling vanaf het moment van incidentmelding tot de oplossing van het incident zijn daarbij zichtbaar gemaakt. Dit proces bestaat uit drie lagen: klant, managing director en support, waarbij elke een belangrijk rol speelt in de evaluatie, afhandeling en communicatie van incidenten. De implementatie van dit proces verbetert de efficiëntie bij het beheren van incidenten, verkort de doorlooptijd en verhoogt de klanttevredenheid. Dit draagt bij aan Datacadabra's strategie voor informatiebeveiliging door de nadruk te leggen op goede samenwerking binnen de organisatie en snelle, klantgerichte actie.



Figuur 4: IRP

De "Managing Director" pool in een BPMN-diagram is gescheiden om aan te geven dat de directeur een belangrijke rol speelt in het proces die losstaat van de dagelijkse operationele activiteiten. Hier zijn een aantal redenen waarom de pool apart kan zijn:

- In het BPMN-diagram voor incidentrespons vertegenwoordigt de aparte pool van de Managing Director (MD) hun centrale rol in de besluitvorming, waarbij ze cruciale keuzes maken die de richting van de organisatie kunnen beïnvloeden, vooral tijdens incidenten.
- Als incidenten escaleren, kan de MD andere processen in gang zetten die buiten standaardprocedures vallen, zoals het initiëren van noodplannen of het maken van belangrijke publieke aankondigingen.
- De MD houdt ook toezicht op en controleert het incidentresponsproces, waarbij ze zorgen dat de genomen maatregelen in lijn zijn met de organisatiedoelstellingen en de organisatie beschermen, wat hun eindverantwoordelijkheid en macht binnen het proces bevestigt.

5.4. Versterking van interne communicatie en leiderschap

Om de deelvraag 'Hoe kan Datacadabra de samenwerking en communicatie tussen afdelingen verbeteren om een geïntegreerde aanpak van informatiebeveiliging te waarborgen?' volgens de ISO 27001 verder uit te werken, is het van belang te kijken naar specifieke richtlijnen en praktijken die daarbij aansluiten. Deze norm biedt richtlijnen en praktijken voor het opzetten, implementeren, onderhouden en continu verbeteren van een informatiebeveiligingsbeheersysteem (ISMS) binnen een organisatie. De norm benadrukt het belang van het beoordelen van informatiebeveiligingsrisico's en het implementeren van passende beveiligingsmaatregelen. Dit helpt organisaties bij het beschermen van informatie en het versterken van de vertrouwelijkheid, integriteit en beschikbaarheid van hun gegevens.

Om de samenwerking en communicatie bij Datacadabra te verbeteren voor effectieve informatiebeveiliging, worden de volgende stappen aanbevolen, zoals beschreven in bijlage 10.10:

1. **Versterken van de Communicatiestructuur**: Verbetering van de communicatieprocedures is noodzakelijk, zoals blijkt uit interviews (bijlage 10.10, interviews 1 en 2).
2. **Verbeteren van Feedbackprocessen**: Feedbackmechanismen moeten worden verbeterd voor effectievere communicatie, zoals geanalyseerd in bijlage 10.10, interviews 1 en 2.
3. **Rol van Leiderschap in Communicatie**: Leiderschapsontwikkeling is cruciaal voor het verbeteren van communicatie over informatiebeveiliging (zie hoofdstuk 2.4 en bijlage 10.10.2).
4. **Uitbreiding van Training en Bewustwording**: Regelmatige trainingssessies zijn nodig om het bewustzijn over informatiebeveiliging te verhogen.
5. **Ontwikkeling van een Centraal Communicatieplatform**: Een centraal platform voor het delen van updates is essentieel voor efficiënte communicatie.
6. **Implementatie van een ISMS**: Datacadabra moet een Information Security Management System implementeren voor een systematische aanpak van informatiebeveiliging (ISO 27001).
7. **Interne Communicatie volgens ISO 27001**: Regelmatige en duidelijke communicatie is nodig om bewustzijn en verantwoordelijkheden te vergroten.
8. **Rol in Leiderschap en Communicatie**: Het definiëren van rollen en verantwoordelijkheden binnen de organisatie is essentieel voor een effectieve informatiebeveiliging.
9. **Feedback- en Verbeteringsprocessen**: Het implementeren van feedbackmechanismen is belangrijk voor continue verbetering en betrokkenheid van werknemers.
10. **Regelmatige Evaluatie en Audit**: Periodieke audits zijn nodig om de effectiviteit van het ISMS te beoordelen en te verbeteren.
11. **Incidentmanagement en Responsplanning**: Een effectief incidentresponsplan is essentieel voor een snelle en efficiënte reactie op beveiligingsincidenten.

Voor meer toelichting en implementatie van deze stappen, zie bijlage 10.14 en bijlage 10.14.1. Deze maatregelen waarborgen een geïntegreerde aanpak van informatiebeveiliging binnen Datacadabra en verbeteren de beveiliging van gegevens.

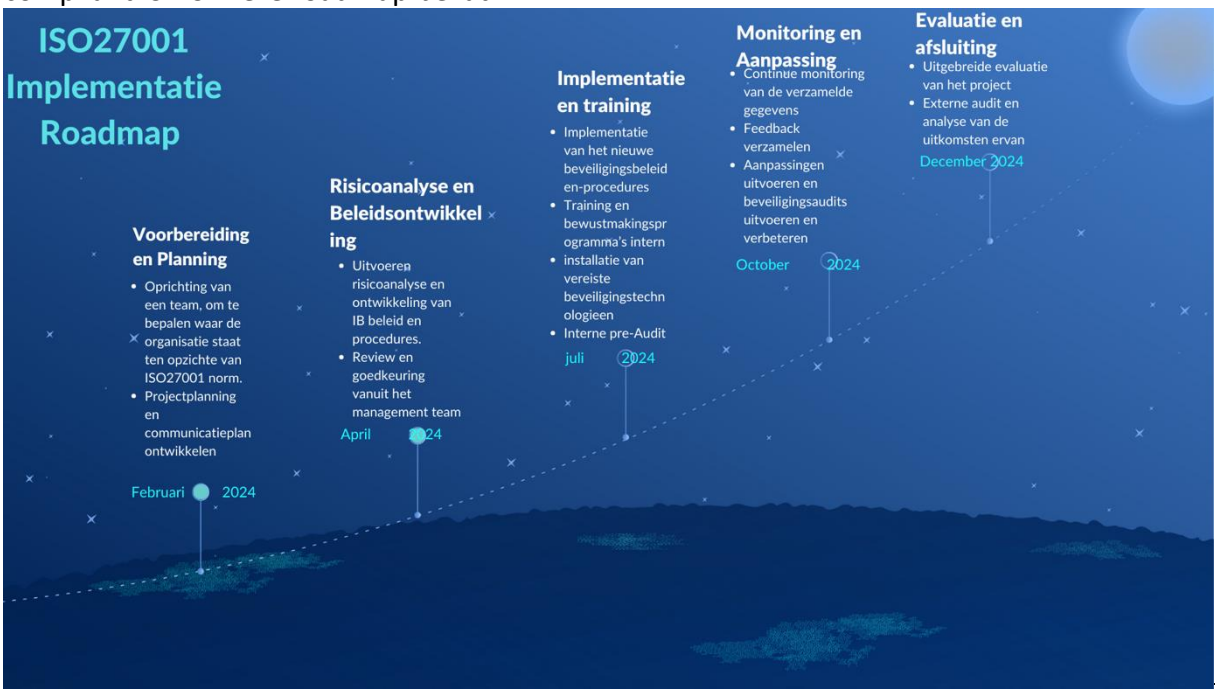
5.5. Implementatie van ISO 27001 bij Datacadabra

De waarborging van verbeterde informatiebeveiliging bij Datacadabra wordt gegarandeerd door de toekomstige implementatie van ISO 27001. De implementatie van ISO 27001 is zorgvuldig gepland met een roadmap die Datacadabra stap voor stap door volgt om de implementatie in orde te krijgen. Die loopt van een GAP-analyse en risicobeoordeling tot de uiteindelijke audit en certificering. Deze keuze is gebaseerd op uitgebreide analyses van Datacadabra's beveiligingsstatus en -behoeften.

Deze keuze werd onderbouwd door:

1. **Grondige risicoanalyse:** door het identificeren van specifieke beveiligingsrisico's en het beoordelen van de bestaande infrastructuur en praktijken, werd duidelijk dat een gestructureerde en internationaal erkende benadering nodig was.
2. **Naleving van wet- en regelgeving:** met de vereisten van compliance in gedachten, zoals GDPR zie hiervoor theoretisch kader hoofdstuk 2.5, werd de ISO 27001-standaard als passend beschouwd vanwege de nadruk ervan op continue naleving en verbetering.
3. **Stakeholderverwachtingen:** het toenemende belang dat klanten, partners en investeerders hechten aan informatiebeveiliging, maakte ISO 27001 een goede keuze voor het verbeteren van vertrouwen en reputatie.
4. **Internationale best practices:** ISO 27001 is wereldwijd erkend als norm die best practices voor informatiebeveiliging vertegenwoordigt, wat bijdraagt aan het concurrentievoordeel van Datacadabra in de technologiemarkt.

De implementatieroadmap voor ISO 27001 binnen Datacadabra is ontworpen om een gestructureerde overgang te bieden van de huidige stand van zaken naar een volledig compliant ISMS. Deze roadmap bevat:



Figuur 5: Roadmap

Deze gestructureerde aanpak is van belang voor Datacadabra om niet alleen te voldoen aan de normen van ISO 27001, maar ook om een cultuur van continue verbetering en

aanpassingsvermogen te ontwikkelen. Deze aanpak is essentieel voor het beschermen van gevoelige informatie en de bedrijfsmiddelen van de organisatie tegen de dynamische bedreigingen van de digitale wereld.

De kern van deze aanpak is de continue evaluatie en bijstelling van de beveiligingsstrategie. Dit proces begint met een regelmatige, grondige beoordeling van Datacadabra's beveiligingsprocessen en -systemen. Deze beoordeling houdt niet alleen rekening met de huidige normen en praktijken, maar kijkt ook vooruit, anticiperend op potentiële toekomstige risico's en technologische ontwikkelingen. Dit omvat het periodiek toetsen van het Incident Respons Plan (IRP) op effectiviteit, het regelmatig updaten van beveiligingsprotocollen en het trainen van medewerkers in de nieuwste beveiligingspraktijken.

Een belangrijk onderdeel van deze cultuur is het bevorderen van bewustzijn en betrokkenheid van alle medewerkers bij beveiligingskwesties. Door training en bewustmakingscampagnes versterkt Datacadabra het algemene beveiligingsbewustzijn binnen de organisatie. Dit helpt niet alleen bij het identificeren en mitigeren van risico's, maar bevordert ook een omgeving waarin continue verbetering een natuurlijk onderdeel is van de bedrijfscultuur.

6. Conclusie

6.1. Analyse van informatiebeveiligingsrisico's

Uit het onderzoek blijkt dat Datacadabra wordt geconfronteerd met zowel interne tekortkomingen (zoals onvolkomen beveiligingsinfrastructuur en gebrek aan bewustzijn bij medewerkers) als externe gevaren (zoals cyberaanvallen en datalekken). De bevindingen, afgeleid uit interviews met belanghebbenden, benadrukken de noodzaak om de databeveiliging en het bewustzijn van medewerkers te verbeteren, en om externe gevaren en regelgevingsnaleving te beheersen.

6.2. Risicobeheerproces

Datacadabra's beoogde risicobeheerproces, gebaseerd op ISO 27001, omvat een uitgebreide analyse van bedrijfsrisico's en het opstellen van gerichte actieplannen. Dit proces benadrukt het belang van een systematische aanpak voor het identificeren, beoordelen en beheersen van risico's om de bedrijfsveiligheid te verbeteren en continuïteit te waarborgen in een dynamische zakelijke en technologische omgeving.

6.3. Optimalisatie informatiebeveiliging

Voor de optimalisatie van informatiebeveiliging stelt Datacadabra voor om een streng beveiligingsbeleid in te voeren, vooral met betrekking tot gegevensbescherming in de cloud. Dit vereist verbeteringen in de IT-infrastructuur en technologie, evenals de implementatie van gedetailleerde plannen voor training, audits en incidentenbeheer. Deze maatregelen zijn gericht op het verhogen van de beveiliging en het vereenvoudigen van de naleving van moderne dataregels.

6.4. Versterken van interne communicatie en leiderschap

De strategie van Datacadabra om de samenwerking en communicatie tussen afdelingen te verbeteren voor een geïntegreerde informatiebeveiliging is in lijn met ISO 27001. De focus ligt op het versterken van de communicatiestructuur, het verbeteren van feedbackprocessen, en het benadrukken van de rol van leiderschap in communicatie. Deze stappen zijn cruciaal voor het verhogen van de effectiviteit van informatiebeveiligingspraktijken en het bevorderen van een cultuur van continue verbetering.

6.5. Implementatie van ISO 27001 binnen Datacadabra

Datacadabra is van plan om in de toekomst de implementatie van ISO 27001 om haar informatiebeveiliging te versterken, in gang te zetten. Dit proces, ondersteund door grondige risicoanalyses en naleving van regelgeving, is essentieel om internationale best practices te volgen en het concurrentievoordeel van Datacadabra in de IT-wereld te vergroten. De roadmap zorgt voor naleving en implementatie van ISO 27001 en bevordert een cultuur van continue verbetering, wat van belang is voor de langdurige bescherming van gevoelige informatie en bedrijfsmiddelen.

6.6. Conclusie op de hoofdvraag

Dit onderzoek benadrukt de noodzaak voor Datacadabra om haar informatiebeveiliging te verbeteren door zich te richten op drie kerngebieden: het identificeren van specifieke risico's die bijdragen aan het gebrek aan informatiebeveiliging, het ontwikkelen van strategieën om deze risico's aan te pakken, en het integreren van informatietechnologie in bedrijfsprocessen. De analyse van de specifieke risico's biedt inzicht in de kwetsbaarheden binnen de organisatie. Het aanpakken van deze risico's vereist een combinatie van technologische en organisatorische maatregelen. Ten slotte is de integratie van

informatietechnologie in de bedrijfsvoering essentieel voor een duurzame verbetering van de informatiebeveiliging.

Om de informatiebeveiliging te versterken, zou Datacadabra zich verder moeten inzetten en verdiepen in de implementatie van de ISO27001. Voor een gestructureerde aanpak, die ontworpen is om aan de diverse beveiligingsbehoeften te voldoen. Het belang van risicomanagement ligt in het vermogen van Datacadabra om potentiële beveiligingsbedreigingen proactief te identificeren en te beheren, waardoor risico's aanzienlijk worden verminderd. Procesoptimalisatie zorgt ervoor dat de beveiligingsprocedures voortdurend worden bijgehouden, wat leidt tot efficiëntere en effectievere beveiligingsmaatregelen.

Het ontwikkelen van een beveiligingscultuur is belangrijk, omdat het ervoor zorgt dat alle medewerkers zich bewust zijn van en bijdragen aan de beveiligingsinspanningen, wat de algehele beveiligingshouding van Datacadabra versterkt. Door deze strategie te implementeren, kan Datacadabra niet alleen haar risico's op het gebied van informatiebeveiliging effectief herkennen en verminderen, maar ook een meer betrouwbare informatiebeveiligingsomgeving creëren.

7. Aanbeveling

Om de informatiebeveiliging bij Datacadabra te verbeteren en richting ISO 27001-certificering te bewegen, is een gestructureerde aanpak noodzakelijk. Datacadabra moet allereerst haar processen herzien en inrichten met een duidelijke focus op veiligheid. Dit omvat het maken van duidelijke afbakeningen voor de beveiliging en het vaststellen van specifieke rolverdelingen. Belangrijk hierbij is de invoering van uitgebreide bewustwordings- en opleidingsprogramma's, integratie van geavanceerde monitoring- en detectietools, en het ontwikkelen van formele procedures voor reputatiebeheer en incidentrespons.

1. **Afbakeningen voor Veiligheid**: Duidelijke grenzen moeten worden gesteld tussen verschillende niveaus van toegang tot gevoelige informatie. Dit kan inhouden het scheiden van netwerken, het beperken van toegang tot kritieke systemen, en het instellen van duidelijke richtlijnen voor dataopslag en -beheer.
2. **Rolverdeling**: Het creëren van specifieke rollen binnen de organisatie, zoals een Chief Information Security Officer (CISO) die verantwoordelijk is voor het overzien van alle aspecten van informatiebeveiliging, en Data Protection Officers (DPO's) voor het beheren van gegevensbescherming en naleving van AVG/GDPR. Daarnaast is het belangrijk om IT-personeel op te leiden in specifieke beveiligingsprotocollen en hen duidelijke verantwoordelijkheden te geven.

Deze maatregelen, in combinatie met de in bijlage 10.14 voorgestelde roadmap en timeline, zullen een robuuste structuur vormen voor Datacadabra's informatiebeveiligingsbeheer, wat een essentiële stap is in de richting van ISO 27001-certificering.

7.1. Aanvullende aanbeveling

Het is aanbevolen dat Datacadabra een continue beoordeling van haar informatiebeveiligingsvereisten en -uitdagingen implementeert, bij voorkeur op kwartaalbasis. Hoewel eerdere onderzoeksresultaten zich niet op deze voortdurende veranderingen concentreerden, vanwege tijdsbeperkingen en de focus op direct toepasbare oplossingen, is het nu essentieel om verder te kijken. De initiële focus lag op het ontwikkelen van een basisstrategie in overeenstemming met ISO 27001-normen.

De suggesties, zoals het ontwikkelen van een cybersecurity dashboard, het integreren van AI en machine learning voor dreigingsdetectie, en het opzetten van een gespecialiseerd incidentrespons team, weerspiegelen de dynamische en steeds complexer wordende beveiligingsomgeving van Datacadabra. Deze aanbevelingen concentreren zich op het verbeteren van real-time monitoring, het verhogen van de responsiviteit en het versterken van de algemene beveiligingsinfrastructuur.

Datacadabra wordt geadviseerd om de aangedragen beveiligingsmaatregelen actief te integreren en toe te passen in de huidige systemen en processen. Dit omvat een periodieke evaluatie en aanpassing van de strategieën om te zorgen dat ze continu afgestemd blijven op de unieke behoeften en doelstellingen van de organisatie. Deze proactieve benadering zal bijdragen aan een dynamische en effectieve informatiebeveiliging.

8. Discussie

De validiteit van dit onderzoek wordt bevestigd door de toepassing van internationaal erkende normen (ISO 27001) en uitgebreid literatuuronderzoek. Deze aanpak garandeert dat de bevindingen en aanbevelingen niet alleen relevant zijn voor Datacadabra, maar ook voor andere organisaties die vergelijkbare informatiebeveiligingsuitdagingen ervaren. Dit verhoogt de externe validiteit, aangezien de resultaten toepasbaar en overdraagbaar zijn naar vergelijkbare bedrijfscontexten en uitdagingen in informatiebeveiliging.

De resultaten van het onderzoek laten zien dat de manier waarop Datacadabra nu zorgt voor de beveiliging van informatie beter kan. Ze gebruiken nu al sterke regels van ISO 27001 en goede methodes, maar er zijn nog dreigingen die ze kunnen verbeteren. Bijvoorbeeld, ze kunnen kunstmatige intelligentie (AI) gebruiken om bedreigingen sneller te vinden en een speciaal overzicht maken voor hun internetveiligheid. Dit laat zien dat, ook al hebben ze al een goede basis, ze moeten blijven werken aan het verbeteren van hun beveiliging omdat de gevaren op internet steeds veranderen.

De verwachting was dat de bestaande informatiebeveiligingsstrategie van Datacadabra, gebaseerd op de ISO 27001-normen, voldoende zou zijn om alle relevante risico's te beheren. Echter, de resultaten tonen aan dat, ondanks deze sterke basis, er aanvullende, vooruitstrevende maatregelen nodig zijn om de informatiebeveiliging te optimaliseren. Dit suggereert dat de complexiteit en dynamiek van hedendaagse cyberdreigingen een meer adaptieve en toekomstgerichte aanpak vereisen dan oorspronkelijk verwacht.

De verbetering in informatiebeveiliging kan worden verklaard door de gestructureerde aanpak en toewijding van Datacadabra aan de ISO 27001-normen, zoals ondersteund door literatuur en praktijkcases.

De keuze om geavanceerde technologieën zoals AI en cybersecurity dashboards in te zetten, kan gezien worden als een proactieve benadering van Datacadabra om haar informatiebeveiliging te versterken. Deze keuze weerspiegelt een begrip dat in de snel veranderende digitale wereld, waarin bedreigingen continu evolueren, een dynamische en innovatieve aanpak vereist is.
De bevindingen bieden nieuwe inzichten in de toepassing van ISO 27001 in een specifieke bedrijfscontext, zoals uiteengezet in het theoretisch kader.

Deze resultaten suggereren dat Datacadabra's informatiebeveiliging kan verbeteren door de aanbevolen methoden toe te passen, wat een versterkte bescherming tegen cyberdreigingen biedt. Het onderzoek focuste voornamelijk op ISO 27001-normen, wat een beperking vormt omdat andere benaderingen of technologieën niet werden overwogen. Dit kan de reikwijdte van de bevindingen beperken. Vervolgonderzoek zou kunnen focussen op het integreren van verschillende beveiligingsnormen en geavanceerde technologieën, zoals kunstmatige intelligentie, om de diepte en effectiviteit van Datacadabra's informatiebeveiligingsstrategie verder te verkennen en te versterken.

9. Bibliografie

(sd). Opgehaald van MindTools: https://www.mindtools.com/ag6pkn9/root-cause-analysis

(sd). Opgehaald van NEN: https://www.nen.nl/ict/digitale-ehtiek-en-veiligheid/cyber-privacy/informatiebeveiliging

(sd). Opgehaald van GDRP: https://gdpr--info-eu.translate.goog/?_x_tr_sl=en&_x_tr_tl=nl&_x_tr_hl=nl&_x_tr_pto=sc

(sd). Opgehaald van Journal of Information Security and Applications: https://www.sciencedirect.com/journal/journal-of-information-security-and-applications/publish/guide-for-authors

(sd). Opgehaald van arxiv: https://arxiv.org/abs/2305.00945

(2015). Opgehaald van DXfferent: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjD9_L63emDAxU81gIHHVYJCW4QFnoECBUQAQ&url=https%3A%2F%2Fdxfferent.nl%2Fblog%2Fiso%2Fiso-27001-controls-annex-a-uitgelegd%2F&usg=AOvVaw0uDCNClKaOewuv9UV-PTLa&opi=89978449

(2018). Opgehaald van NIST: https://www.cyberark.com/resources/ebooks/strengthening-critical-infrastructure-security?utm_source=google&utm_medium=paid_search&utm_term=pam_critical_infrastructure_emea_english_be_nl_lu&utm_content=ebook_strengthening_critical_infrastructure_security_w

(2019, 01 25). Opgehaald van ToolSHero: https://www.toolshero.com/leadership/competing-values-framework/

(2023, 12 19). Opgehaald van Lean Six Sigma Groep: Https://leansixsigmagroep.nl/lean-agile-en-six-sigma/bpmn-business-processing-model-notation/

Boom management. (2023, 2 7). Opgehaald van https://boommanagement.nl/artikel/alles-stakeholders-stakeholdermanagement-en-de-stakeholdertheorie/

Boom Management. (2023). Opgehaald van https://boommanagement.nl/artikel/alles-stakeholders-stakeholdermanagement-en-de-stakeholdertheorie/

Bureau Tromp. (2021, 8 2). Opgehaald van https://bureautromp.nl/root-cause-analyse-rca/#:~:text=Een%20Root%20Cause%20Analyse%20(RCA)%20heeft%20als%20doel%20om%20de,dat%20het%20probleem%20nogmaals%20optreedt.

Chen, L. G. (sd). *New approaches to password*. Opgehaald van https://iacr.org/archive/asiacrypt2004/33290228/33290228.pdf

continuous improvement. (sd). Opgehaald van https://www.betterup.com/blog/continuous-improvement#:~:text=Continuous%20improvement%20is%20the%20process,improvement%20method%20originated%20in%20Japan.

Datacadabra. (1, 1 2023). *Datacadabra.nl*. Opgehaald van www.datacadabra.nl

DXfferent BV. (22, 11 2023). *ISO27001 controles*. Opgehaald van https://dxfferent.nl/blog/iso/iso-27001-controls-annex-a-uitgelegd/

GertjanSchop. (2023, 4 23). Opgehaald van Managementmodellensite: https://managementmodellensite.nl/swot-analyse/

Kampshoff, S. A. (2016, juli 11). Opgehaald van communicatieplan: Https://issuu.com/annekampshoff/docs/communicatieplan_anne_kampshoff

Lias. (2013). Opgehaald van Inergy: https://www.googleadservices.com/pagead/aclk?sa=L&ai=DChcSEwi7gZnk0emDAxXkCQYAHbUlDA8YABACGgJ3cw&ae=2&gclid=Cj0KCQiA2KitBhCIARIsAPPMEhKI1NJ4jti4zJ

0gR_wOq1uEibPhIpFU6tJfqZHSBZ9KVEooL8FPupAaAt4oEALw_wcB&ohost=www.google.com&cid=CAESVuD2Jfh3tAZl7Qk5RLSkrwQs7
Okta. (sd). *Identitiy*. Opgehaald van https://www.okta.com/
Pfleeger. (2003). Opgehaald van security computing: https://eopcw.com/assets/stores/Computer%20Security/lecturenote_1704978481security-in-computing-5-e.pdf
scribbr. (2023, 10 30). Opgehaald van https://www.scribbr.nl/modellen/gap-model-servqual/
Stealthlabs. (2022, 12 27). *Cybersecurity Solutions*. Opgehaald van ttps://www.stealthlabs.com/
Stoneburgner, G. (2002). Opgehaald van https://www.googleadservices.com/pagead/aclk?sa=L&ai=DChcSEwiJiNOM1OmDAxV6WUECHW7qBxgYABACGgJ3cw&ae=2&gclid=Cj0KCQiA2KitBhCIARIsAPPMEhIF7ms6FVKjUGw0KudQ_k1M95DycIuGoQ9w1FaUKSfciNDfuJe6g3caArNCEALw_wcB&ohost=www.google.com&cid=CAESVuD2TPgq1x_3gj_Tcr_0_XFW6
Vleeshouwers,L. (2022, 10 30). *Scribbr*. Opgehaald van Https://www.scribbr.nl/modellen/gap-model-servqual/
Wiley&Sons, C. (1996). *protocols, algorithms, and source code* . Opgehaald van https://mrajacse.files.wordpress.com/2012/01/applied-cryptography-2nd-ed-b-schneier.pdf

10. Bijlagen

Wordt verder vervolgd met de interviews en andere analyse documenten

10.1. Interviews deelvraag 1

Interview 0

Datum	Doel van het Interview	Deelnemers
25 augustus 2023	Bespreken van de huidige staat van informatiebeveiliging bij Datacadabra, identificeren van de belangrijkste uitdagingen.	Rita (Interviewer), Catherine ter Haar (OM Datacadabra)

Interviewer: Hi, Catherine. Kun je iets vertellen over de huidige staat van informatiebeveiliging bij Datacadabra?
Catherine: Goedemorgen. Ja, momenteel ervaren we een tekort in onze informatiebeveiliging. Dit heeft geleid tot klantenverlies, voornamelijk omdat we geen erkend certificaat hebben, hiervoor kun je de kwartaalcijfers erbij halen en zien dat er vooral verlies is gedraaid sinds de potentiële en huidige klanten meer waarde zijn gaan hechten aan informatiebeveiliging.
Interviewer: Hoe heeft dit gebrek aan informatiebeveiliging Datacadabra beïnvloed?
Catherine: Het heeft onze betrouwbaarheid geschaad, vooral omdat onze klanten onze data science en AI-oplossingen gebruiken voor kritieke processen. Klanten zijn terughoudend zonder gegarandeerde veiligheid, wat eigenlijk in deze tijd wel logisch is. Ik zie veel voorbijkomen op het nieuws en in praktijk, kwesties van datalek/verlies van data en etc.
Interviewer: Wat zijn de plannen om deze uitdagingen aan te pakken?
Catherine: We werken aan het versterken van onze beveiligingsprotocollen en het behalen van een ISO 27001-certificaat. Ook verbeteren we onze interne trainingen en bewustzijn over informatiebeveiliging. Hopelijk kunnen we met behulp van jouw onderzoek veel zaken sneller af tikken wat vooraf moeten gebeuren.b
Interviewer: Hoe belangrijk is data voor jullie klanten?
Catherine: Zeer belangrijk. Onze klanten vertrouwen op de constante beschikbaarheid en veiligheid van onze diensten. We moeten die vertrouwen waarborgen door onze informatiebeveiliging te verbeteren.
Interviewer: Wat betekent dit voor de toekomst van Datacadabra?
Catherine: Het is essentieel voor onze groei en uitbreiding binnen de EU. We moeten aantonen dat we betrouwbare en veilige technologische oplossingen bieden.

Interview 1

Interviewer	Rita Simon
Naam Kandidaat	C. ter Haar
Datum	27 september 2023
Doelstelling	Inventarisatie naar bedreigingen, doelstelling om SWOT te maken

Strengths (Sterktes)

- Welke unieke bronnen heeft Datacadabra die de informatiebeveiliging ten goede komen?

A: Momenteel minimaal, maar wel zijn er partijen zoals (security) bedrijven en data bedrijven die beschikken over certificaten. Zo zorgen wij deels ervoor dat data beveiligd s

- Op welke aspecten van onze IT-infrastructuur zijn we het meest trots?

A: We handelen snel en denken vaak uit oplossingen voor de problemen. Ook onze snelle respons en flexibiliteit is een pluspunt.

Weaknesses (Zwaktes)

- Welke aspecten van onze huidige informatiebeveiligingspraktijken zijn onvoldoende?

A: Ons personeel is nog niet volledig getraind in het herkennen van phishing-pogingen

- In welke gebieden heeft ons personeel meer training of bewustzijn nodig over informatiebeveiliging?

A: In vooral omgaan met autorisaties en beveiligen van data

Opportunity's (Kansen)

- Hoe kunnen recente technologische vooruitgangen Datacadabra helpen om onze informatiebeveiliging te verbeteren?

A: Cloud-technologie biedt ons kansen om beter schaalbare beveiligingsoplossingen te implementeren.

- Zijn er nieuwe markttrends of -reguleringen die ons kunnen aanzetten tot verbetering van onze beveiligingsprotocollen?

A: Klantvragen en klantvertrouwen

Threats (Dreigingen)

- Welke externe beveiligingsbedreigingen zouden onze bedrijfsvoering kunnen verstoren?

A: Phishing-aanvallen worden steeds geavanceerder en zijn moeilijk te detecteren.

- Hoe kan een gebrek aan informatiebeveiliging onze reputatie bij klanten beïnvloeden?

A: Een datalek leidt ons tot onrust en klantenverlies

Interview 2

Interviewer	Rita Simon
Naam Kandidaat	GJ Naber
Datum	27 september 2023
Doelstelling	Inventarisatie naar bedreigingen, doelstelling om SWOT te maken

Strengths (Sterktes)

- Welke unieke bronnen heeft Datacadabra die de informatiebeveiliging ten goede komen?

A: Onze versleutelingstechnieken voor gevoelige data zijn state-of-the-art

- Op welke aspecten van onze IT-infrastructuur zijn we het meest trots?

A: snelle respons op incidenten

Weaknesses (Zwaktes)

- Welke aspecten van onze huidige informatiebeveiligingspraktijken zijn onvoldoende?

A: We hebben geen formele procedure voor het melden van beveiligingsincidenten.

- In welke gebieden heeft ons personeel meer training of bewustzijn nodig over informatiebeveiliging?

A: Er is onvoldoende bewustzijn over het belang van software-updates onder personeel

Opportunities (Kansen)

- Hoe kunnen recente technologische vooruitgangen Datacadabra helpen om onze informatiebeveiliging te verbeteren?

A: certificaat, bijbehorende softwarepakket

- Zijn er nieuwe markttrends of -reguleringen die ons kunnen aanzetten tot verbetering van onze beveiligingsprotocollen?

A: Industriestandaarden zoals ISO 27001 zorgen ervoor dat we onze beveiligingspraktijken continu verbeteren

Threats (Dreigingen)

- Welke externe beveiligingsbedreigingen zouden onze bedrijfsvoering kunnen verstoren?

A: Datalek, online aanvallen?

- Hoe kan een gebrek aan informatiebeveiliging onze reputatie bij klanten beïnvloeden?

A: Klanten beginnen bewijzen van onze beveiligingsmaatregelen te vragen voordat ze zakendoen.

Interview 3

Interviewer	Rita Simon
Naam Kandidaat	Vincent
Datum	27 september 2023
Doelstelling	Inventarisatie naar bedreigingen, doelstelling om SWOT te maken

Strengths (Sterktes)

- Welke unieke bronnen heeft Datacadabra die de informatiebeveiliging ten goede komen?

A: Momenteel niet veel bekend mbt informatiebeveiliging

- Op welke aspecten van onze IT-infrastructuur zijn we het meest trots?

A: De in-house ontwikkelde software zorgt voor een unieke aanpassing aan onze beveiligingsbehoeften

Weaknesses (Zwaktes)

- Welke aspecten van onze huidige informatiebeveiligingspraktijken zijn onvoldoende?

A: Wij voeren niet regelmatig beveiligingsaudits uit, echter wordt er minimaal mee gedaan.

- In welke gebieden heeft ons personeel meer training of bewustzijn nodig over informatiebeveiliging?

A: De training voor nieuwe medewerkers omvat geen informatiebeveiligingsprotocollen.

Opportunities (Kansen)

- Hoe kunnen recente technologische vooruitgangen Datacadabra helpen om onze informatiebeveiliging te verbeteren?

A: Wij denken dat als wij bewuster bezig gaan met het gebruik van onze tools en data en juiste training, dat informatie binnen onze afdeling beveiligd zal zijn

- Zijn er nieuwe markttrends of -reguleringen die ons kunnen aanzetten tot verbetering van onze beveiligingsprotocollen?

A: -

Threats (Dreigingen)

- Welke externe beveiligingsbedreigingen zouden onze bedrijfsvoering kunnen verstoren?

A: Datalek, DDoS- aanvallen, en hardware exploits

- Hoe kan een gebrek aan informatiebeveiliging onze reputatie bij klanten beïnvloeden?

A: Negatieve media-aandacht rondom datalekken in onze industrie heeft sommige klanten voorzichtiger gemaakt.

SWOT-analyse

Strengths	Weaknesses
1. Innovatie en Technologie 2. Kennis en Expertise	2. Ontbreken van beveiligingsinfrastructuur 3. Bewustzijn en Training 3. Afhankelijkheid van Cruciale Gegevens

Opportunities	Threats
3. Regelgeving als Richtlijn 2. Marktvraag	2. Datalekken en Gegevensverlies 3. Reputatieschade 4. Nalevingskosten 5. Aansprakelijkheid 6. Verlies van klantvertrouwen 7. Intellectueel eigendom

Figuur 5: SWOT-analyse

Bij Datacadabra hebben we een aantal specifieke uitdagingen geïdentificeerd die bijdragen aan ons huidige gebrek aan informatiebeveiliging. Deze uitdagingen zijn essentieel om te herkennen en aan te pakken om onze informatiebeveiligingspraktijken te versterken.

1. **Diversiteit en Integratie van Systemen**: We hebben geconstateerd dat de verscheidenheid aan gebruikte systemen en tools niet optimaal geïntegreerd zijn. Deze fragmentatie kan zwakke plekken in onze beveiligingsstructuur creëren, waardoor het moeilijker wordt om een naadloze beveiligingsstrategie te hanteren.
2. **Medewerkersbewustzijn en Training**: Een ander kritiek punt is het gebrek aan bewustzijn en training van onze medewerkers op het gebied van informatiebeveiliging. Aangezien menselijke fouten een aanzienlijk risico kunnen vormen, is het verhogen van het beveiligingsbewustzijn onder het personeel essentieel.
3. **Incidentrespons en Beheermaatregelen**: Ons vermogen om te reageren op beveiligingsincidenten is nog in ontwikkeling, wat suggereert dat we niet volledig voorbereid zijn op het snel adresseren en beheren van mogelijke inbreuken.
4. **Monitoring en Detectie**: Er zijn ook tekortkomingen in onze monitoring- en detectieprocessen geïdentificeerd. Dit betekent dat we niet altijd in staat zijn om beveiligingsdreigingen tijdig te identificeren, wat ons reactievermogen op incidenten vertraagt.
5. **Beheer van Derde Partijen**: De interactie met externe partijen vormt een aanzienlijk risico dat nog niet volledig onder controle is. Het managen van deze externe beveiligingsrisico's is een complexe taak die een gedegen aanpak vereist.
6. **Risicobeheer**: Onze aanpak van risicobeheer moet worden versterkt. Het lijkt erop dat onze huidige risicobeoordelings- en beheerprocessen niet afdoende zijn om alle potentiële risico's die we hebben geïdentificeerd, te ondervangen.
7. **Beveiligingsmentaliteit**: Tot op heden lijkt onze aanpak van informatiebeveiliging reactief te zijn geweest, met verbeteringen die worden doorgevoerd na het ontstaan van problemen. Een verschuiving naar een meer proactieve beveiligingsmentaliteit is noodzakelijk om onze systemen robuuster te maken.
8. **Technologische Kwetsbaarheden**: Tot slot is er een behoefte aan het adresseren van technologische kwetsbaarheden in onze infrastructuur. De keuze van de juiste tools

en de configuratie van onze oplossingen zijn cruciale stappen die we moeten nemen om onze informatiebeveiliging te waarborgen.

In conclusie, het is duidelijk dat een multidimensionale aanpak vereist is om de informatiebeveiliging bij Datacadabra te verbeteren. Door deze specifieke gebieden aan te pakken, kunnen we een meer robuust en veilig informatiesysteem bouwen dat de gegevens van onze klanten en onze bedrijfsvoering beschermt.

10.1.1. Meeting CTO en MD

Samenvatting Vergadering: Informatiebeveiliging bij Datacadabra
Datum: 18-10-2023
Wie waren er: Managing Director (MD) en de Chief Technology Officer (CTO) van Datacadabra
Doel: Bespreken van de risico's voor onze informatiebeveiliging en wat we eraan kunnen doen
Belangrijkste Punten:

1. **Risico's Besproken:**
    - De CTO legde uit over problemen zoals datalekken, gegevensverlies en hoe slecht dit is voor ons bedrijf.
    - Ze praatten over hoe belangrijk het is om onze e-mails beter te beveiligen en ervoor te zorgen dat alleen de juiste mensen toegang hebben tot belangrijke informatie.
2. **Wat betekent dit voor ons bedrijf:**
    - Ze bespraken hoe deze problemen Datacadabra kunnen raken, vooral ons werk met AI en data-analyse.
    - Als klanten en leveranciers ons niet meer vertrouwen, kan dit slecht zijn voor onze positie op de markt en onze groei.
3. **Plannen om dit aan te pakken:**
    - Er werden plannen gemaakt om elk probleem aan te pakken, en deze moeten voldoen aan de ISO 27001 normen.
    - Er werd gesproken over het beter maken van onze beveiliging en het trainen van onze medewerkers om bewuster te zijn van veiligheidsrisico's.
    - Ze spraken ook over het belang van een goed plan voor als er iets misgaat, vooral voor datalekken.
4. **Volgen van regels:**
    - Het is heel belangrijk dat we ons aan de regels houden en ze benadrukten de mogelijke kosten als we dat niet doen.
    - De CTO stelde voor om regelmatig te controleren of we nog steeds aan alle regels voldoen.
5. **Volgende stappen en wie doet wat:**
    - De MD vroeg de CTO om een plan te maken voor alles wat ze besproken hadden.
    - Ze spraken af om elkaar regelmatig te ontmoeten om te kijken hoe het gaat met de verbeteringen.

Conclusies:

Ze waren het erover eens dat we goed moeten letten op onze informatiebeveiliging. De MD zei dat iedereen in het bedrijf moet helpen om de beveiliging beter te maken. De CTO gaat ervoor zorgen dat we de risico's aanpakken en houdt het management op de hoogte.

Interview 4 Gert-Jan Risico Analyse

Interviewer	Rita Simon
Deelnemer	Gert-Jan Naber
Datum	20-09-2023
Doelstelling	Het evalueren en verbeteren van de huidige risicobeheerstrategieën en -processen van de organisatie door middel van inzichten en feedback verzameld van interne en externe belanghebbenden

1. **Hoe schat u de effectiviteit in van het huidige "Monitoring en Detectieproces" binnen de organisatie?**

Om eerlijk te zijn, onze huidige monitoring en detectieprocessen zijn nog in een beginstadium. We gebruiken basis antivirussoftware en firewallbeveiliging, maar we zijn ons ervan bewust dat we moeten investeren in geavanceerdere systemen om echt effectief te zijn

2. **Kunt u de huidige workflow beschrijven van het rapportage- en analyseproces na een beveiligingsincident?**

Wanneer er een beveiligingsincident wordt gedetecteerd, is het onze procedure om dit onmiddellijk te rapporteren aan ons IT-team. Vervolgens voeren zij een eerste analyse uit. Echter, onze workflow is nog niet geformaliseerd en dit is iets waar we aan werken om te verbeteren.

3. **Hoe vaak worden incidentresponsprocedures bijgewerkt en geoefend binnen uw organisatie?**

We hebben onze incidentresponsprocedures nog niet formeel bijgewerkt of geoefend. Het staat op onze agenda voor het komende kwartaal om deze processen te formaliseren en te oefenen met betrokken teams.

4. **Welke tools en technieken gebruikt uw organisatie momenteel voor datalekpreventie?**

Zoals eerder vermeld, vertrouwen we momenteel op standaard beveiligingssoftware. We zijn ons ervan bewust dat dit niet voldoende is en overwegen daarom extra tools zoals encryptie en intrusion detection systemen

5. **Hoe gaat uw organisatie om met de back-up en herstel van gegevens om potentiële gegevensverlies te voorkomen?**

We voeren regelmatige back-ups uit, maar hebben nog geen uitgebreid herstelplan. Dit is iets waar we aan moeten werken om ervoor te zorgen dat we snel kunnen reageren in het geval van gegevensverlies.

6. **Op welke manier wordt het vertrouwen van klanten en leveranciers gemeten en beheerd?**

Klant- en leveranciersvertrouwen wordt momenteel niet formeel gemeten. We zijn van plan om enquêtes en feedbacksessies te introduceren om dit beter te kunnen beheren

7. **Hoe worden de kosten van naleving en aansprakelijkheid gemonitord en gecontroleerd?**

We zijn ons pas recent bewust geworden van de kosten die samenhangen met naleving en aansprakelijkheid, en zijn in de beginfase van het monitoren en controleren van deze kosten

8. **Wat zijn de procedures voor het beheer van reputatieschade en hoe worden deze geactiveerd?**

We hebben geen formele procedures voor reputatiemanagement. Dit is een gebied waar we verbetering nodig hebben en we zullen extern advies inwinnen om deze processen te ontwikkelen.

9. **Hoe worden operationele storingen en de impact ervan op de organisatie beoordeeld?**

Operationele storingen worden ad hoc beoordeeld. We realiseren ons dat we een systematische aanpak nodig hebben om de impact hiervan te begrijpen en te verminderen

10. **Wat zijn de stappen die uw organisatie neemt om intellectueel eigendom te beschermen?**

We hebben algemene richtlijnen voor het beveiligen van intellectueel eigendom, zoals wachtwoordbescherming en beperkte toegang, maar erkennen dat we moeten investeren in sterkere maatregelen zoals digitale rechtenbeheer en uitgebreide werknemerstraining.

11. **Hoe evalueert Datacadabra de effectiviteit van de specifieke actieplannen voor elk geïdentificeerd risico, en hoe wordt deze evaluatie gebruikt om de risicobeheerstrategieën continu te verbeteren in overeenstemming met de veranderende regelgevingslandschap en bedrijfsomgeving?**

Datacadabra evalueert de effectiviteit van haar actieplannen door regelmatig de uitvoering en resultaten van deze plannen te beoordelen tegen de vastgestelde numerieke scores voor prioriteit, die zijn gebaseerd op de waarschijnlijkheid en impact van elk risico. Deze evaluatieproces, ondersteund door de ISO 27001 standaarden, stelt ons in staat om continu te monitoren of de genomen beveiligingsmaatregelen en nalevingsinspanningen effectief zijn in het verminderen van de risico's tot een acceptabel niveau.

De feedback verkregen uit deze evaluaties wordt gebruikt om onze risicobeheerstrategieën voortdurend aan te passen. Wanneer een actieplan niet de gewenste resultaten oplevert of wanneer nieuwe risico's ontstaan door veranderingen in de regelgeving of bedrijfsomgeving, worden de risicobeoordelingstabellen bijgewerkt. Dit zorgt ervoor dat de risico’s met de

hoogste ernst altijd de nodige aandacht krijgen en dat onze aanpak altijd up-to-date en in lijn is met de beste praktijken in de industrie en de vereisten van ISO 27001.

Interview 5 Mark Bulthuis

Interviewer	Rita Simon
Deelnemer	Mark Bulthuis
Datum	20-09-2023
Doelstelling	Het evalueren en verbeteren van de huidige risicobeheerstrategieën en -processen van de organisatie door middel van inzichten en feedback verzameld van interne en externe belanghebbenden.

1. **Hoe schat u de effectiviteit in van het huidige "Monitoring en Detectieproces" binnen de organisatie?**

Als nieuwkomer zie ik dat we basismonitoring hebben, maar de diepte van detectie is beperkt. Ik zou zeggen dat er ruimte is voor verbetering, vooral in termen van geautomatiseerde dreigingsdetectie.

2. **Kunt u de huidige workflow beschrijven van het rapportage- en analyseproces na een beveiligingsincident?**

Voor zover ik weet, wordt een incident via e-mail gerapporteerd en handmatig door het team geanalyseerd. De workflow lijkt ad hoc en zou baat hebben bij een meer gestructureerde aanpak.

3. **Hoe vaak worden incidentresponsprocedures bijgewerkt en geoefend binnen uw organisatie?**

Ik ben nog niet betrokken geweest bij een update of oefening van incidentresponsprocedures. Mijn indruk is dat dit niet regelmatig gebeurt

4. **Welke tools en technieken gebruikt uw organisatie momenteel voor datalekpreventie?**

We hebben standaard firewalls en antimalware, maar ik ben nog niet tegengekomen dat we geavanceerde preventietechnologieën gebruiken zoals DLP-systemen of geavanceerde endpointbescherming.

5. **Hoe gaat uw organisatie om met de back-up en herstel van gegevens om potentiële gegevensverlies te voorkomen?**

Back-ups lijken gepland, maar ik ben niet volledig op de hoogte van het herstelproces. Het lijkt erop dat er geen duidelijk herstelplan is in geval van een grote verstoring.

6. **Op welke manier wordt het vertrouwen van klanten en leveranciers gemeten en beheerd?**

Ik heb geen meetinstrumenten voor vertrouwen gezien. Wellicht is dit iets wat meer op het niveau van het management wordt gedaan.

7. **Hoe worden de kosten van naleving en aansprakelijkheid gemonitord en gecontroleerd?**

Ik heb geen inzage in hoe kosten worden gemonitord; als technisch specialist is dat buiten mijn huidige werkscope.

8. **Wat zijn de procedures voor het beheer van reputatieschade en hoe worden deze geactiveerd?**

Reputatiemanagementprocedures zijn niet iets waar ik direct mee te maken heb gehad, maar ik heb gehoord dat er een noodplan moet zijn, alhoewel ik niet weet hoe dit werkt.

9. **Hoe worden operationele storingen en de impact ervan op de organisatie beoordeeld?**

In de korte tijd dat ik hier ben, heb ik gemerkt dat storingen meestal case-by-case worden aangepakt zonder een formele post-mortem analyse.

10. **Wat zijn de stappen die uw organisatie neemt om intellectueel eigendom te beschermen?**

Intellectueel eigendom wordt beschermd met toegangscontroles en wachtwoordbeleid, maar ik ben nog niet bekend met een uitgebreid IP-beveiligingsplan.

Interview 6 met Peter Hoekstra

Interviewer	Rita Simon
Deelnemer	Peter Hoekstra
Datum	12-09-2023
Doelstelling	Hierbij gaat het om dat het bedrijf zich aan de wetten en regelgeving houdt en zich daarmee bewuster maakt over informatiebeveiliging

Interview 7 met CTO

Interviewer	Rita Simon
Deelnemer	Mark Bulthuis
Datum	10-12-2023
Doelsrellinf	Een dieper inzicht te verkrijgen in de huidige beveiligingsuitdagingen van het bedrijf en de plannen voor het verbeteren van de informatiebeveiliging

Interviewer: Mark, wat zijn de belangrijkste beveiligingsuitdagingen bij Datacadabra?

Mark (CTO): We moeten onze informatiebeveiliging en technologie verbeteren. Er zijn inconsistenties in de handhaving van ons beleid en we moeten onze infrastructuur updaten om aan de ISO 27001 en AVG/GDPR te voldoen.
Interviewer: Hoe pakken jullie dit aan?
Mark: Na analyse en overleg met adviseurs werken we aan beleidsversterking en technologische upgrades. Dit omvat betere training voor personeel en efficiëntere beveiligingsmaatregelen.
Interviewer: En de toekomst?
Mark: We streven naar een geoptimaliseerde beveiliging om Datacadabra beter te beveiligen en het vertrouwen van onze klanten te versterken.

1. Hoe schat u de effectiviteit in van het huidige "Monitoring en Detectieproces" binnen de organisatie?

Als aandeelhouder houd ik de algemene prestatie-indicatoren in de gaten. Ik ben tevreden zolang ik zie dat we compliant zijn en geen grote incidenten hebben. Details over de processen laat ik aan het management over.

2. **Kunt u de huidige workflow beschrijven van het rapportage- en analyseproces na een beveiligingsincident?**

Ik verwacht dat alle incidenten grondig worden geanalyseerd en dat er een rapport van het management komt over de genomen acties. De exacte workflow is voor mij als aandeelhouder niet dagelijks zichtbaar.

3. **Hoe vaak worden incidentresponsprocedures bijgewerkt en geoefend binnen uw organisatie?**

Ik ga ervan uit dat het team deze procedures regelmatig bijwerkt; het is iets dat ik bespreek tijdens de bestuursvergaderingen om ervoor te zorgen dat onze belangen worden beschermd.

4. **Welke tools en technieken gebruikt uw organisatie momenteel voor datalekpreventie?**

Ik ben niet betrokken bij de operationele keuze van tools en technieken. Echter, ik steun investeringen in robuuste systemen die onze data beveiligen, wat essentieel is voor onze bedrijfswaarde.

5. **Hoe gaat uw organisatie om met de back-up en herstel van gegevens om potentiële gegevensverlies te voorkomen?**

Het management heeft me verzekerd dat we sterke back-upprotocollen hebben. Ik controleer of de investeringen die we doen in technologie overeenkomen met de beste praktijken in de industrie.

6. **Op welke manier wordt het vertrouwen van klanten en leveranciers gemeten en beheerd?**

Voor mij is het belangrijk dat ons bedrijf een goede reputatie heeft. Ik houd toezicht op klanttevredenheid en leveranciersrelaties door regelmatige updates en rapporten van het management.

7. **Hoe worden de kosten van naleving en aansprakelijkheid gemonitord en gecontroleerd?**

Ik bekijk de financiële rapportages en zorg ervoor dat de kosten voor naleving gerechtvaardigd zijn en niet onze winstmarges ondermijnen, terwijl we toch aan alle regelgeving voldoen.

8. **Wat zijn de procedures voor het beheer van reputatieschade en hoe worden deze geactiveerd?**

- Geen idee

9. **Hoe worden operationele storingen en de impact ervan op de organisatie beoordeeld?**

De impact van storingen op onze financiële en operationele prestaties is voor mij van belang.

10. **Wat zijn de stappen die uw organisatie neemt om intellectueel eigendom te beschermen?**

Als aandeelhouder zorg ik ervoor dat we investeren in goede juridische ondersteuning om ons intellectueel eigendom te beschermen. Ik vertrouw op ons juridisch team om ons eigendom veilig te stellen.

10.1.2. Analyse samenvatting van de interviews

1. **Bewustzijn en prioritering op Managementniveau**

De managing director is bewust van de tekortkomingen binnen de huidge beveiligingsmaatregelen en ziet de noodzaak wel erin om aanpassingen te brengen. Echter, de specifieke technische en operationele kennis over de processen ontbreekt, wat wijst op een kloof tussen management en technische uitvoering.

2. **Technische competentie en ervaring**

Als wij kijken naar de technische kant, enkel op de interviews gebaseers, lijkt er echt wel een niveau te zitten in detail bewustzijn voor de operationele aspecten van beveiliging. Echter wordt er voor alsnog niet bewust omgegaan met de data die verkregen wordt, hoewel ze wel bekend zijn met de risico's e ernst ervan.

3. **Nieuwe perspectieven vs gevestigde processen**

Er is niet een volledige inwerkprocedure, al helemaal niet punten waar er op gelet moet worden met betrekking tot informatiebeveiliging binnen het bedrijf. Volgens de CTO, Mark dus, worden de nieuwe medewerkers met onvolledigheden ingewerkt omdat er simpel weg veel inwerkprocedures en beleidsstukken mist.

4. **Strategisch overzichten en aandeelhoudersbelangen**

Vanuit het management wordt er focust gelegd op de reputatie en financiën van een organisatie. En erg minder op het operationele of technische detailniveau. De aandeelhouder vindt niet noodzakelijk om ook daarmee bezig te zijn, hij vertrouwt erop dat de technische afdeling zelf uitkomt met de CTO. Dit benadrukt dat er mogelijk een discrepantie is tussen wat de aandeelhouders zien en begrijpen en de dagelijkse realiteit van het informatiebeveiligingslandschap binnen de organisatie.

5. **Procedures en communicatie**

Er lijkt een groot gat in communicatie. Er is gebrek aan formele en gestructureerde procedures te zijn, zoals het gebrek aan formele reputatiemanagementprocedures en ad ho beoordelingen van operationele storingen. Dit duidt op noodzaak voor meer gestructureerde processen en communicatiekanalen.

6. **Respons op incidenten**

Uit meerdere gesprekken met de stakeholders, komt naar boven dat incidentrespons nog niet volwassen is. Hiermee wordt er bedoeld dat er geen of minimale updates/ oefeningen worden uitgevoerd. Dit is een aanzienlijk risico voor de organisatie en wijst op de behoefte aan een gestructureerde aanpak voor incidentmanagement.

7. **Compliance en kostenbeheersing**

De bewustwording rond de kosten van naleving en aansprakelijkheid begint te groeien, maar er is nog geen duidelijk beheer of monitoring van deze kosten.

8. **Datamanagement en bescherming**

Back-up- en herstelprocedures zijn NIET aanwezig maar worden wel regelmatig uitgevoerd. Wel ontbreekt er een uitgebreid herstelplan wat aangeeft dat de organisatie kwetsbaar kan zijn voor gegevensverlies.

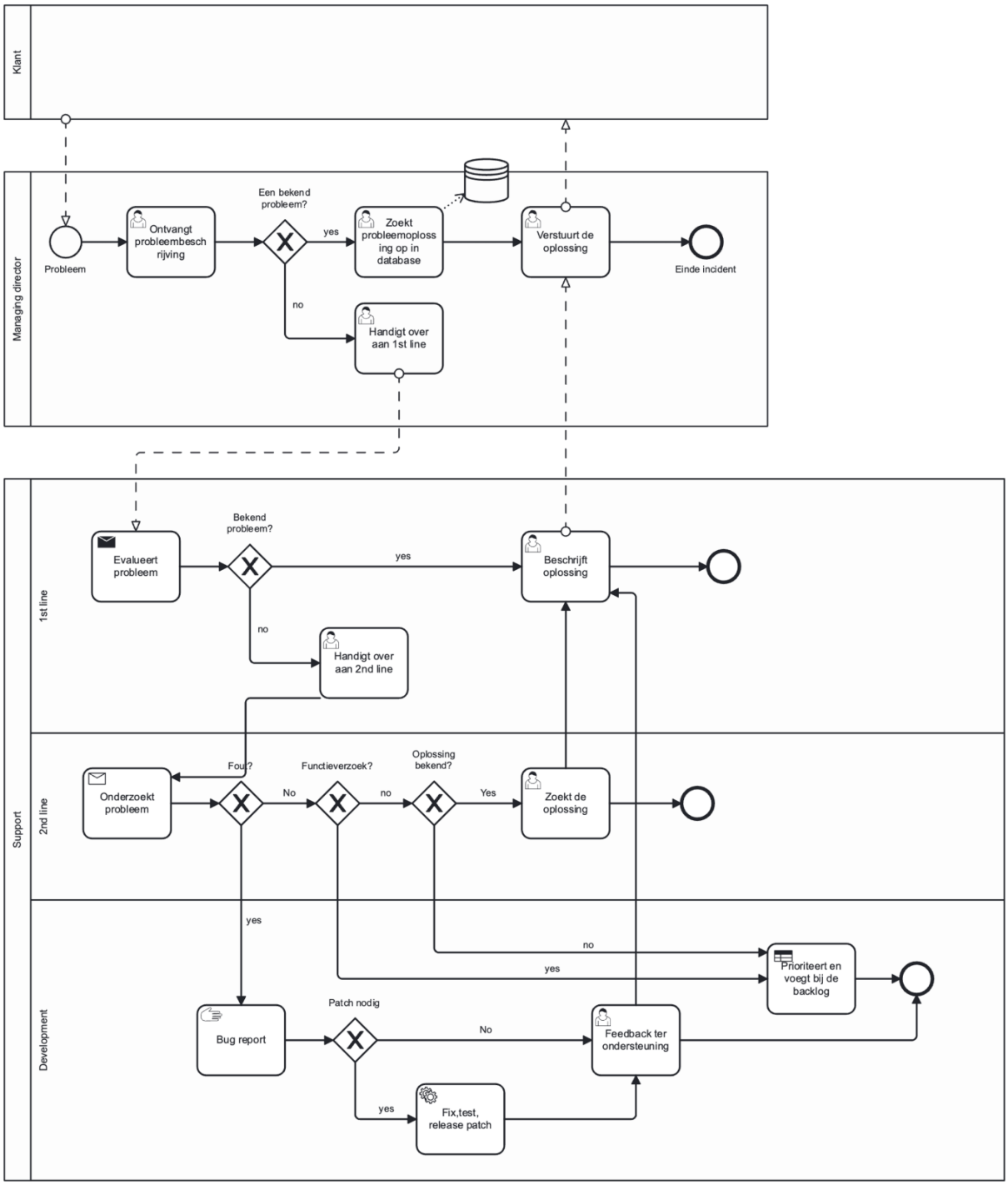
Conclusie

Deze analyse geeft aan dat Datacadabra's huidige aanpak van informatiebeveiliging en risicobeheer een gefragmenteerde aanpak is die verbetering behoeft. Datacadabra moet werken aan het overbruggen van de kloof tussen managementbewustzijn en technische uitvoering, het formaliseren van processen, het versterken van de incidentrespons en het verbeteren van de communicatie over de gehele linie. Een samenhangende strategie die rekening houdt met zowel de zakelijke als technische aspecten van informatiebeveiliging zal cruciaal zijn voor het verbeteren van hun beveiligingshouding en het voldoen aan de verwachtingen van alle stakeholders.

10.2. IRP

In dit hoofdstuk wordt het nieuwe incidentresponsplan van Datacadabra besproken, een belangrijk onderdeel om te voldoen aan de ISO 27001-normen. Het adequaat reageren op en beheren van incidenten is cruciaal voor het beschermen van informatie en het behouden van vertrouwen van klanten. Dit nog te implementeren proces wordt inzichtelijk gemaakt met een BPMN-visualisatie, waarbij duidelijk wordt hoe klanten, de directie en de supportafdeling samenwerken. We lichten stap voor stap toe, vanaf het moment dat een klant een incident meldt tot de oplossing ervan. Het hoofddoel is om te laten zien hoe Datacadabra van plan is om incidenten efficiënt te beheren, analyseren en oplossen. Dit alles

benadrukt de noodzaak van een goede samenwerking binnen het bedrijf, snelle actie en focus op de klant. Dit proces is een essentieel onderdeel van Datacadabra's strategie voor informatiebeveiliging.



Figuur 7: SupportBPMN

Voorgestelde Implementatie van Incident Respons Proces voor Datacadabra (BPMN Beschrijving)

Deze BPMN-beschrijving illustreert een voorgesteld incidentresponsproces voor Datacadabra, dat nog geïmplementeerd moet worden. Dit proces is ontworpen om te voldoen aan de vereisten van ISO 27001 en benadrukt een systematische aanpak voor het

omgaan met incidenten binnen de organisatie. Het proces omvat drie hoofdlagen: Klant, Managing Director, en Support.

1. **Klantlaag:**
- **Incidentmelding:** Klanten van Datacadabra melden incidenten via een vastgesteld kanaal. Deze meldingen zijn de startpunten voor het responsproces.
2. **Managing Director Laag:**
- **Evaluatie Incident:** De Managing Director van Datacadabra beoordeelt de incidentmelding. Er wordt gekeken of het een bekend of een nieuw incident is.
- **Bekende Incidenten:** Voor bekende incidenten met bestaande oplossingen worden deze oplossingen direct gecommuniceerd naar de klant.
- **Onbekende Incidenten:** Nieuwe of onbekende incidenten worden doorgegeven aan de Support-afdeling voor verdere analyse.
3. **Support Laag:**
- **Eerste Lijn Support:** Deze laag hanteert een eerste beoordeling van het incident. Bij bekende problemen wordt direct een oplossing aangedragen.
- **Tweede Lijn Support:** Complexe of onbekende incidenten worden geëscaleerd naar een meer gespecialiseerd supportteam voor diepgaande analyse.
- **Development Team:** Voor technische oplossingen wordt het probleem doorgestuurd naar het Development Team van Datacadabra
- **Ontwikkeling en Evaluatie:** Hier worden oplossingen ontwikkeld, geëvalueerd en getest.
- **Implementatie:** Na succesvolle tests wordt de oplossing geïmplementeerd.
- **Communicatie naar Klant:** De oplossing of statusupdate wordt gecommuniceerd naar de klant, waarmee het proces wordt afgerond.

Dit voorgestelde proces biedt een duidelijke en gestructureerde methode voor Datacadabra om incidenten te beheren en te reageren in overeenstemming met ISO 27001-normen. De implementatie van dit proces zal de efficiëntie verbeteren, de doorlooptijd van incidenten verkorten en zorgen voor een hogere klanttevredenheid. Het benadrukt ook het belang van interne communicatie en samenwerking tussen verschillende afdelingen binnen de organisatie.

10.3. Integratie van IT en beveiliging in bedrijfsprocessen

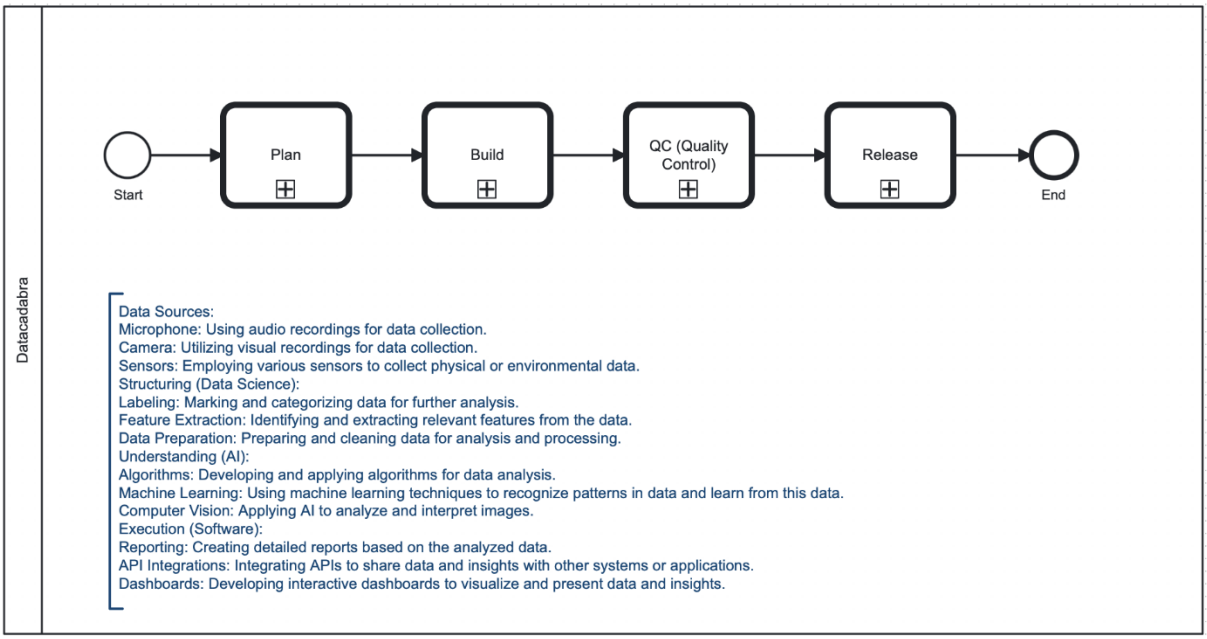
Hieronder staan de bedrijfsprocessen van Datacadabra beschreven en visueel in een BPMN weergegeven.

10.3.1. Bedrijfsprocessen

Dit hoofdstuk biedt een overzicht van de kernbedrijfsprocessen bij Datacadabra, een innovatief bedrijf gespecialiseerd in kunstmatige intelligentie (AI) en data-analyse. Deze processen, ontworpen en goedgekeurd door de Chief Technology Officer (CTO), zijn gebaseerd op de gedetailleerde analyse van interne documentatie van Datacadabra. Ze weerspiegelen de integratie van IT en informatiebeveiliging, essentieel voor het leveren van geavanceerde technologische oplossingen.

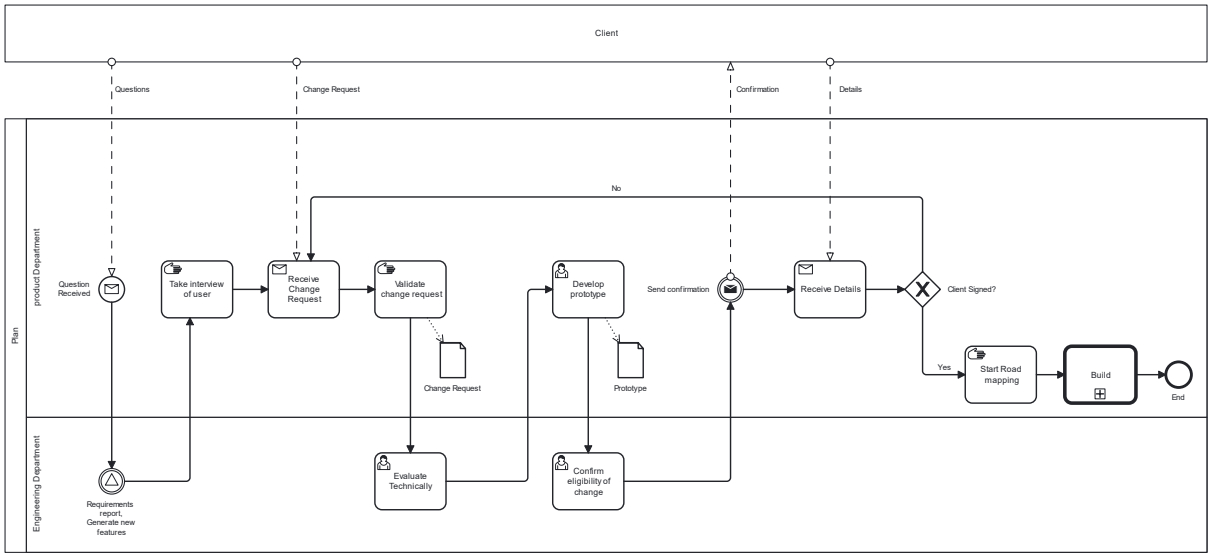
Door de verschillende fasen van planning tot release te verkennen, benadrukt dit hoofdstuk hoe Datacadabra streeft naar het balanceren van innovatie en efficiëntie met de hoogste normen van veiligheid en betrouwbaarheid in hun producten en diensten. Hierbij wordt de nadruk gelegd op de voortdurende aanpassing aan de veranderende technologische eisen en de toekomstige ontwikkelingen binnen het bedrijf.

De bovenstaande afbeelding laat zien hoe de ontwikkeling van een dienst of product eruitziet in grote lijnen. In de onderstaande afbeeldingen wordt elke proces in een BPMN uitgewerkt.

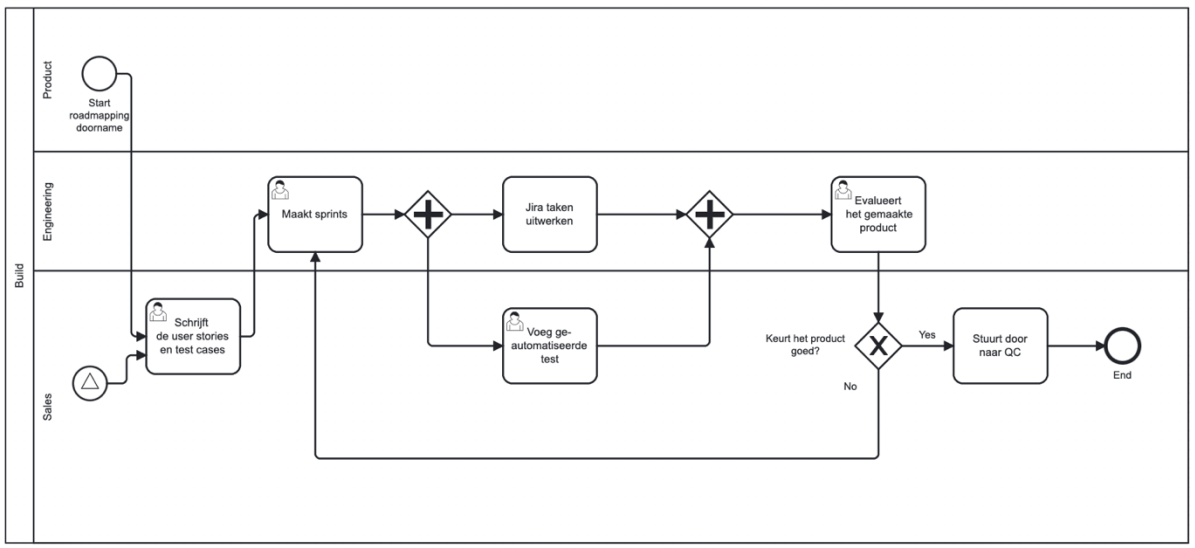


Figuur 8: subprocesses

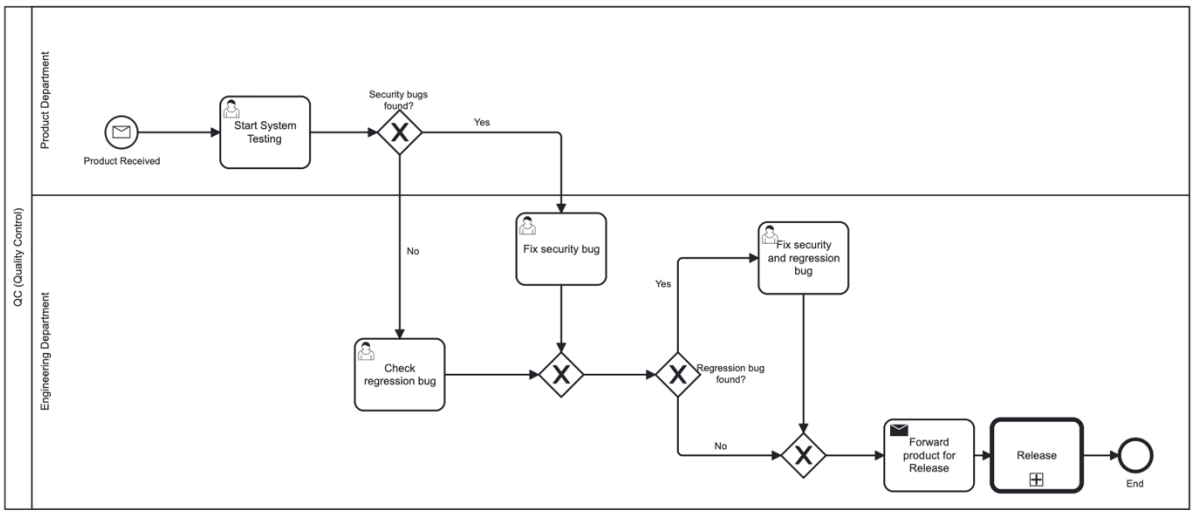
Hieronder zijn de bovenstaande processen uitgebreider uitgewerkt. De beschrijving van de processen in grote lijnen is hieronder gegeven. Deze gedetailleerde fases weerspiegelen het zorgvuldige en systematische proces dat Datacadabra hanteert bij de ontwikkeling en implementatie van hun AI-gedreven softwareproducten en diensten, waarbij kwaliteit en klanttevredenheid vooropstaan.



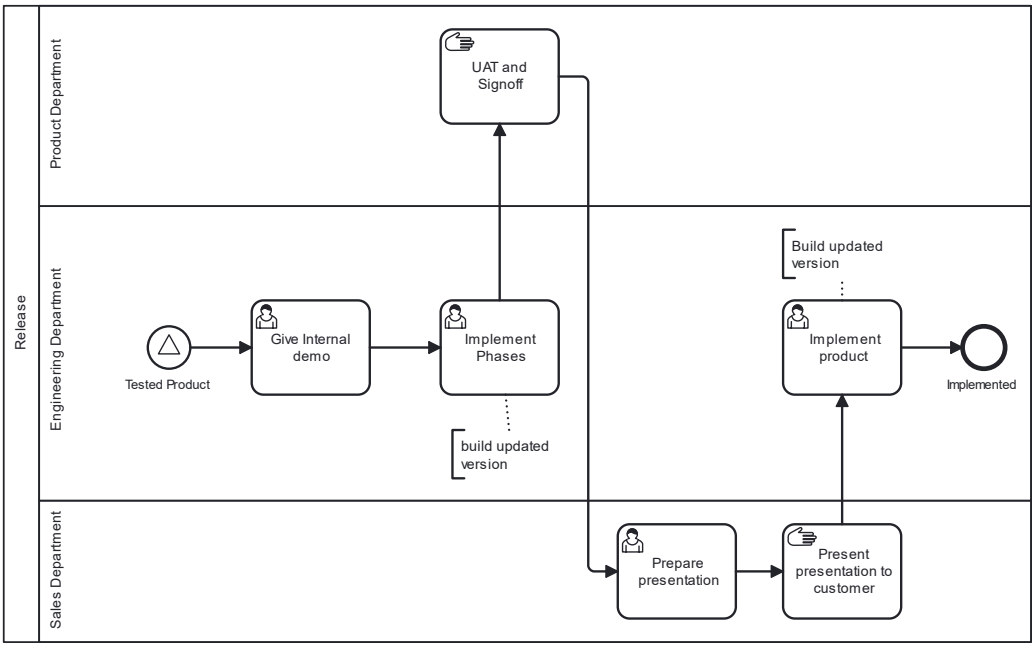
Figuur 9: IT-departement



Figuur 8: build



Figuur 9: Quality control



Figuur10: Release fase

Planfase

Initiatie en Behoefteanalyse:

- **Klantvragen:** Wanneer Datacadabra verzoeken of vragen van klanten ontvangt, initieert dit de planningsfase. Deze verzoeken kunnen gaan over nieuwe functies, verbeteringen of aanpassingen van AI-gebaseerde producten of diensten.
- **Behoefteanalyse:** Een tussentijdse gebeurtenis verzamelt vereisten en nieuwe functieaanvragen. Het productteam voert vervolgens interviews uit om de klantbehoeften grondig te begrijpen.
- **Validatie van Verzoek:** Na ontvangst van een wijzigingsverzoek voert het productteam een initiële validatie uit, waarna het technisch wordt geëvalueerd door het engineeringteam.

Prototyping en Klantbevestiging:

- **Ontwikkeling Prototype:** Het productteam ontwikkelt een voorlopig prototype of concept om de haalbaarheid van de vereisten te demonstreren.
- **Technische Bevestiging:** Het engineeringteam bevestigt de technische uitvoerbaarheid en geschiktheid van de voorgestelde wijzigingen.
- **Klantovereenkomst:** De klant wordt voorzien van gedetailleerde informatie en specificaties. Bij goedkeuring start het productteam met de routekaart en gaat over naar de bouwfase. Bij afwijzing wordt het wijzigingsverzoek herzien.

Bouwfase

Ontwikkeling en Implementatie:

- **Roadmapping en User Stories:** Na goedkeuring van de routekaart, ontwikkelt het verkoopsteam gebruikersverhalen en testgevallen die de basis vormen voor de softwareontwikkeling.
- **Sprint Planning in Jira:** Het engineeringteam plant en organiseert sprints in Jira voor een gestructureerde en gefaseerde ontwikkelingsaanpak.

Parallelle Ontwikkeling en Testen:

- **Automatische Tests en Taakuitvoering:** Terwijl het verkoopsteam automatische tests toevoegt, werkt het engineeringteam parallel aan de ontwikkelingstaken.
- **Foutafhandeling en Bugfixing:** Bij eventuele fouten tijdens het testen worden bugs gegenereerd, die vervolgens door het engineeringteam worden opgelost.

Beoordeling en Kwaliteitscontrole:

- **Productevaluatie:** Het vervaardigde product wordt geëvalueerd door het engineeringteam. Bij goedkeuring wordt het product doorgestuurd naar de kwaliteitscontrole. Bij afkeuring keert het proces terug naar de sprintfase.

Kwaliteitscontrole

Systeemtesten en Bugfixing:

- **Start van Systeemtesten:** Na goedkeuring start het productteam met uitgebreide systeemtesten.
- **Veiligheids- en Functietesten:** Er wordt gecontroleerd op veiligheidsbugs en andere functionele tekortkomingen. Bij bugs wordt de engineeringafdeling ingeschakeld voor reparatie.

Regression Testing en Finalisatie:

- **Regression Testing:** Na het oplossen van alle bugs, voert het engineeringteam regressietesten uit om de algehele stabiliteit en functionaliteit te waarborgen.
- **Product doorsturen voor Release:** Zodra geen verdere bugs worden gevonden, wordt het product klaargemaakt voor de releasefase.

Releasefase

Demonstratie en Implementatie:

- **Interne Demo en Faseimplementatie:** Het engineeringteam organiseert een interne demonstratie van het geteste product en begint met de implementatiefasen.
- **UAT en Sign-Off:** Het productteam voert User Acceptance Testing (UAT) uit en geeft een formele goedkeuring voor release.

Presentatie en Klantlevering:

- **Voorbereiding Presentatie:** Het verkoopsteam bereidt een gedetailleerde presentatie voor om het product aan de klant te demonstreren.
- **Klantlevering:** Na een succesvolle presentatie en goedkeuring van de klant, zorgt het engineeringteam voor de uiteindelijke levering en implementatie van het product bij de klant.

Hieronder wordt het proces van een sale (klant) afhandeling geschetst.
Dit procesmodel illustreert de stappen die Datacadabra neemt vanaf het eerste klantcontact tot aan de aflevering van de dienst of het product, inclusief offertevoorbereiding, goedkeuring, plannen, facturering en het onderhouden van klantrelaties. Het laat zien hoe verschillende afdelingen en systemen samenwerken om een efficiënte en klantgerichte service te bieden.

De beschrijving is hieronder:
Pool: Klant

1. **Start van het Proces**: Het proces begint wanneer de klant contact opneemt met de verkoopafdeling van Datacadabra.

Pool: Datacadabra

Lane: Sales Department

- **Voorbereiden Quotatie in Offri (Sales Opportunity)**: De salesafdeling bereidt een quotatie voor in Offri op basis van de behoeften en eisen van de klant. Deze informatie wordt vastgelegd in het CRM-systeem.

Lane: CRM System

- **Melding met Approval**: Het CRM-systeem genereert een melding die een goedkeuringsverzoek naar de managing director stuurt.

Lane: Managing Director

- **Plannen Maken voor de Opdracht**: Na goedkeuring van de offerte stelt de managing director een plan op voor de uitvoering van de opdracht.
- **Overview Sturen van het Werk**: De managing director stuurt een overzicht van het geplande werk naar de officemanager voor verdere actie.

Lane: Office Manager

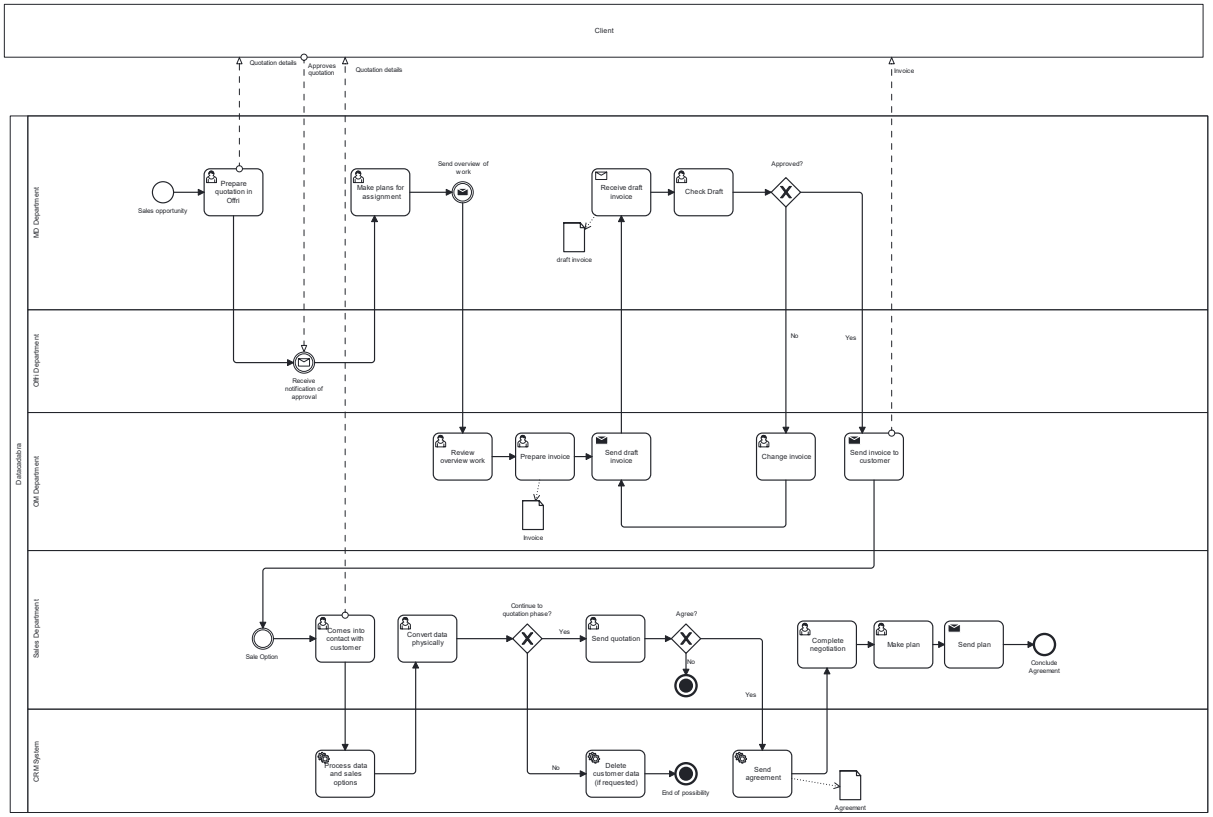
- **Werk Reviewen en Invoice Voorbereiden**: De officemanager reviewt het werk en bereidt de factuur (invoice) voor.
- **Draft Sturen**: De draft van de factuur wordt ter goedkeuring naar de managing director gestuurd.

Lane: Managing Director

- **Draft Controleren en Goedkeuren/Niet Goedkeuren**: De managing director controleert de draft en keurt deze goed of stuurt deze voor aanpassingen terug naar de officemanager.
    - Bij **goedkeuring** wordt de definitieve factuur naar de klant verzonden.
    - Bij **niet goedkeuring** gaat het document terug naar de officemanager voor aanpassing.

Lane: Sales Department

- **Contact met Klant**: De salesafdeling onderhoudt gedurende het gehele proces contact met de klant om eventuele vragen te beantwoorden en updates te verstrekken.
- **CRM Data Aanpassen**: Gebaseerd op de uitkomsten van de offerte en het klantcontact worden de gegevens in het CRM-systeem bijgewerkt.
    - **Voorstel Goed**: Indien het voorstel wordt geaccepteerd, wordt de klantgegevens bijgewerkt en het proces voortgezet.
    - **Voorstel Niet Goed**: Als het voorstel wordt afgewezen, wordt de klant uit het actieve verkoopproces verwijderd en wordt hun data uit de actieve sales pipeline verwijderd.



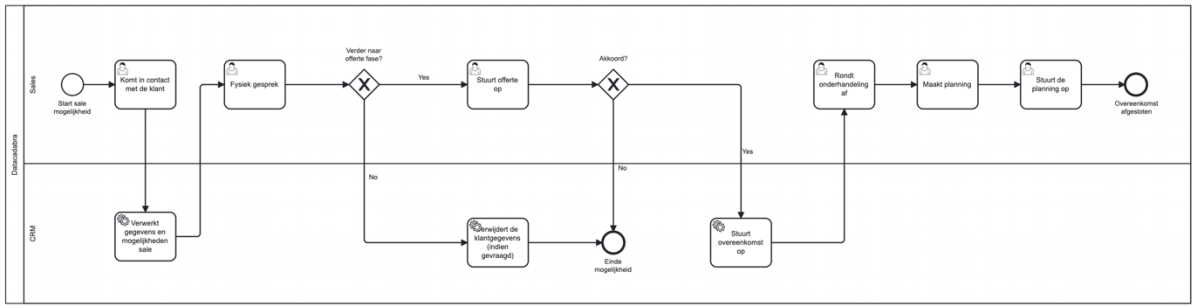
Figuur 3: Datacadabra business processes

De BPMN-schets voor het verkoopproces bij Datacadabra maakt gebruik van hun CRM-softwarepakket om de interacties met klanten efficiënt te beheren. Het proces begint wanneer een potentiële klant wordt geïdentificeerd of benaderd. Als er een verkoopkans wordt vastgesteld, worden de klantgegevens in het CRM-systeem ingevoerd. Vervolgens voert een verkoper van Datacadabra een persoonlijk gesprek met de klant om de behoeften en mogelijkheden te bespreken.

Als het voorstel positief wordt ontvangen, wordt er een offerte naar de klant gestuurd. Als de klant echter niet geïnteresseerd lijkt, wordt de verkoopkans beëindigd en de relevante informatie uit het CRM-systeem verwijderd.

Bij een akkoord op de offerte, verloopt het proces verder naar het opstellen van een overeenkomst, het maken van een planning en het afronden van de onderhandelingen. Als de offerte echter niet wordt geaccepteerd, eindigt het verkoopproces en worden de gegevens van deze specifieke kans uit het CRM-systeem verwijderd.

Dit BPMN-proces toont de gestructureerde stappen die Datacadabra volgt in hun verkoopcyclus, van de eerste interactie met de klant tot het afronden van de verkoop of het beëindigen van de verkoopkans, met een sterke nadruk op gegevensbeheer binnen hun CRM-systeem.



Figuur 13: CRM

10.4. GAP-Analyse

De onderstaande analyse van Datacadabra's informatiebeveiliging is het resultaat van grondige gesprekken met twee stakeholders binnen de organisatie: de Chief Technology Officer (CTO) en de Managing Director (MD). Deze interviews hebben inzicht gegeven in diverse aspecten van de organisatie's huidige informatiebeveiligingsstrategie, de effectiviteit ervan, en gebieden die verbetering behoeven. Het rapport richt zich op het evalueren van het bestaande beveiligingsbeleid, de infrastructuur, naleving van wettelijke normen, en procedures voor incidentbeheer. Deze uitkomsten bieden een basis voor het formuleren van een strategisch actieplan ter versterking van Datacadabra's beveiligingspostuur in het digitale landschap.

Analyse van de Huidige Staat van Informatiebeveiliging bij Datacadabra

1. Beoordelen van het Huidige Beleid
   - **Bestaand Beleid**: Datacadabra heeft een basisinformatiebeveiligingsbeleid ontwikkeld.
   - **Naleving**: Dit beleid wordt echter niet consequent toegepast of gehandhaafd in de praktijk. Dit kan leiden tot inconsistente beveiligingspraktijken en verhoogde kwetsbaarheden.
2. Evaluatie van Beveiligingsinfrastructuur
   - **Beveiligingstools en -protocollen**: Datacadabra gebruikt basisbeveiligingstools zoals firewalls en antivirusprogramma's.
   - **Effectiviteit**: Deze tools zijn mogelijk niet optimaal geconfigureerd of geüpdatet, wat het risico op beveiligingsinbreuken kan verhogen. Het gebruik van versleutelingstechnieken is mogelijk niet uitgebreid of geavanceerd.
3. Compliance Check
   - **GDPR Naleving**: Er is een minimale inspanning om te voldoen aan de GDPR, voornamelijk gericht op werknemersgegevens.
   - **Algemene Compliance**: De algemene naleving van relevante wetgeving en normen zoals ISO 27001 is laagdrempelig, wat wijst op een potentieel gebrek aan bewustzijn of middelen voor grondige compliance.
4. Incidentbeheer

- **Procedures**: Er zijn geen gestructureerde of gedocumenteerde procedures voor het omgaan met beveiligingsincidenten.
- **Respons**: Dit gebrek aan procedures kan leiden tot trage of ineffectieve respons op incidenten, wat de impact van beveiligingsinbreuken kan vergroten.

Definiëren van de Gewenste Staat van Informatiebeveiliging bij Datacadabra BV
Voor Datacadabra, kunnen we de gewenste staat van informatiebeveiliging definiëren aan de hand van verschillende essentiële aspecten. Deze omvatten het hebben van een geoptimaliseerd beveiligingsbeleid, een geavanceerde beveiligingsinfrastructuur, volledige compliance met relevante wetgeving en regelgeving, en een robuust systeem voor incidentbeheer.

1. Geoptimaliseerd Beveiligingsbeleid
    - **Ontwikkeling**: Het ontwikkelen van een uitgebreid informatiebeveiligingsbeleid dat voldoet aan internationale normen, zoals ISO 27001 en de best practices in de industrie.
    - **Handhaving**: Actieve handhaving van dit beleid binnen alle niveaus van de organisatie, inclusief regelmatige trainingen en bewustwordingscampagnes voor medewerkers.
2. Geavanceerde Beveiligingsinfrastructuur
    - **Up-to-Date Technologie**: Implementatie van de nieuwste beveiligingstechnologieën, zoals geavanceerde firewalls, intrusion detection systems (IDS), en geavanceerde versleutelingstechnieken.
    - **Regelmatige Updates**: Zorgen voor regelmatige updates en onderhoud van de beveiligingsinfrastructuur om op de hoogte te blijven van de nieuwste beveiligingsdreigingen en kwetsbaarheden.
3. Volledige Compliance
    - **GDPR en Andere Reguleringen**: Volledige naleving van de GDPR en andere relevante wetgeving, met een specifieke focus op de bescherming van persoonsgegevens en dataprivacy.
    - **Audits en Reviews**: Regelmatige audits en compliance reviews om te garanderen dat het bedrijf consistent voldoet aan alle vereisten.
4. Robuust Incidentbeheer
    - **Duidelijk Gedefinieerde Procedures**: Ontwikkeling van duidelijk gedefinieerde en gedocumenteerde procedures voor incidentbeheer, inclusief responsplannen voor verschillende soorten beveiligingsincidenten.
    - **Training en Oefeningen**: Regelmatige trainingen en oefeningen voor het personeel om te zorgen voor een snelle en effectieve respons in geval van beveiligingsincidenten.

Identificatie van Specifieke Verbeteringsgebieden
Voor Datacadabra, kan je specifieke verbeteringsgebieden op het gebied van informatiebeveiliging identificeren. Deze verbeteringen zijn gericht op het aanpakken van de huidige tekortkomingen en het versterken van het algehele beveiligingspostuur van het bedrijf.

1. Beleidsverbetering en Handhaving
    - **Herziening van het Beleid**: Het huidige informatiebeveiligingsbeleid moet worden herzien en versterkt om te voldoen aan de laatste standaarden en best practices.
    - **Handhavingsmechanismen**: Implementatie van duidelijke handhavingsmechanismen, zoals regelmatige controles en sancties voor niet-naleving.
2. Upgrade van Beveiligingstools
    - **Investering in Geavanceerde Technologie**: Investering in geavanceerde beveiligingstechnologieën zoals geavanceerde firewalls, intrusion prevention systems (IPS), en endpoint protection oplossingen.
    - **Regelmatige Evaluatie en Update**: Zorgen dat alle beveiligingstools regelmatig worden geëvalueerd en geüpdatet om de nieuwste bedreigingen aan te kunnen.
3. Training en Bewustzijn
    - **Ontwikkeling van Trainingsprogramma's**: Het ontwikkelen van uitgebreide trainingsprogramma's voor alle medewerkers om hun kennis over informatiebeveiliging te vergroten.
    - **Regelmatige Bewustwordingssessies**: Organiseren van regelmatige bewustwordingssessies over de nieuwste beveiligingsdreigingen en beste praktijken.
4. Compliance Monitoring
    - **Implementatie van Compliance Checks**: Regelmatige interne en externe audits om de naleving van relevante wet- en regelgeving te waarborgen.
    - **Feedback en Verbeteringsprocessen**: Implementatie van processen voor het verzamelen van feedback en het continu verbeteren van compliance-praktijken.
5. Ontwikkeling van Incidentbeheerprotocollen
    - **Opstellen van Protocollen**: Het ontwikkelen van gedetailleerde incidentbeheerprotocollen voor verschillende soorten beveiligingsincidenten.
    - **Training en Oefeningen**: Regelmatig trainen van het personeel in deze protocollen en het organiseren van oefeningen om de paraatheid te verhogen.

Actieplan voor Verbetering
Voor Datacadabra, een bedrijf dat zich in een fase van intensieve groei en ontwikkeling bevindt, is het essentieel om een effectief actieplan voor de verbetering van hun informatiebeveiliging op te stellen. Hieronder volgt een gedetailleerd plan om de geïdentificeerde verbeteringen door te voeren, prioriteiten te stellen en de implementatie en voortgang te monitoren.

1. Actieplan Opstellen
    - **Ontwikkelen van het Plan**: Creëer een uitgebreid actieplan met specifieke taken, verantwoordelijkheden, deadlines en benodigde middelen voor elke geïdentificeerde verbetering.
    - **Betrokkenheid van Teams**: Zorg voor betrokkenheid van relevante teams en afdelingen, zoals IT, HR, en management, om een integrale aanpak te waarborgen.
2. Prioriteiten Stellen

- **Kritieke Verbeteringen Identificeren**: Identificeer welke verbeteringen het meest kritisch zijn voor de organisatie. Dit kan bijvoorbeeld het updaten van de beveiligingsinfrastructuur of het ontwikkelen van incidentbeheerprotocollen zijn.
- **Tijdlijn Opstellen**: Stel een realistische tijdlijn op voor de implementatie, waarbij de meest urgente acties voorrang krijgen.

3. Implementatie en Monitoring
   - **Fasegewijze Implementatie**: Voer de verbeteringen gefaseerd uit, beginnend met de meest kritieke. Dit zorgt voor beheersbaarheid en minimaliseert verstoring van de bedrijfsvoering.
   - **Voortgangsmonitoring**: Stel regelmatige check-ins en beoordelingen in om de voortgang te monitoren. Dit kan wekelijks of maandelijks zijn, afhankelijk van de aard van de verbetering.
   - **Feedback Loop**: Implementeer een feedbackmechanisme om voortdurende input van betrokkenen te verzamelen en aanpassingen te maken waar nodig.

10.4.1. Samengevat GAP-analyse

De huidige staat van informatiebeveiliging bij Datacadabra toont significante ruimte voor verbetering. Het is van essentieel belang dat het bedrijf werkt aan het versterken en consequent handhaven van hun informatiebeveiligingsbeleid. Dit omvat het up-to-date houden van beveiligingstools, het versterken van hun aanpak van compliance, en het ontwikkelen van gestructureerde procedures voor incidentbeheer.
Een meer proactieve benadering van informatiebeveiliging zal niet alleen de weerbaarheid van Datacadabra tegen cyberaanvallen verbeteren, maar ook hun reputatie en betrouwbaarheid in de markt versterken. Dit is vooral belangrijk voor een bedrijf dat intensief met data werkt en afhankelijk is van cloudopslag en geavanceerde data-analysetools.

De gewenste staat van informatiebeveiliging voor Datacadabra moet gericht zijn op het creëren van een omgeving waarin informatiebeveiliging een integraal onderdeel is van de bedrijfscultuur. Dit omvat het hebben van een robuust en actief gehandhaafd beveiligingsbeleid, geavanceerde en up-to-date beveiligingsinfrastructuur, volledige naleving van relevante wet- en regelgeving, en effectief incidentbeheer. Door deze aspecten aan te pakken, kan Datacadabra niet alleen hun huidige beveiligingsniveau verhogen, maar ook een solide basis leggen voor toekomstige groei en ontwikkeling in een steeds meer datagedreven wereld.

Door deze specifieke verbeteringsgebieden aan te pakken, kan Datacadabra hun informatiebeveiliging aanzienlijk verbeteren. Dit omvat het versterken van hun beleid, het upgraden van hun beveiligingstools, het verhogen van het bewustzijn en de kennis van medewerkers, het waarborgen van compliance, en het ontwikkelen van effectieve incidentbeheerprotocollen. Deze stappen zullen bijdragen aan een veiligere en meer veerkrachtige organisatie.

Een gestructureerd en doordacht actieplan is cruciaal voor Datacadabra om hun informatiebeveiliging effectief te verbeteren. Door prioriteiten te stellen en een gefaseerde aanpak te hanteren, kunnen zij de risico's verlagen en hun beveiligingshouding versterken. Regelmatige monitoring en de mogelijkheid tot aanpassing zorgen ervoor dat het plan

dynamisch en responsief blijft in overeenstemming met de evoluerende behoeften en dreigingen van de organisatie.

10.5. Samenvatting meeting CTO

Samenvatting Meeting: Verbetering Informatiebeveiliging Datacadabra
Datum: 25-10-2023 **Aanwezig:** Rita Simon (afstudeerder), Mark Bulthuis (CTO)
Agendapunten:

1. Huidige Stand van Zaken
2. Analyse van gebreken
3. Voorstel verbeteringen

Samenvatting:

- De huidige informatiebeveiliging van Datacadabra, gehaald uit de gesprekken met de CTO en MD, vertoont tekortkomingen in de informatiebeveiliging. Het beleid wordt inconsistent toegepast en de gebruikte tools zoals firewalls en antivirusprogramma's zijn mogelijk verbogen.
- Er is een minimale acties/inzet en inspanning waargenomen op het gebied van GDPR-hanteren en streven naar en een gebrek aan een gestructureerde aanpak voor incidentbeheer.
- Een voorgesteld actieplan omvat het herzien van het informatiebeveiligingsbeleid, het ontwikkelen van geavanceerde beveiligingsinfrastructuur, het waarborgen van volledige compliance, en het opzetten van een sterk incidentbeheersysteem. Dit omvat investeringen in technologie, het ontwikkelen van trainingsprogramma's, regelmatige audits, en het opstellen van incidentbeheerprotocollen.
- De implementatie van deze verbeteringen vereist een gedetailleerd actieplan, betrokkenheid van relevante teams, prioritering van kritieke verbeteringen, gefaseerde implementatie, voortgangsmonitoring en een feedbackloop.

Actiepunten:

1. Vernieuwing van het beleid en ontwikkeling van een goed passend beleid.
2. Investering in nieuwe technologieën die kunnen bijdragen aan beveiliging.
3. Ontwikkeling van trainingsprogramma's voor personeel.
4. Opstellen van regelmatige audits en incidentbeheerprotocollen.
5. Opzetten van een duidelijke implementatie- en feedbackstructuur.

Volgende Stappen:

- Uitwerken van een gedetailleerd actieplan.
- Plannen van vervolgmeetings voor voortgangscontrole en afstemming.

Afsluiting: De meeting benadrukte het belang van het verbeteren van de informatiebeveiliging binnen Datacadabra en legde de basis voor de noodzakelijke stappen voorwaarts. Er is overeenstemming bereikt over de urgentie en de noodzaak van actie, met een duidelijke focus op praktische incosistentie en continue verbetering.

10.6. Vergadering met Gert-Jan

Verslag van het Gesprek met Managing Director op 13 november 2023

Op 13 november 2023 vond een cruciaal gesprek plaats tussen Rita Simon en de Managing Director (MD) van Datacadabra, Gert-Jan. Het doel van dit gesprek was om de kwestie van informatiebeveiliging en het ontbreken van een erkend certificaat binnen de organisatie te bespreken en de impact ervan op het bedrijf te evalueren.

Het gesprek begon met een overzicht van de recente gebeurtenissen en incidenten met betrekking tot informatiebeveiliging, waaronder datalekken en phishingaanvallen. Deze incidenten benadrukten de urgentie van het probleem en leidden tot klantenverlies Gert-Jan erkende dat deze kwesties een serieuze bedreiging vormden voor de reputatie en groei van Datacadabra.

Gert-Jan benadrukte het belang van het verbeteren van informatiebeveiliging en het verkrijgen van een erkend certificaat om het vertrouwen van klanten en potentiële klanten te herstellen. Het gesprek wees op de noodzaak om snel actie te ondernemen om de risico's te verminderen en de positie van Datacadabra op de markt te versterken.

Het gesprek eindigde met een consensus dat het cruciaal was om onmiddellijk stappen te ondernemen om informatiebeveiliging te verbeteren en het certificeringsproces op te starten. Er werd afgesproken dat Gert-Jan en Rita Simon nauw zouden samenwerken om dit proces te leiden en ervoor te zorgen dat Datacadabra haar reputatie en klantenbestand kon behouden en uitbreiden.

Dit verslag dient als documentatie van het gesprek en zal dienen als leidraad voor toekomstige acties om informatiebeveiliging binnen Datacadabra te versterken.

13-11-2023

10.7. Huidige situatieanalyse

Overzicht van huidige IT-en beveiligingsinfrastructuur

Als onderdeel van een uitgebreide evaluatie van de IT-infrastructuur en -strategie van Datacadabra, heb ik zowel documentanalyse als interviews gebruikt om een gedetailleerd beeld te krijgen van de technologische omgeving binnen het bedrijf. Door het zorgvuldig doornemen van interne documenten, zoals netwerkschema's, software-inventarislijsten en beveiligingsprotocollen, kon ik een technisch en gedetailleerd inzicht krijgen in de hardware, software en cyberbeveiligingsmaatregelen van het bedrijf.

Aanvullend hierop heb ik diepte-interviews gevoerd met de stakeholders binnen de organisatie, waaronder IT-managers, netwerkbeheerders en softwareontwikkelaars. Deze gesprekken boden waardevolle inzichten in hoe de technologische hulpmiddelen en systemen concreet bijdragen aan de bedrijfsprocessen en -efficiëntie. Het combineren van deze twee onderzoeksmethoden - documentanalyse en interviews - stelde me in staat om een holistisch en genuanceerd beeld te vormen van de IT-infrastructuur bij Datacadabra

10.7.1. Overzicht van de huidige IT en beveiligingsinfrastructuur

1. IT-Infrastructuur:
   - **Hardware en Netwerken:** Uitleg van de huidige hardware, waaronder servers, werkstations en netwerkapparatuur. Details over de netwerkstructuur, zoals WAN/LAN-configuraties, en het gebruik van cloudservices.
   - **Software en Applicaties:** Beschrijving van bedrijfsspecifieke applicaties, operationele software, en kantoorautomatiseringstools. Focus op hoe deze tools bijdragen aan de bedrijfsprocessen en -efficiëntie.
   - **Cyberbeveiliging:** Overzicht van de huidige beveiligingsmaatregelen, waaronder firewalls, antivirusprogramma's, inbraakdetectiesystemen en versleutelingstechnieken.

2. Beveiligingsbeleid en -procedures:
   - **Beleidsdocumenten:** Inventarisatie van bestaande beleidsrichtlijnen en protocollen die de informatiebeveiliging sturen.
   - **Compliance en Standaarden:** Status van de naleving van relevante normen (zoals ISO 27001) en wettelijke vereisten (zoals GDPR).
   - **Incidentbeheer:** Beschrijving van de huidige procedures voor het beheren van beveiligingsincidenten en de respons op cyberaanvallen.

Samenvatting van bestaande bedrijfsprocessen en hun relatie met IT

1. Kernbedrijfsprocessen:
   - **Productontwikkeling:** Hoe IT wordt ingezet in de ontwikkeling van nieuwe producten of diensten, met inbegrip van softwareontwikkeling en data-analyse.
   - **Klantenservice en Support:** De rol van IT in klantenondersteuning, klantrelatiebeheer en communicatiekanalen.
   - **Operaties en Logistiek:** Beschrijving van hoe IT-systemen worden gebruikt in de dagelijkse bedrijfsvoering, inclusief voorraadbeheer, orderverwerking en logistiek.

2. IT-afhankelijkheid:
   - **Automatisering:** Hoe IT bijdraagt aan de automatisering van bedrijfsprocessen, efficiëntieverhoging en kostenbesparing.

- **Gegevensbeheer:** Het gebruik van IT in het verzamelen, opslaan en analyseren van bedrijfsgegevens, en hoe dit bijdraagt aan besluitvorming en strategieontwikkeling.
- **Communicatie en Samenwerking:** De rol van IT in interne en externe communicatie, samenwerkingstools en het delen van informatie.

3. Risico's en Kwetsbaarheden:

- **Beveiligingsrisico's:** Identificatie van mogelijke beveiligingsrisico's die voortvloeien uit de huidige IT-infrastructuur en bedrijfsprocessen.
- **Afhankelijkheid van Technologie:** Beoordeling van de risico's die samenhangen met de afhankelijkheid van technologie, zoals systeemuitval, datalekken en cyberaanvallen.

10.7.2. Beleid en procedures

Na uitgebreid onderzoek binnen de organisatie van Datacadabra, waarbij diverse bronnen en afdelingen zijn geraadpleegd, heb ik de volgende bevindingen over hun beveiligingsbeleid en -procedures kunnen samenstellen:

1. **Beleidsdocumenten**
    - Datacadabra heeft een formeel informatiebeveiligingsbeleid opgesteld, maar uit mijn onderzoek blijkt dat dit beleid niet actief wordt gehandhaafd. Dit leidt tot inconsistenties in de manier waarop informatiebeveiliging in de praktijk wordt gebracht.
2. **Compliance en Standaarden**
    - **ISO 27001**: Er is geen duidelijk bewijs dat Datacadabra actief streeft naar naleving van ISO 27001, wat wijst op een mogelijk gebrek aan een gestructureerde aanpak van informatiebeveiliging.
    - **GDPR**: Mijn onderzoek toont aan dat er binnen Datacadabra aanzienlijke inspanningen worden geleverd om te voldoen aan de AVG/GDPR voor de persoonlijke gegevens van de werknemers. Echter, voor de gegevens die het bedrijf verzamelt en verwerkt via hun Google Cloud-diensten, lijkt er minder nadruk te liggen op AVG-compliance. Dit kan een risico vormen gezien de vereisten en potentiële sancties van de GDPR.
3. **Incidentbeheer**
    - Er zijn geen specifieke protocollen of procedures voor incidentbeheer vastgesteld binnen Datacadabra Dit is zorgwekkend, aangezien in het geval van een beveiligingsincident, het bedrijf mogelijk niet adequaat is voorbereid om effectief te reageren.

Mijn bevindingen suggereren dat hoewel Datacadabra enige inspanningen heeft geleverd om te voldoen aan de AVG voor hun werknemers, er aanzienlijke ruimte voor verbetering is in de algehele benadering van informatiebeveiliging. De organisatie zou baat hebben bij een meer gestructureerde benadering van hun informatiebeveiligingsbeleid en een versterking van hun incidentbeheerprocedures. Dit zou niet alleen de beveiliging van hun systemen en data verbeteren, maar ook helpen om aan de complexe eisen van moderne dataregelgeving te voldoen.

10.7.3. Kern bedrijfsprocessen

De integratie van IT in deze kernbedrijfsprocessen stelt Datacadabra in staat om efficiënter en effectiever te opereren, de klanttevredenheid te verbeteren en een concurrentievoordeel te behalen in hun markt

1. **Productontwikkeling**

- **Softwareontwikkeling**: IT speelt een cruciale rol in de ontwikkeling van softwareproducten bij Datacadabra Dit omvat het gebruik van geavanceerde ontwikkelingstools, programmeertalen, en platforms voor versiebeheer. Agile methodologieën worden vaak toegepast om flexibiliteit en efficiëntie in het ontwikkelingsproces te waarborgen.
- **Data-analyse**: Data-analyse is een sleutelelement in de productontwikkeling, waarbij gebruik wordt gemaakt van big data-technologieën en analytische tools. Deze analyses helpen bij het identificeren van markttrends, klantvoorkeuren en potentiële verbeterpunten voor producten.

2. **Klantenservice en Support**

- **Klantenondersteuning**: IT maakt het mogelijk om efficiënte en effectieve klantenservice te bieden. Dit omvat het gebruik van CRM-systemen (Customer Relationship Management) om interacties met klanten te beheren en te analyseren, wat leidt tot betere klantrelaties en -tevredenheid.
- **Communicatiekanalen**: Datacadabra gebruikt diverse IT-gestuurde communicatiekanalen, zoals e-mail, sociale media, live chat en helpdesksystemen, om klantenondersteuning te bieden. Deze systemen zorgen voor een snelle en consistente respons op klantvragen.

3. **Operaties**

- **Voorraadbeheer**: IT-systemen worden ingezet voor nauwkeurig voorraadbeheer, wat essentieel is voor het beheersen van kosten en het waarborgen van productbeschikbaarheid. Geautomatiseerde systemen helpen bij het bijhouden van voorraadniveaus en het voorspellen van toekomstige voorraadbehoeften.
- **Orderverwerking**: IT stelt Datacadabra in staat om orders efficiënt te verwerken, van ontvangst tot levering. Systemen voor orderbeheer integreren met voorraadbeheer en klantgegevens om een soepele doorstroom van bestellingen te garanderen.

10.7.4. IT-Afhankelijkheid

Automatisering:

1. **Data-Analyse en Verwerking**: Datacadabra maakt intensief gebruik van Python voor data-analyse en verwerking. Dit helpt bij het efficiënt verwerken van grote datasets en het verkrijgen van inzichten die van cruciaal belang zijn voor hun bedrijfsstrategie.
2. **Beperkte Automatisering**: Als start-up heeft Datacadabra nog niet de capaciteit om geavanceerde automatiseringstools zoals chatbots te implementeren. De focus ligt op het gebruik van bestaande tools en technologieën die kosteneffectief en schaalbaar zijn.
3. **Efficiëntie in Werkprocessen**: Hoewel uitgebreide automatisering beperkt is, streeft Datacadabra ernaar om hun werkprocessen te stroomlijnen met behulp van beschikbare IT-middelen, waardoor ze een efficiëntere workflow kunnen handhaven.

Gegevensbeheer:

1. **Gegevensopslag in Google Cloud**: Alle bedrijfsgegevens worden opgeslagen in Google Cloud, wat zorgt voor veilige en schaalbare opslagoplossingen. Dit stelt hen in staat om grote hoeveelheden data effectief te beheren.
2. **Data-analyse voor Besluitvorming**: Met behulp van Python en andere data-analysetools, analyseert Datacadabra hun gegevens voor strategische besluitvorming. Dit helpt hen om beter geïnformeerde beslissingen te nemen die gebaseerd zijn op concrete gegevensinzichten.
3. **Focus op Data-Intensieve Strategieën**: Als een data-gedreven start-up, richt Datacadabra zich op het verzamelen en analyseren van relevante gegevens om hun producten en diensten te verbeteren.

Communicatie en Samenwerking:

1. **Interne Communicatie**: Voor interne communicatie vertrouwt Datacadabra op eenvoudige maar effectieve tools zoals e-mail en standaard samenwerkingssoftware.
2. **Beperkte Externe Communicatiehulpmiddelen**: Wegens beperkte middelen en een focus op kernactiviteiten, gebruikt Datacadabra basis communicatiehulpmiddelen voor externe communicatie, zoals e-mail en traditionele sociale media.
3. **Samenwerking via Cloud-Based Tools**: Ze maken gebruik van cloud-gebaseerde samenwerkingstools voor projectmanagement en het delen van documenten, wat essentieel is voor het ondersteunen van hun flexibele en dynamische werkomgeving.

10.8. Upgrade van beveiligingstechnologie en -infrastructuur

Upgrade van beveiligingstechnologie en -infrastructuur

Datacadabra's huidige inzet van Google Cloud voor dataopslag en Python voor data-analyse en -verwerking vormt een solide basis voor hun IT-operaties. Deze focus is het resultaat van uitgebreide meetings, interviews en een grondige analyse van de beschikbare documentatie binnen de organisatie. De effectieve integratie van deze technologieën biedt het potentieel voor toekomstige uitbreidingen in verschillende gebieden zoals softwareontwikkeling, klantenservice en operationele processen. Toekomstige implementaties kunnen Agile methodologieën, CRM-systemen, geavanceerde communicatiekanalen en geautomatiseerde systemen voor voorraad- en orderbeheer omvatten. Deze geplande uitbreidingen zullen Datacadabra in staat stellen om efficiënter te opereren en een concurrentievoordeel te behalen in hun markt, gedreven door inzichten verkregen uit interne bronnen.

De aanbevolen technologieën voor Datacadabra zijn gekozen op basis van hun vermogen om specifieke aspecten van informatiebeveiliging aan te pakken. Hieronder licht ik de keuzes toe, met verwijzingen naar relevante best practices:

1. **KnowBe4 voor Cybersecurity Training:**
    - **Reden voor Keuze:** KnowBe4 wordt erkend voor zijn uitgebreide aanpak van cybersecuritytraining en bewustwording, wat cruciaal is voor het voorkomen van menselijke fouten in informatiebeveiliging.
    - **Bronvermelding Best Practices:** KnowBe4 staat bekend om zijn effectieve trainingen en is erkend in diverse onderzoeken en artikelen over cybersecurity bewustwording.
2. **Google Cloud Platform voor Veilige Dataopslag:**
    - **Reden voor Keuze:** Het Google Cloud Platform biedt robuuste beveiligingsfuncties en is in staat om te voldoen aan diverse internationale normen, waaronder ISO 27001 en AVG/GDPR.

- **Bronvermelding Best Practices:** Verschillende casestudies en onderzoeken benadrukken de veiligheidsmaatregelen en compliance-capaciteiten van het Google Cloud Platform.

3. **Veeam Backup voor Robuuste Back-upprotocollen:**
    - **Reden voor Keuze:** Veeam Backup biedt betrouwbare en flexibele back-upoplossingen, wat essentieel is voor dataherstel en bedrijfscontinuïteit.
    - **Bronvermelding Best Practices:** Veeam wordt vaak genoemd in industriële beoordelingen en rapporten als een toonaangevende oplossing voor back-up en disaster recovery.
4. **Mimecast voor E-mailbeveiliging:**
    - **Reden voor Keuze:** Mimecast biedt uitgebreide bescherming tegen e-mailgerelateerde dreigingen, inclusief phishing, wat een veelvoorkomende bron van beveiligingsinbreuken is.
    - **Bronvermelding Best Practices:** Mimecast is vaak aanbevolen in beveiligingsgerelateerde publicaties voor zijn effectieve e-mailbeveiligingsoplossingen.
5. **Microsoft Teams of Slack voor Veilige Interne Communicatie:**
    - **Reden voor Keuze:** Deze platforms bieden veilige en efficiënte interne communicatieopties, wat belangrijk is voor het handhaven van de integriteit van informatie binnen een organisatie.
    - **Bronvermelding Best Practices:** Zowel Microsoft Teams als Slack worden regelmatig genoemd in best practices voor veilige interne communicatie.
6. **OneTrust voor Compliance Management:**
    - **Reden voor Keuze:** OneTrust biedt oplossingen die organisaties helpen bij het beheren van compliance met betrekking tot AVG/GDPR en andere relevante wetgevingen.
    - **Bronvermelding Best Practices:** OneTrust wordt vaak genoemd in compliance-gerelateerde literatuur als een effectief hulpmiddel voor het beheren van privacy en regelgeving.

Deze technologieën zijn geselecteerd op basis van hun reputatie, functionaliteit en de specifieke behoeften van Datacadabra bij het versterken van hun informatiebeveiliging. De implementatie ervan zal helpen bij het opzetten van een robuust en compliant informatiebeveiligingssysteem.

1. **Functionaliteiten**: Technologieën met uitgebreide beveiligingsfuncties, zoals gegevensversleuteling, geavanceerde toegangscontrolesystemen en uitgebreide monitoringcapaciteiten voor incidentdetectie, is nodig voor Datacadabra, een bedrijf die zich enorm inzet voor
2. **Reputatie**: de voorkeur aan producten van leveranciers met een bewezen staat van dienst in betrouwbaarheid en klantondersteuning geven.
3. **Specifieke Behoeften**: De software moet naadloos integreren met Datacadabra's bestaande IT-infrastructuur, flexibel genoeg zijn om mee te groeien met het bedrijf, en voldoen aan hun unieke beveiligingsvereisten.
4. **Best Practices**: Kiezen voor oplossingen die in overeenstemming zijn met industrie standaarden zoals ISO 27001 en AVG/GDPR, en die effectief zijn gebleken in vergelijkbare organisaties.

Deze technologieën zijn geselecteerd op basis van hun reputatie, functionaliteit en de specifieke behoeften van Datacadabra bij het versterken van hun informatiebeveiliging. De implementatie ervan zal helpen bij het opzetten van een robuust en compliant informatiebeveiligingssysteem.

1. **Functionaliteiten**: Technologieën met uitgebreide beveiligingsfuncties, zoals gegevensversleuteling, geavanceerde toegangscontrolesystemen en uitgebreide monitoringcapaciteiten voor incidentdetectie, is nodig voor Datacadabra, een bedrijf die zich enorm inzet voor
2. **Reputatie**: de voorkeur aan producten van leveranciers met een bewezen staat van dienst in betrouwbaarheid en klantondersteuning geven.
3. **Specifieke Behoeften**: De software moet naadloos integreren met Datacadabra's bestaande IT-infrastructuur, flexibel genoeg zijn om mee te groeien met het bedrijf, en voldoen aan hun unieke beveiligingsvereisten.
4. **Best Practices**: Kiezen voor oplossingen die in overeenstemming zijn met industrie standaarden zoals ISO 27001 en AVG/GDPR, en die effectief zijn gebleken in vergelijkbare organisaties.

10.8.1. Case study

1. **KnowBe4**
    - **Case Study**: Een groot financieel bedrijf implementeerde KnowBe4 om het bewustzijn van cyberveiligheid bij de werknemers te stuk te verbeteren. Door de modules voor trainingen te gebruiken, daalde het aantal geslaagde phishing-pogingen.
    - **Bron**: "KnowBe4 Case Studies" op de KnowBe4 website.
2. **Google Cloud Platform**
    - **Case Study**: Een e-commerce bedrijf heeft succesvol operaties opgeschaald door gebruik te maken van de schaalbaarheid en beveiligingsfuncties van Google Cloud, als resultaat was er dus een beter datamanagement terug te zien en tevreden huidige en potentiële klanten.
    - **Bron**: "Google Cloud Platform Success Stories" op de Google Cloud website.
3. **Veeam Backup**
    - **Case Study**: Veeam was een succes implelementatie voor een gezondheidszorgorganisatie, door Veeam werd de dataherstelcapaciteit verbeterd. Dit resulteerde vervolgens in een sneller herstel na dataverlies en betere compliance in de gezondheidszorgnormen.
    - **Bron**: "Veeam Customer Success Stories" op de Veeam website.
4. **Mimecast**
    - **Case Study**: Juridisch bedrijf heeft de Mimecast geïmplementeerd voor de e-mailbevestiging en zagen daardoor vermindering in het aantal malware- en phishing-aanvallen.
    - **Bron**: "Mimecast Case Studies" op de Mimecast website.
5. **Microsoft Teams/Slack**
    - **Case Study**: Een IT-consultancybedrijf implementeerde Microsoft Teams om de communicatie en samenwerking te verbeteren binnen de organisatie, wat leidde tot efficiëntere projectuitvoering en klanttevredenheid.

- **Bron**: "Microsoft Teams Customer Stories" op de Microsoftwebsite.

6. **OneTrust**
    - **Case Study**: Een internationaal marketingbedrijf implementeerde OneTrust voor het beheer van AVG/GDPR-compliance, als resultaat heeft het bedrijf gezien dat de dataprivacy werd verbeterd en verminderde risico's in misbruik in de datawereld.
    - **Bron**: "OneTrust Customers" op de OneTrust website.

Om het plaatje compleet te maken en voor de volledige verhalen, check de bronnen die ik je heb aangewezen. Die verhalen laten zien hoe andere bedrijven diezelfde tech-dingen hebben aangepakt en er goed mee voor de dag zijn gekomen. Dit laat mooi zien dat het voor Datacadabra ook haalbaar is en wat het hen kan opleveren.

10.9. Beheerstrategie

Deze strategieën zullen Datacadabra helpen bij het effectief beheren van hun risico's, het beschermen van hun activa en reputatie, en het waarborgen van bedrijfscontinuïteit in een steeds veranderende zakelijke en technologische omgeving. Hoofdstuk 6 geeft ook welke risico beheerst, aangepakt of geaccepteerd moet worden. Bij de acceptatie of “negeren” van de risico’s doordat de impact laag is, wordt behandeld in het informatiebeveiligingsbeleid van Datacadabra.

Behandelingsplannen voor Risico's bij Datacadabra

1. **Datalek en Gegevensverlies**
    - **Risicovermindering**: Implementeer geavanceerde cybersecuritymaatregelen zoals Multifactorauthenticatie en end-to-end encryptie. Voer regelmatige cybersecuritytrainingen uit voor medewerkers om bewustzijn te vergroten.
    - **Risico-overdracht**: Sluit cyberverzekeringen af om financiële impact van datalekken en gegevensverlies te dekken.
    - **Risicovermijding**: Beperk toegang tot gevoelige gegevens tot alleen essentiële medewerkers en gebruik beveiligde cloudopslagoplossingen.
2. **Reputatieschade**
    - **Risicobeheersing**: Ontwikkel een crisiscommunicatieplan voor snelle en effectieve respons in geval van reputatieschade.
    - **Risico-acceptatie**: Accepteer een zeker niveau van risico, gezien het onvoorspelbare karakter van reputatieschade, maar zorg voor een solid plan voor reputatiemanagement.
3. **Nalevingskosten en Aansprakelijkheid**
    - **Risicovermindering**: Zorg voor naleving van relevante wet- en regelgeving door continue monitoring en aanpassing van processen.
    - **Risico-overdracht**: Overweeg juridische verzekeringen om mogelijke aansprakelijkheidskosten te dekken.
4. **Operationele Storingen**
    - **Risicovermindering**: Voer regelmatige onderhouds- en updatecycli uit voor technologische systemen. Ontwikkel bedrijfscontinuïteits- en rampenherstelplannen.
    - **Risico-acceptatie**: Accepteer dat kleine operationele storingen kunnen optreden, maar zorg voor snelle en effectieve responsmechanismen.
5. **Verlies van Intellectueel Eigendom**
    - **Risicovermindering**: Implementeer strikte toegangscontroles en beveiligingsprotocollen voor de bescherming van intellectueel eigendom.
    - **Risico-overdracht**: Gebruik patenten en auteursrechten om wettelijke bescherming te bieden voor intellectueel eigendom.

Implementatie van Behandelingsplannen

Voor een effectieve implementatie van deze behandelingsplannen is het essentieel dat Datacadabra:

- De verantwoordelijkheden duidelijk toewijst voor het beheer van elk risico.

- Regelmatige beoordelingen en updates van de risicobeheerstrategieën uitvoert.
- Voldoende middelen en trainingen voorziet voor de uitvoering van deze plannen.
- Zorgt voor een cultuur van risicobewustzijn en proactief management binnen de gehele organisatie.

10.9.1. Annex A

Elke dreiging is toegewezen aan een risico-eigenaar met de juiste kennis en bevoegdheid, wat zorgt voor effectief risicobeheer. Door deze gestructureerde benadering kan Datacadabra gerichte maatregelen implementeren om risico's te beheersen en de algehele bedrijfsveiligheid en -efficiëntie te verbeteren.

Om deze uitgebreide risicoanalyse voor Datacadabra uit te werken, zullen we de acht eerdergenoemde risico's in detail bekijken en ze toewijzen aan specifieke risico-eigenaren, terwijl we ook de kans en impact van elk risico beoordelen. Vervolgens worden passende beheersmaatregelen en eventuele aanvullende acties vastgesteld.

Datalek

- **Omschrijving**: Malware op productiesystemen kan leiden tot datalekken, waardoor klanten geen toegang meer hebben tot hun gegevens.
- **Risico-eigenaar**: IT Security Manager
- **Kans**: Midden (Kan 1 x per jaar voorkomen)
- **Impact**: Hoog (€10.001 – €50.000)
- **Risicowaarde**: Midden x Hoog
- **Beheersmaatregel**: Implementeer geavanceerde malware detectie en respons systemen.
- **Aanvullende maatregelen**: Regelmatige security-training voor IT-medewerkers.

2. Gegevensverlies

- **Omschrijving**: Technische storingen kunnen leiden tot onherstelbaar verlies van kritieke bedrijfsgegevens.
- **Risico-eigenaar**: Chief Technology Officer
- **Kans**: Laag (Kan 1 x in de 5 jaar voorkomen)
- **Impact**: Zeer hoog (€50.001 – €100.000)
- **Risicowaarde**: Laag x Zeer hoog
- **Beheersmaatregel**: Implementeer robuuste back-up- en disaster recovery-oplossingen.
- **Aanvullende maatregelen**: Investeer in redundante opslagsystemen.

3. Reputatieschade

- **Omschrijving**: Negatieve publiciteit door datalekken kan leiden tot aanzienlijke reputatieschade.
- **Risico-eigenaar**: Chief Marketing Officer
- **Kans**: Hoog (Kan 5 x per jaar voorkomen)
- **Impact**: Hoog (€10.001 – €50.000)
- **Risicowaarde**: Hoog x Hoog

- **Beheersmaatregel**: Ontwikkel een crisiscommunicatieplan en reputatiemanagementstrategie.
- **Aanvullende maatregelen**: Mediatraining voor senior management.

4. Nalevingskosten

- **Omschrijving**: Verhoogde regelgeving kan leiden tot aanzienlijke nalevingskosten.
- **Risico-eigenaar**: Compliance Officer
- **Kans**: Midden (Kan 1 x per jaar voorkomen)
- **Impact**: Midden (€5.001 – €10.000)
- **Risicowaarde**: Midden x Midden
- **Beheersmaatregel**: Implementeer een compliance monitoring en rapportagesysteem.
- **Aanvullende maatregelen**: Regelmatige compliance training voor relevante teams.

5. Aansprakelijkheidskosten

- **Omschrijving**: Productaansprakelijkheid door softwarefouten kan leiden tot aansprakelijkheidsclaims.
- **Risico-eigenaar**: Chief Product Officer
- **Kans**: Laag (Kan 1 x in de 5 jaar voorkomen)
- **Impact**: Hoog (€10.001 – €50.000)
- **Risicowaarde**: Laag x Hoog
- **Beheersmaatregel**: Versterk het software test- en kwaliteitsborgingsproces.
- **Aanvullende maatregelen**: Aanschaf van productaansprakelijkheidsverzekering.

6. Operationele Storingen

- **Omschrijving**: Stroomstoringen kunnen leiden tot productieverlies en operationele verstoringen.
- **Risico-eigenaar**: Operations Manager
- **Kans**: Midden (Kan 1 x per jaar voorkomen)
- **Impact**: Midden (€5.001 – €10.000)
- **Risicowaarde**: Midden x Midden
- **Beheersmaatregel**: Implementeer bedrijfscontinuïteitsplanning en noodstroomvoorzieningen.
- **Aanvullende maatregelen**: Regelmatige tests van noodstroomsystemen.

7. Intellectueel Eigendom Verlies

- **Omschrijving**: Diefstal van intellectueel eigendom kan leiden tot concurrentienadelen.
- **Risico-eigenaar**: Chief Legal Officer
- **Kans**: Zeer laag (Kan 1 x in de 10 jaar voorkomen)
- **Impact**: Zeer hoog (€50.001 – €100.000)
- **Risicowaarde**: Zeer laag x Zeer hoog
- **Beheersmaatregel**: Implementeer strikte toegangscontroles en monitor intellectueel eigendom.
- **Aanvullende maatregelen**: Juridische acties om intellectuele eigendomsrechten af te dwingen.

Elke dreiging is toegewezen aan een risico-eigenaar met de juiste kennis en bevoegdheid, wat zorgt voor effectief risicobeheer. Door deze gestructureerde benadering kan Datacadabra gerichte maatregelen implementeren om risico's te beheersen en de algehele bedrijfsveiligheid en -efficiëntie te verbeteren.

10.9.2. Actieplannen

Voor een uitgebreide uitwerking van de actieplannen voor elk risico bij Datacadabra, al er worden beschreven hoe de geselecteerde beveiligingscontroles worden geïmplementeerd en wie verantwoordelijk is voor elke actie:

Datalek

- **Actieplan**: Implementatie van geavanceerde malware detectie en respons systemen.
- **Verantwoordelijk**: Mark is verantwoordelijk voor het selecteren, implementeren en onderhouden van deze systemen.
- **Stappen**:
    1. Selecteer een geschikte malware detectie en responsoplossing.
    2. Configureer de oplossing specifiek voor de IT-infrastructuur van Datacadabra.
    3. Train IT-medewerkers in het gebruik en onderhoud van het systeem.
    4. Voer regelmatige tests en updates uit om ervoor te zorgen dat de systemen effectief blijven.

2. Gegevensverlies

- **Actieplan**: Implementatie van robuuste back-up- en disaster recovery-oplossingen.
- **Verantwoordelijk**: Chief Technology Officer (mark) is belast met het leiden van deze implementatie.
- **Stappen**:
    1. Bepaal de belangrijkste data-assets en beoordeel hun back-upbehoeften.
    2. Selecteer en implementeer passende back-up- en disaster recovery-oplossingen.
    3. Train relevante teams in het gebruik van deze oplossingen.
    4. Voer regelmatig back-up-tests uit om betrouwbaarheid te verzekeren.

3. Reputatieschade

- **Actieplan**: Ontwikkeling van een crisiscommunicatieplan en reputatiemanagementstrategie.
- **Verantwoordelijk**: IT-security manager en Managing Director (GJ) is verantwoordelijk voor het opstellen en implementeren van dit plan.
- **Stappen**:
    1. Ontwikkel een uitgebreid communicatieplan voor crisismanagement.
    2. Train het management en communicatieteams in de uitvoering van het plan.
    3. Stel monitoringsystemen in om de online en offline reputatie van het bedrijf te volgen.

4. Voer regelmatig simulatieoefeningen uit om de voorbereiding te testen.

4. Nalevingskosten

- **Actieplan**: Implementatie van een compliance monitoring en rapportagesysteem.
- **Verantwoordelijk**: Managing director is belast met het opzetten en onderhouden van dit systeem.
- **Stappen**:
    1. Identificeer relevante wet- en regelgeving voor Datacadabra.
    2. Implementeer systemen voor het monitoren en rapporteren van compliance.
    3. Train relevante teams in compliance procedures en rapportagevereisten.
    4. Voer regelmatige audits uit om naleving te waarborgen.

5. Aansprakelijkheidskosten

- **Actieplan**: Versterking van het software test- en kwaliteitsborgingsproces.
- **Verantwoordelijk**: Vincent zorgt voor de implementatie en handhaving van verbeterde testprocedures.
- **Stappen**:
    1. Evalueer en verbeter de huidige test- en kwaliteitsborgingsprocessen.
    2. Implementeer nieuwe testmethoden en -tools.
    3. Train ontwikkelaars en QA-teams in verbeterde processen.
    4. Voer regelmatige audits uit om de kwaliteit van de software te garanderen.

6. Operationele Storingen

- **Actieplan**: Implementatie van bedrijfscontinuïteitsplanning en noodstroomvoorzieningen.
- **Verantwoordelijk**: Operations Manager en CTO leidt deze inspanningen.
- **Stappen**:
    1. Ontwikkel en documenteer uitgebreide bedrijfscontinuïteitsplannen.
    2. Zorg voor noodstroomvoorzieningen en redundante systemen.
    3. Train relevante teams in het uitvoeren van bedrijfscontinuïteitsplannen.
    4. Voer regelmatig tests uit om de effectiviteit van de plannen te verifiëren.

7. Intellectueel Eigendom Verlies

- **Actieplan**: Implementatie van strikte toegangscontroles en monitoring van intellectueel eigendom.
- **Verantwoordelijk**: OM (officemanager), Catherine CTO beheert deze beveiligingsmaatregelen.
- **Stappen**:
    1. Identificeer en classificeer intellectueel eigendom binnen de organisatie.
    2. Implementeer beveiligingsmaatregelen, waaronder toegangscontroles en monitoring.
    3. Train relevante medewerkers in het beschermen van intellectueel eigendom.

4. Voer regelmatig audits uit om de bescherming van intellectueel eigendom te verzekeren.

Deze actieplannen zijn ontworpen om de specifieke risico's waarmee Datacadabra wordt geconfronteerd aan te pakken, met een duidelijke verdeling van verantwoordelijkheden en gedetailleerde stappen voor de implementatie van beveiligingscontroles.

10.9.3. Keuzes voor de actieplannen Datacadabra

De volgende keuzes in de actieplannen zijn het resultaat van uitgebreide gesprekken met diverse stakeholders bij Datacadabra, waaronder leidinggevenden, IT-specialisten, en managers. Hierbij is ook gekeken naar best practices in de branche.

1. **Datalek**
- **Keuze van Actieplan**: De keuze voor geavanceerde malware detectie en respons systemen kwam voort uit gesprekken met de IT-afdeling, waarbij duidelijk werd dat proactieve detectie van bedreigingen essentieel is. Best practices in de branche benadrukken het belang van deze systemen voor moderne cyberveiligheid.

2. **Gegevensverlies**
- **Keuze van Actieplan**: Op basis van feedback van de technologieteams en het analyseren van best practices, is besloten dat robuuste back-up- en disaster recovery-oplossingen cruciaal zijn voor het veiligstellen van bedrijfsgegevens.

3. **Reputatieschade**
- **Keuze van Actieplan**: De marketingafdeling, in overleg met het management, benadrukte het belang van een solide crisiscommunicatieplan en reputatiemanagementstrategie. Deze keuze weerspiegelt best practices in crisisbeheer.

4. **Nalevingskosten**
- **Keuze van Actieplan**: De keuze voor een compliance monitoring en rapportagesysteem is gebaseerd op aanbevelingen van de juridische afdeling en compliance officers, in lijn met industrienormen voor regelgevingsbeheer.

5. **Aansprakelijkheidskosten**
- **Keuze van Actieplan**: Na raadpleging van productontwikkelingsteams en analyse van risico's, is geconcludeerd dat het versterken van software test- en kwaliteitsborgingsprocessen noodzakelijk is om aansprakelijkheidsrisico's te verminderen.

6. **Operationele Storingen**
- **Keuze van Actieplan**: Deze keuze is gemaakt na overleg met managing director en het beoordelen van best practices voor bedrijfscontinuïteit en noodplanning in vergelijkbare organisaties.

7. **Intellectueel Eigendom Verlies**
- **Keuze van Actieplan**: In samenwerking met de juridische afdeling en op basis van branchenormen is besloten dat het beschermen van intellectueel eigendom een prioriteit is, waarbij strikte toegangscontroles en monitoring centraal staan.

Deze keuzes, gemaakt in samenwerking met en na raadpleging van verschillende afdelingen binnen Datacadabra, weerspiegelen een gezamenlijke inspanning om een

risicobeheerstrategie te ontwikkelen die in lijn is met zowel de interne behoeften van de organisatie als met externe best practices. Deze collaboratieve aanpak zorgt voor een gedegen en goed onderbouwd risicobeheerbeleid.

Interview 8

Interviewer	Rita Simon
Deelnemer	Mark Bulthuis CTO
Doelstelling	Achterhalen wat de aanpak is van risicobeheerproces binnen Datacadabra
Datum	7-11-2023

Rita: "Goedemiddag, bedankt dat u vandaag met mij wilt spreken over het risicobeheerproces bij Datacadabra. Kunt u ons eerst vertellen wat de aanleiding was voor het ontwikkelen van dit nieuwe proces?"

CTO: "De aanleiding was een duidelijke noodzaak om onze informatiebeveiligingspraktijken te verbeteren en beter af te stemmen op de standaarden van ISO 27001."

Rita: "Kunt u mij meer vertellen over hoe dit proces eruit zal zien?"

CTO: "We zijn van plan om te beginnen met een grondige risicoanalyse, uitgevoerd door ons beveiligingsteam samen met externe experts. Vervolgens zullen we, in samenwerking met de afdelingshoofden, specifieke actieplannen ontwikkelen voor elk geïdentificeerd risico."

Rita: "Hoe zorgt u ervoor dat deze actieplannen effectief worden uitgevoerd?"

CTO: "Elk risico wordt toegewezen aan een afdelingshoofd, die optreedt als risico-eigenaar. Zij zullen verantwoordelijk zijn voor het uitvoeren van de actieplannen binnen hun afdelingen. We zullen ook regelmatig de voortgang evalueren om de effectiviteit van deze plannen te waarborgen."

Rita: "Hoe ziet u de rol van technologie in dit nieuwe risicobeheerproces?"

CTO: "Technologie speelt een cruciale rol. We zullen geavanceerde beveiligingsoplossingen zoals multi-factor authenticatie en end-to-end-encryptie implementeren, naast het geven van regelmatige cybersecuritytrainingen aan ons personeel."

Rita: "Tot slot, hoe zal dit nieuwe proces bijdragen aan de algehele bedrijfsveiligheid en efficiëntie bij Datacadabra?"

CTO: "Dit proces zal ons helpen om proactief en systematisch de risico's te beheren. Met een duidelijke verantwoordelijkheidsverdeling en concrete uitvoeringsstappen zullen we onze bedrijfsveiligheid aanzienlijk verbeteren en tegelijkertijd de operationele efficiëntie verhogen."

10.10. Analyse communicatiestructuur

Interview 9

Interviewer	Rita Simon
Naam deelnemer	Catherine Ter Haar
Doel	Communicatiestructuur achter halen en vervolgens met de uitkomsten, patronen vinden.
Datum	14-11-2023

Hoe zou je de huidige communicatiestructuur binnen Datacadabra beschrijven?

- Ik vind onze communicatie vrij informeel, iedereen communiceert met elkaar via Slack, app, mail of telefonisch. Er zijn geen procedures of handleidingen hoe het wel zou moeden.

Welke communicatiekanalen worden het meest gebruikt voor interne communicatie? Zijn deze effectief voor informatiebeveiligingszaken?

- E-mail en Slack

Hoe regelmatig vindt communicatie plaats tussen verschillende afdelingen over informatiebeveiligingsonderwerpen?

- Communicatie over beveiliging gebeurt alleen als er een probleem is. Er is geen regelmatig schema.

Hoe duidelijk vind je de communicatie over informatiebeveiliging? Wordt complexe informatie op een begrijpelijke manier gecommuniceerd?

- Ik vind de informatie redelijk, maar er is weinig gelegenheid voor vragen of discussie, want het wordt niet erg goed gehandhaafd momenteel binnen de organisatie. Er zijn veel punten waar eraan gewerkt moet worden en daarom willen wij as jaar ISO 27001 implementeren en onderhouden.

Zijn er systemen of processen voor het geven van feedback over de interne communicatie? Hoe effectief zijn deze?

- Nee, We kunnen feedback geven tijdens vergaderingen, maar er lijkt weinig verandering te zijn.

Hoe spelen leidinggevenden een rol in de communicatie over informatiebeveiliging? Is hun rol effectief en duidelijk?

- Ik als manager ben erg toegankelijk en speel een actieve rol in de communicatie

Ervaar je consistentie in de communicatie over informatiebeveiliging binnen de organisatie?

- Er is geen consistentie; het varieert sterk van week tot week

Hoe effectief is de informatie-uitwisseling tussen afdelingen over belangrijke beveiligingsupdates of -wijzigingen?

- Ik vind dat we niet goed op de hoogte worden gehouden van beveiligingsupdates. Dit komt ook deels door ons zelf omdat wij daar niet veel mee bezig zijn op dit moment. Het is wel een vooruitstreven.

Worden er regelmatig trainingen of informatiesessies gehouden over informatiebeveiliging? Hoe beoordeel je de kwaliteit en frequentie van deze sessies?

- Trainingen zijn beschikbaar in wel weinige mate.

Welke verbeteringen zou je willen aanbrengen in de communicatiestructuur of -methoden met betrekking tot informatiebeveiliging?

- Het zou nuttig zijn om meer interactieve sessies te hebben in plaats van alleen e-mails

Interview 10

Interviewer	Rita Simon
Naam deelnemer	Gert Jan Naber
Doel	Communicatiestructuur achter halen en vervolgens met de uitkomsten, patronen vinden.
Datum	21 -11-2023

Hoe zou je de huidige communicatiestructuur binnen Datacadabra beschrijven?

- Ik vind onze communicatie vrij gedecentraliseerd; elke afdeling heeft zijn eigen stijl en aanpak.

Welke communicatiekanalen worden het meest gebruikt voor interne communicatie? Zijn deze effectief voor informatiebeveiligingszaken?

- E-mail en Slack

Hoe regelmatig vindt communicatie plaats tussen verschillende afdelingen over informatiebeveiligingsonderwerpen?

- Er zijn wekelijkse updates via e-mail, slack en vergaderingen.

Hoe duidelijk vind je de communicatie over informatiebeveiliging? Wordt complexe informatie op een begrijpelijke manier gecommuniceerd?

- De communicatie is duidelijk, maar we krijgen te veel informatie in één keer.

Zijn er systemen of processen voor het geven van feedback over de interne communicatie? Hoe effectief zijn deze?

- Nee, we kunnen feedback geven tijdens vergaderingen, maar er lijkt weinig verandering te zijn. Er moet een duidelijk plan van aanpak komen

Hoe spelen leidinggevenden een rol in de communicatie over informatiebeveiliging? Is hun rol effectief en duidelijk?

- Leidinggevenden lijken soms afgezonderd van de rest, wat de communicatie belemmert**.**

Ervaar je consistentie in de communicatie over informatiebeveiliging binnen de organisatie?

- Communicatie over het algemeen, omdat het een informeel procedure is, en informeel bedrijf, gaat het enorm snel en soepel. Echter wordt er over informatiebeveiliging weinig gecommuniceerd.

Hoe effectief is de informatie-uitwisseling tussen afdelingen over belangrijke beveiligingsupdates of -wijzigingen?

- Informatiedeling gebeurt, maar kan meer gestructureerd en tijdig

Worden er regelmatig trainingen of informatiesessies gehouden over informatiebeveiliging? Hoe beoordeel je de kwaliteit en frequentie van deze sessies?

- Trainingen zijn beschikbaar in wel weinige mate, maar niet verplicht, dus niet iedereen neemt deel

Welke verbeteringen zou je willen aanbrengen in de communicatiestructuur of -methoden met betrekking tot informatiebeveiliging?

- Een centraal communicatieplatform zou helpen om informatie beter te organiseren

10.10.1. Analyse van de uitkomsten

De gemiddelde score van een categorie wordt berekend door de som van alle scores in die categorie te nemen en vervolgens te delen door het aantal scores. Op de uitkomsten is er categorisatie toegepast, 1 tot 5. Waarbij 1 staat voor een negatieve of ineffectieve communicatie en 5 voor een zeer positieve of effectieve communicatie. Deze scores zijn vervolgens gebruikt om de gemiddelden en standaarddeviaties voor elke categorie te berekenen. De formule is als volgt:

Gemiddelde:

$$\frac{\sum \text{Scores}}{\text{Aantal scores}}$$

Voor de categorie "Communicatiestructuur" met scores 3 en 2:
Gemiddelde=3+22=2.5Gemiddelde=23+2=2.5

Standaarddeviatie:

$$\sqrt{\frac{\sum(x-\text{Gemiddelde})^2}{\text{Aantal scores}}}$$

Voor de categorie "Communicatiestructuur" met scores 3 en 2 en een gemiddelde van 2.5:
Standaarddeviatie=(3−2.5)2+(2−2.5)22=0.5Standaarddeviatie=2(3−2.5)2+(2−2.5)2=0,5

Categorie	Gemiddelde	Standaarddeviatie
Communicatiestructuur	2.5	0.5
Communicatiekanalen	4.0	0.0

Categorie	Gemiddelde	Standaarddeviatie
Frequentie van Communicatie	2.5	0.5
Duidelijkheid	3.5	0.5
Feedback Mechanismen	2.0	0.0
Rol van Leidinggevenden	3.0	1.0
Consistentie	2.5	0.5
Effectiviteit van Informatiedeling	3.0	0.0
Trainingen en Sessies	3.0	0.0
Verbeterpunten	4.0	0.0

Tabel 5: communicatieanalyse

Maatstaf gemiddelde:
Deze maatstaf biedt inzicht in het niveau van tevredenheid binnen een specifieke categorie. Het is nuttig om te begrijpen wat over het algemeen goed werkt en wat verbetering behoeft in de communicatie.

Maatstaf standaarddeviatie:
Deze statistiek meet de mate van variatie in de antwoorden. Een kleine standaarddeviatie duidt op een hoge mate van overeenstemming onder de respondenten over een bepaald aspect van de communicatie, terwijl een grotere standaarddeviatie wijst op een grotere diversiteit in de percepties en ervaringen van individuen.

Keuze voor de berekeningen:
Gemiddelde:

1. De keuze voor gemiddelde berekenen is gedaan omdat het gemiddelde een algemene indicatie geeft van de centrale tendens of het 'gemiddelde' niveau reacties.

Het is belangrijk voor de analyse om een snel overzicht te krijgen van de algemene houding of perceptie onder de stakeholders.

2. Het gemiddelde maakt het mogelijk om verschillende categorieën of aspecten van de enquête direct met elkaar te vergelijken.

Standaarddeviatie:

1. De standaarddeviatie geeft aan hoeveel de antwoorden variëren rond het gemiddelde. Dit is cruciaal om te begrijpen hoe divers de meningen zijn.
2. Een lage standaarddeviatie duidt op een hoge mate van overeenstemming onder de respondenten, terwijl een hoge standaarddeviatie wijst op grotere meningsverschillen. Dit is belangrijk voor het bepalen van gebieden waarover overeenstemming bestaat en waar meer aandacht nodig is vanwege verschillende meningen.

Analyse van de uitkomsten:

1. **Structuur en Frequentie van Interne Communicatie**:
    - Met gemiddelden van 2.5 voor beide aspecten, toont deze analyse een middelmatig niveau van tevredenheid of effectiviteit aan. De

standaarddeviatie van 0.5 laat zien dat er variaties zijn in de percepties van deze communicatieaspecten, wat op inconsistenties binnen de organisatie kan duiden. Hieruit volgt dat er mogelijkheden zijn tot verbetering, althans de verbetering moet gedaan worden.

2. **Communicatiemiddelen, Feedbackprocessen, Efficiëntie in Informatiedeling, Trainingen, en Verbeteringsvoorstellen**:
    - Deze categorieën vertonen uniforme scores (standaarddeviatie van 0.0), wat aangeeft dat er een algemene overeenstemming is onder de respondenten over deze aspecten. Dit wijst op een algemene tevredenheid en overeenstemming onder de respondenten over de manier waarop deze aspecten van communicatie binnen Datacadabra worden afgehandeld.
3. **Rol en Impact van Leidinggevenden op Communicatie**:
    - Deze categorie laat de meeste variatie in antwoorden zien, met een standaarddeviatie van 1.0. Dit wijst op uiteenlopende meningen en ervaringen betreft de rol en effectiviteit van leidinggevenden in communicatieprocessen. Het is een indicatie dat er aandacht besteed moet worden aan hoe leiderschap de interne communicatie beïnvloedt, met mogelijkheid tot verbetering

Kortom, de analyse laat zien dat er binnen Datacadabra specifieke gebieden zijn in communicatie die verbetering behoeven. Er is variatie in hoe de rol van leidinggevenden wordt ervaren, terwijl er over andere aspecten zoals de gebruikte communicatiemiddelen en feedbackprocessen brede overeenstemming bestaat.

10.10.2. Versterking van interne communicatie en leiderschap

Om de deelvraag 'Hoe kan Datacadabra de samenwerking en communicatie tussen afdelingen verbeteren om een geïntegreerde aanpak van informatiebeveiliging te waarborgen?' volgens de ISO 27001 verder uit te werken, is het van belang te kijken naar specifieke richtlijnen en praktijken die daarbij aansluiten.

Bij het verbeteren van de samenwerking en communicatie binnen Datacadabra voor effectieve informatiebeveiliging, ligt de focus op de onderstaande alinea's. Deze stappen, in lijn met ISO 27001, dragen bij aan het waarborgen van een geïntegreerde aanpak van informatiebeveiliging binnen de organisatie. Meer gedetailleerde informatie over deze stappen en hun implementatie is te vinden in bijlage 10.9 van het interview.

Versterken van de communicatiestructuur

De huidige communicatiestructuur binnen Datacadabra, zoals geïdentificeerd in de interviewresultaten (zie bijlage 10.9 interview 1 en 2 (gemiddelde score van 2,5 met een standaarddeviatie van 0,5)), duidt op een behoefte aan meer gestructureerde communicatieprocedures binnen de organisatie. Voor een effectievere informatiebeveiligingsaanpak is het essentieel om vaste communicatiekanalen en regelmatige updates in te stellen. Dat leidt tot een consistente en transparante uitwisseling van aan informatiebeveiliging gerelateerde kwesties tussen afdelingen.

Verbeteren van feedbackprocessen

Uit de analyse naar de uitkomsten van de interviews die gehouden is met de OM en MD, terug te vinden in de bijlage 10.9 interview 1 en 2, blijkt dat de huidige feedbackmechanismen een beperkte effectiviteit hebben (gemiddelde score van 2,0). Hierbij is de standaarddeviatie en de gemiddelde berekend van de uitkomsten, voor een gedetailleerde toelichting over de berekening, is terug te vinden in bijlage 10.9. Het implementeren van een gestructureerd feedbackproces, zoals regelmatige enquêtes of feedbacksessies, verhoogt de betrokkenheid van medewerkers bij het verbeteren van communicatieprocessen en bevordert een cultuur van voortdurende verbetering.

Rol van leiderschap in communicatie

Na de analyse van de cultuur van Datacadabra, zie hoofdstuk 2.4, is tijdens het onderzoek opgemerkt dat bij Datacadabra leiderschap een rol speelt in het verbeteren van effectieve communicatie, vooral op het gebied van informatiebeveiliging. Zie hiervoor de samenvatting van het gesprek in bijlage 10.14 en het organogram, dat overduidelijke hiërarchie laat zien. De leidinggevenden binnen de organisatie, die beïnvloed zijn door de adhocracycultuur, stimuleren innovatie en buiten de gebaande paden treden. Dit is essentieel voor het aanpakken van beveiligingsuitdagingen in een groeiend, datagedreven bedrijf als Datacadabra. Door training en workshops kunnen leidinggevenden hun communicatievaardigheden verbeteren, wat kan zorgen voor een duidelijke en effectieve sturing van informatiebeveiligingsinitiatieven. Actieve betrokkenheid en duidelijke communicatie is belangrijk voor het verspreiden van een cultuur, met eigenschappen zoals het bewustzijn over informatiebeveiliging en streven naar een verbeterde omgeving wat informatiebeveiliging betreft.

Uitbreiding van training en bewustwording
De gemiddelde score voor trainingen en cursussen was 3,0, wat de behoefte aan meer gestructureerde en verplichte trainingen op het gebied van informatiebeveiliging onderstreept. Interactieve, regelmatige trainingssessies vergroten het bewustzijn en begrip van medewerkers, wat van cruciaal belang is voor het garanderen van effectieve informatiebeveiligingspraktijken.

Ontwikkeling van een centraal communicatieplatform
Respondenten verklaarden dat het opzetten van een centraal communicatieplatform de efficiëntie van de informatie-uitwisseling zou vergroten. Het platform moet toegankelijk zijn voor alle medewerkers en moet dienen als het primaire medium voor het delen van updates en begeleiding op het gebied van informatiebeveiliging.

Hieronder is de analyse uitkomst van de interviews die plaats heeft gevonden binnen Datacadabra, zie voor een uitgebreidere uitwerking van de analyse bijlage 10.9.1.

Categorie	**Gemiddelde**	**Standaarddeviatie**
Communicatiestructuur	2,5	0,5
Communicatiekanalen	4,0	0,0
Frequentie van communicatie	2,5	0,5
Duidelijkheid	3,5	0,5
Feedbackmechanismen	2,0	0,0
Rol van leidinggevenden	3,0	1,0
Consistentie	2,5	0,5
Effectiviteit van informatiedeling	3,0	0,0
Trainingen en sessies	3,0	0,0
Verbeterpunten	4,0	0,0

Tabel 2: communicatiescore

Door deze stappen te volgen, kan Datacadabra niet alleen de communicatie en samenwerking tussen afdelingen verbeteren, maar ook een sterke, ISO 27001-conforme aanpak van informatiebeveiliging waarborgen. Dat leidt tot verbeterde beveiliging van gegevens.

Implementatie van een information securitymanagement system (ISMS)
Volgens ISO 27001 moet Datacadabra een information securitymanagement system (ISMS) implementeren. Dit omvat het vaststellen van duidelijk beleid, het definiëren van beveiligingsdoelstellingen en het identificeren van risico's en de nodige beveiligingscontroles. Dit systeem dient als de ruggengraat voor alle informatiebeveiligingsactiviteiten en helpt bij het waarborgen van een systematische en consistente aanpak.
Interne communicatie volgens ISO 27001-richtlijnen
Communicatie over informatiebeveiliging moet regelmatig en duidelijk zijn. Dit betekent het organiseren van periodieke vergaderingen, het uitsturen van nieuwsbrieven of updates via het centrale communicatieplatform en het houden van trainingen en workshops. Alle

communicatie moet gericht zijn op het vergroten van het bewustzijn over beveiligingsbeleid, risico's en incidenten, evenals op de verantwoordelijkheden van individuele medewerkers.

Rol in leiderschap en communicatie

Een sleutelelement van ISO 27001 is het duidelijk definiëren van rollen en verantwoordelijkheden met betrekking tot informatiebeveiliging. Dit omvat het toewijzen van specifieke beveiligingstaken aan individuele werknemers of teams en het verzekeren dat iedereen in de organisatie begrijpt hoe zijn of haar acties de algehele informatiebeveiliging beïnvloeden.

Feedback- en verbeteringsprocessen

De clancultuur binnen Datacadabra wordt benadrukt door teamwerk en ondersteuning en biedt een sterke basis voor feedbackprocessen. Dit is een cultuur waarin de medewerkers in een omgeving zijn waar zij zich op hun gemak voelen om hun mening te delen en samen te werken aan verbeteringen. Dit zorgt voor de implementatie van gestructureerde feedbackmechanismen, zoals periodieke enquêtes en feedbacksessies, waardoor werknemers actief betrokken raken bij de verbetering van communicatieprocessen. Deze aanpak is cruciaal in een cultuur van continue verbetering, waarbij feedback niet alleen beloond wordt met waardering, maar als instrument gebruikt wordt voor organisatorische groei en ontwikkeling op het gebied van informatiebeveiliging. Het creëren van effectieve feedbackkanalen is cruciaal. Medewerkers moeten de mogelijkheid hebben om zorgen, suggesties of incidenten te melden. Deze input moet worden gebruikt om continu verbeteringen aan te brengen in het ISMS.

Regelmatige evaluatie en audit

Conform ISO 27001 moet Datacadabra regelmatige interne en externe audits uitvoeren om de effectiviteit van haar ISMS te beoordelen. Dit helpt bij het identificeren van gebieden voor verbetering en zorgt ervoor dat de organisatie voldoet aan de normen en voortdurend haar beveiligingsmaatregelen verbetert.

Incidentmanagement en responsplanning

Zoals gesuggereerd in de interviews, is het ontwikkelen van een effectief incidentresponsplan voor Datacadabra B.V. essentieel. Dit plan moet niet alleen grondig worden opgesteld, maar ook regelmatig worden getest om te zorgen voor paraatheid. Een goed uitgewerkt en regelmatig getest incidentresponsplan stelt Datacadabra in staat om snel en efficiënt te reageren op beveiligingsincidenten. Dit is van cruciaal belang voor het minimaliseren van schade en het snel herstellen van de normale bedrijfsvoering na een incident. Bovendien draagt een robuust incidentresponsplan bij aan het versterken van het vertrouwen van klanten en belanghebbenden in de organisatie. Het toont aan dat Datacadabra proactief is in het beheren van beveiligingsrisico's en serieuze maatregelen neemt om de integriteit van hun gegevens en systemen te beschermen.

10.11. Aanpak risico's

Elke dreiging is toegewezen aan een verantwoordelijke risico-eigenaar, wat bijdraagt aan effectief risicobeheer. Door deze gestructureerde benadering kan Datacadabra gerichte maatregelen implementeren om risico's te beheersen en de algehele bedrijfsveiligheid en -efficiëntie te verbeteren.

Deze actieplannen zijn essentieel om de specifieke risico's bij Datacadabra aan te pakken en zorgen voor een duidelijke verdeling van verantwoordelijkheden en gedetailleerde stappen voor de implementatie.

Risico	**Risicovermindering**	**Risico-overdracht**	**Risicovermijding en risicoacceptatie**
Datalek en gegevensverlies	Implementatie van multifactorauthenticatie, end-to-end-encryptie en regelmatige cybersecuritytrainingen. Voor toelichting van de methodes, zie hoofdstuk 2.6 en 2.7. (*Identity | Okta*, z.d.) (Stealthlabs Inc, 2022)	Afsluiten van cyberverzekeringen voor financiële dekking.	Beperken van toegang tot gevoelige data en gebruik van beveiligde cloudopslag.
Reputatieschade	Ontwikkeling van een crisiscommunicatieplan voor snelle reactie (zie toelichting in het hoofdstuk 3.2.4).'	Niet van toepassing	Accepteren van een bepaald niveau van risico met een plan voor reputatiemanagement.
Nalevingskosten en aansprakelijkheid	Zorgen voor voortdurende naleving van wet- en regelgeving. Zie bijlage 10.1 interview 6	Overwegen van juridische verzekeringen voor dekking van mogelijke kosten.	Niet van toepassing
Operationele storingen	Uitvoeren van regulier onderhoud en updates van systemen, ontwikkelen van bedrijfscontinuïteits- en rampenherstelplannen. Zie voor een toelichting van de uitwerking van het plan hoofdstuk 3.2.3.	Niet van toepassing	Accepteren van kleine storingen met snelle responsmechanismen.

Verlies van intellectueel eigendom	Implementeren van strikte toegangscontroles en beveiligingsprotocollen.	Gebruiken van patenten en auteursrechten voor wettelijke bescherming.	Niet van toepassing

Tabel 4: Aanpak risico's

10.12. Aanvullende aanpak

Deze aanpak, zie bijlage 10.1 voor het interview met de CTO, ondersteund door grondig literatuuronderzoek en overleg met stakeholders, zorgt ervoor dat Datacadabra's informatiebeveiliging in lijn is met ISO 27001 en is aangepast aan de specifieke behoeften en uitdagingen van de organisatie.

1. **Identificatie van datalekrisico's**: ik adviseer het grondig analyseren van IT-beveiligingsrapporten en incidentlogboeken om risico's op datalekken in kaart te brengen. Deze documenten bevatten waardevolle informatie over potentiële zwakke punten en eerdere beveiligingsincidenten. Door deze bronnen te analyseren, kunnen we patronen herkennen en preventieve maatregelen ontwikkelen. Het aanvullen van deze data-analyse met gesprekken met IT-medewerkers is cruciaal. Deze professionals hebben directe ervaring met de dagelijkse beveiligingsuitdagingen en kunnen diepgaande inzichten bieden in specifieke dreigingen, zoals phishingaanvallen, e-mailbeveiliging en identiteitsverificatieprocessen. Hun perspectief is essentieel voor een holistische risicobeoordeling.
2. **Identificatie van gegevensverliesrisico's**: voor Datacadabra is het essentieel om de processen rondom gegevensbeheer en back-upprotocollen grondig te analyseren. Door feedbacksessies te organiseren met personeel dat zich bezighoudt met gegevensbeheer en IT-onderhoud, kunnen we specifieke risico's identificeren die anders over het hoofd gezien kunnen worden. Deze interacties stellen ons in staat om operationele uitdagingen en technische beperkingen vanuit een praktisch perspectief te begrijpen, wat leidt tot effectievere risicobeperkingsstrategieën.
3. **Identificatie van risico's op verlies van vertrouwen**: het verlies van klant- en leveranciersvertrouwen kan ernstige gevolgen hebben. Daarom stel ik voor om klantfeedback en leveranciersbeoordelingen te analyseren. Deze informatiebronnen geven inzicht in de percepties en verwachtingen van onze belangrijkste stakeholders. Door extra aandacht te besteden aan het optimaliseren van onze communicatieprocedures en -effectiviteit, kunnen we niet alleen risico's identificeren, maar ook werken aan het versterken van onze relaties met klanten en leveranciers.
4. **Identificatie van nalevingskostenrisico's**: tot slot adviseer ik een grondige regelgevingsreview en overleg met het juridische team om nalevingskostenrisico's te identificeren. Dit is vooral belangrijk gezien de vereisten van de ISO 27001-normen. Door deze aanpak krijgen we inzicht in de compliance-uitdagingen waarmee Datacadabra te maken heeft en de daaraan gerelateerde kosten. Deze kennis is cruciaal voor het effectief beheren van risico's op het gebied van regelgeving en compliance.

Dit plan, ontwikkeld in samenwerking met de CTO en gebaseerd op grondig onderzoek, stelt Datacadabra in staat om proactief potentiële risico's aan te pakken en de bedrijfsveiligheid en -stabiliteit te waarborgen.

10.13. GAP-analyse aanvullend

Voor het beantwoorden van de deelvraag ‘Hoe kan Datacadabra informatietechnologie integreren in haar bedrijfsprocessen om de informatiebeveiliging te optimaliseren en te waarborgen?’, is het essentieel voor Datacadabra om een geïntegreerde aanpak te hanteren die zowel technologische upgrades als beleidsmatige verbeteringen omvat. Conform ISO 27001 en de AVG (De algemene verordening gegevensbescherming)/GDPR (General Data Protection Regulation) zie hoofdstukken 2.4 en 2.5 moet Datacadabra zich vooral richten op het versterken van de beveiliging van gegevens opgeslagen in Google Cloud.

In de volgende opsomming wordt besproken hoe Datacadabra de integratie van IT en informatiebeveiliging in haar bedrijfsprocessen kan verbeteren:

1. **Huidige versus gewenste situatie**: analyse van de beveiligingsinfrastructuur en beleidsnaleving bij Datacadabra, met een overzicht van noodzakelijke upgrades en verbeteringen om volledige compliance en effectief incidentbeheer te bereiken.
2. **Bedrijfsprocessen en integratiestrategieën**: beschrijving van Datacadabra's verkoopverwerkingsproces, inclusief de stappen om informatiebeveiliging te integreren in afdelingen en functies binnen de organisatie.
3. **Toekomstige ontwikkelingen**: focus op automatisering, privacy-integratie en versterking van de beveiliging in diverse stadia van productontwikkeling om Datacadabra's positie in een complexe technologie- en beveiligingswereld te versterken.
4. **Incident respons plan (IRP)**: overzicht van het IRP-proces bij Datacadabra, inclusief de rollen en interacties tussen klanten, de directie en supportafdeling bij incidentmanagement om de efficiëntie en klanttevredenheid te verhogen.

De focus op versterking van het informatiebeveiligingsbeleid en handhaving en de upgrade van beveiligingstechnologie en -infrastructuur bij Datacadabra, is een gerichte keuze gebaseerd op grondige interne onderzoeken en analyses. Dit besluit is genomen om de volgende redenen:

1. **Versterking van informatiebeveiligingsbeleid en handhaving**: uit het onderzoek binnen Datacadabra, inclusief interviews (zie bijlage 10.1, interviews 4 tot 7), bleek dat hoewel een formeel informatiebeveiligingsbeleid aanwezig is, de handhaving ervan ontbreekt. Deze inconsistentie in uitvoering en het gebrek aan een gestructureerde aanpak in informatiebeveiliging, vooral in relatie tot ISO 27001-naleving en AVG/GDPR-compliance voor gegevens verwerkt via Google Cloud-diensten, brengen aanzienlijke risico's met zich mee. Daarom is er een dringende noodzaak om de handhaving en naleving van deze beleidsmaatregelen te verbeteren.
2. **Upgrade van beveiligingstechnologie en -infrastructuur**: de keuze voor het implementeren van technologische oplossingen, zoals KnowBe4, Google Cloud Platform, Veeam Backup, Mimecast, Microsoft Teams of Slack en OneTrust is gebaseerd op hun functionaliteit, reputatie en de specifieke eisen van het bedrijf. Deze beslissing, onderbouwd door de uitkomsten van een casestudy (zie hoofdstuk 8.6.1 en bijbehorende bronvermelding), is gemaakt om te zorgen voor een robuustere beveiligingsinfrastructuur die in staat is om de hedendaagse cybersecurity-uitdagingen aan te gaan.

Deze gerichte aanpak voor het versterken van het beleid en het upgraden van technologie en infrastructuur is essentieel om te zorgen voor een betrouwbare, effectieve en compliant informatiebeveiligingsomgeving binnen Datacadabra. Dit helpt niet alleen bij het verbeteren van de algehele beveiligingsstandaard van het bedrijf, maar ook bij het voldoen aan de complexe eisen van de hedendaagse dataregelgeving.

10.14. Aanvullende aanbevelingen voor informatiebeveiliging bij Datacadabra

9.12.1: Cybersecurity Dashboard Implementatie

- **Inhoud**: Stap-voor-stap instructies voor de implementatie van een cybersecurity dashboard. Dit omvat softwarekeuzes, data-integratie, opzetten van real-time monitoring, en het personaliseren van dashboards voor verschillende gebruikersgroepen.
- **Doel**: Het realiseren van een centrale hub voor bewaking en alarmering van beveiligingsgebeurtenissen en -trends.

9.12.2: Cybersecurity Drills en Simulaties

- **Inhoud**: Templates en scenario's voor het uitvoeren van cybersecurity drills, waaronder gesimuleerde phishing-aanvallen, ransomware-aanvallen en datalekscenario's. Inclusief evaluatieformulieren en debriefing sjablonen.
- **Doel**: Het versterken van de responsiviteit en voorbereiding van het team op echte beveiligingsincidenten.

9.12.3: Advanced Threat Intelligence en Monitoring Tools

- **Inhoud**: Een overzicht van geavanceerde threat intelligence platforms, met een focus op features zoals automatische dreigingsdetectie, integratie met bestaande beveiligingssystemen en AI-gestuurde analyses.
- **Doel**: Verhogen van proactieve beveiligingsmaatregelen en tijdige dreigingsdetectie.

9.12.4: Toepassing van AI en Machine Learning in Cybersecurity

- **Inhoud**: Een analyse van hoe AI en machine learning kunnen worden ingezet voor verbeterde dreigingsdetectie, anomaliedetectie en gedragsanalyse. Inclusief een lijst van aanbevolen AI-gebaseerde beveiligingsoplossingen.
- **Doel**: Verbeteren van de algehele beveiligingsintelligentie en adaptieve dreigingsrespons.

9.12.5: Externe Beveiligingsaudits

- **Inhoud**: Een handleiding voor het selecteren van een externe beveiligingsauditfirma, voorbereiding op audits en het begrijpen en implementeren van auditresultaten en aanbevelingen.
- **Doel**: Zorgen voor onafhankelijke validatie van beveiligingspraktijken en identificatie van verbeterpunten.

9.12.6: Ontwikkeling van een Incident Response Team

- **Inhoud**: Richtlijnen voor de oprichting van een incidentrespons team, inclusief roldefinities, trainingsschema's, en coördinatieprotocollen.
- **Doel**: Zorgen voor een snelle en gecoördineerde reactie op beveiligingsincidenten.

9.12.7: Geavanceerde Encryptie en Data Masking Technieken

- **Inhoud**: Gedetailleerde uitleg van verschillende encryptie- en data masking-technieken, inclusief best practices voor implementatie en onderhoud.
- **Doel**: Verhogen van de beveiliging van gevoelige data, zowel in rust als tijdens overdracht.

9.12.8: Versterking van End-Point Security

- **Inhoud**: Overzicht van end-point securityoplossingen, best practices voor configuratie, en strategieën voor het beheren van apparaten binnen en buiten het netwerk.
- **Doel**: Versterken van de beveiliging van eindpuntapparaten tegen externe en interne dreigingen.

9.12.9: Periodieke Beleids- en Procesherziening

- **Inhoud**: Schema en methodologie voor regelmatige herziening van beveiligingsbeleid en -processen, inclusief betrokkenheid van stakeholders en feedbackloops.
- **Doel**: Zorgen voor actuele en effectieve beveiligingsbeleid en -procedures.

9.12.10: Partnerschappen met Cybersecurity Bedrijven

- **Inhoud**: Richtlijnen voor het vormen van strategische partnerschappen met cybersecurity bedrijven, inclusief evaluatiecriteria, samenwerkingsmodellen en casestudies.
- **Doel**: Verkrijgen van gespecialiseerde beveiligingsexpertise en toegang tot geavanceerde beveiligingstools.

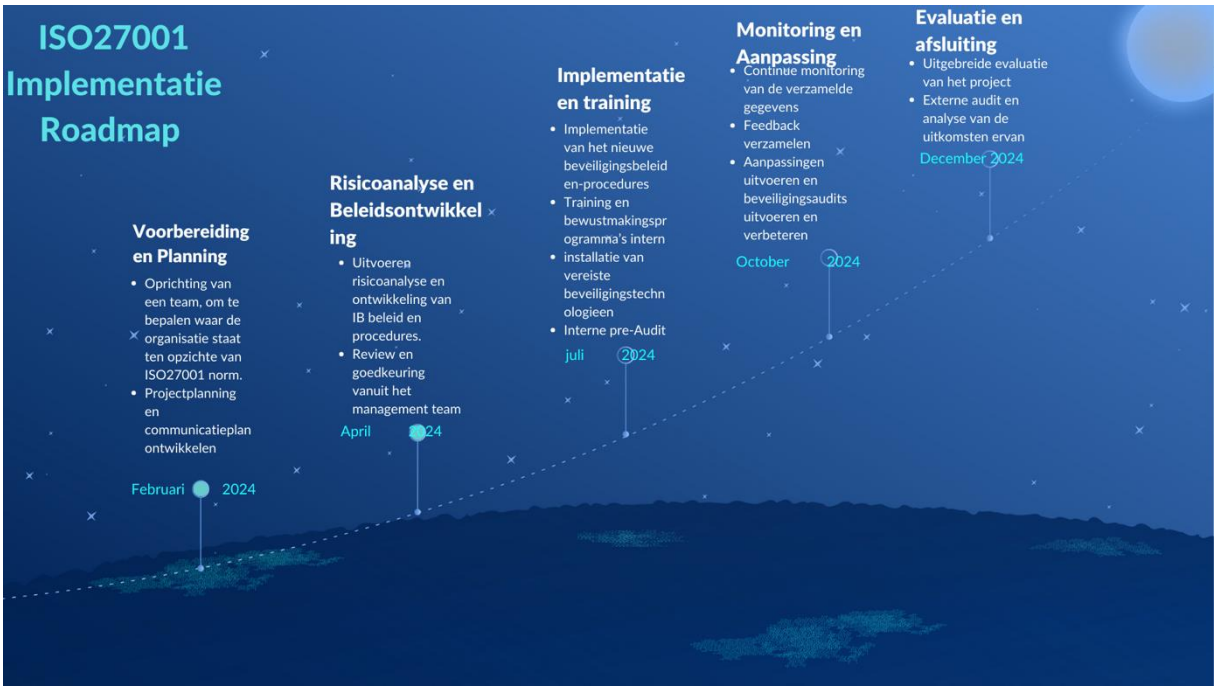
Deze uitgebreide bijlagen bieden een diepgaand inzicht in elke aanbeveling en stellen Datacadabra in staat om haar informatiebeveiliging naar een hoger niveau te tillen door geavanceerde technieken en samenwerkingen toe te passen.

10.14.1. Implementatieplan

Hieronder worden zowel de roadmap als de timeline voor de implementatie van de ISO 27001-norm voor Datacadabra geschetst. De roadmap is ontworpen om Datacadabra een helder beeld te geven van de diverse fases van de implementatie en wat per fase verwacht wordt. Elke fase, van de initiële voorbereiding en planning tot de uiteindelijke evaluatie en afronding, is belangrijk en hoort zorgvuldig te worden doorlopen. De roadmap biedt een gedetailleerd overzicht van de stappen die Datacadabra moet ondernemen om een sterk informatiebeveiligingsbeheersysteem op te zetten.

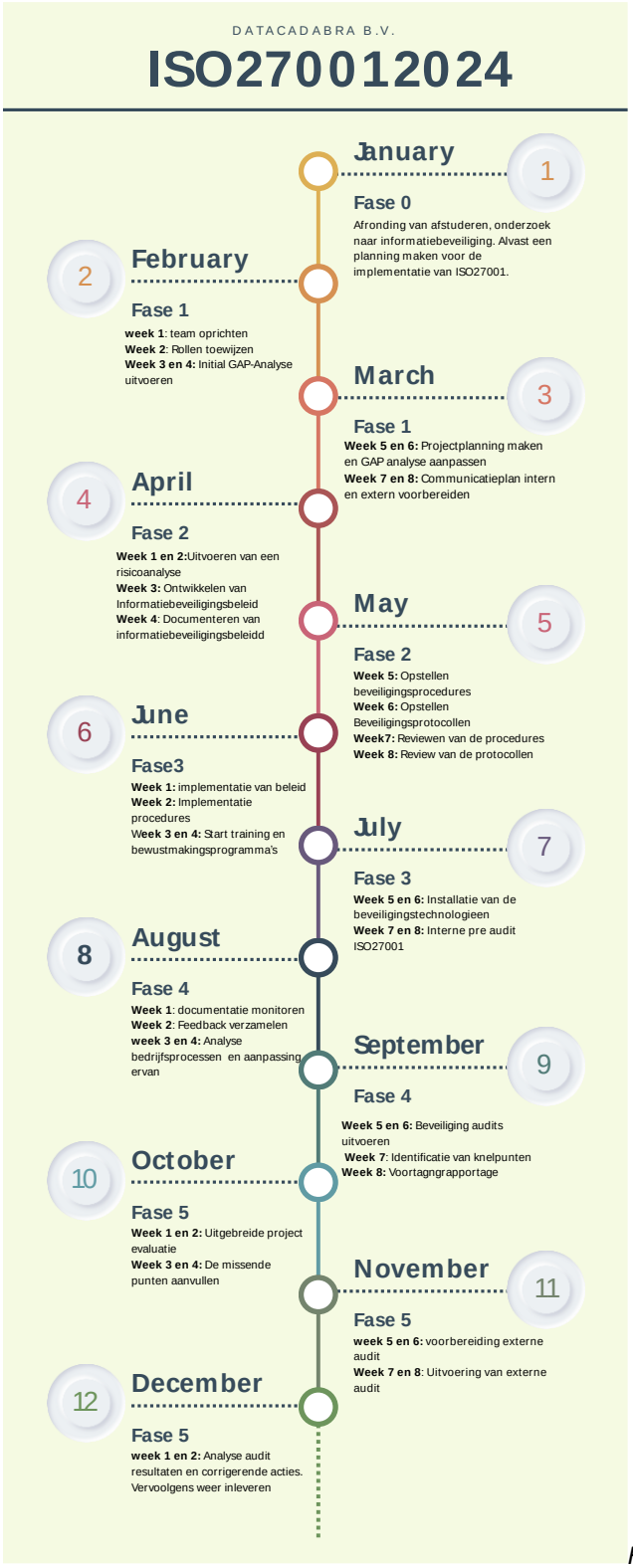
Hieronder volgt een overzicht van de fases met de bijbehorende kernactiviteiten en doelstellingen die de ruggengraat vormen van de implementatiestrategie:

1. Voorbereiding en planning: in deze fase wordt een team opgericht dat de GAP-analyse uitvoert, projectplanning ontwikkelt en een communicatieplan opstelt.
2. Risicoanalyse en beleidsontwikkeling: in deze fase wordt een risicoanalyse uitgevoerd en worden het informatiebeveiligingsbeleid en procedures ontwikkeld.
3. Implementatie en training: in deze fase staat centraal dat de medewerkers van Datacadabra bewuster worden van het beveiligen van de informatie en bewuster met de verkregen data omgaan.
4. Monitoring en aanpassing: in deze fase ligt de nadruk op implementatie, feedback en de verwerking daarvan en het uitvoeren van de audits.
5. Evaluatie en afronding: in deze fase ligt de nadruk op evaluatie en afronding van het project en tot slot de voorbereiding op de externe audit.



Figuur 14: roadmap

Hieronder staat de timeline voor de implementatie van ISO 27001.

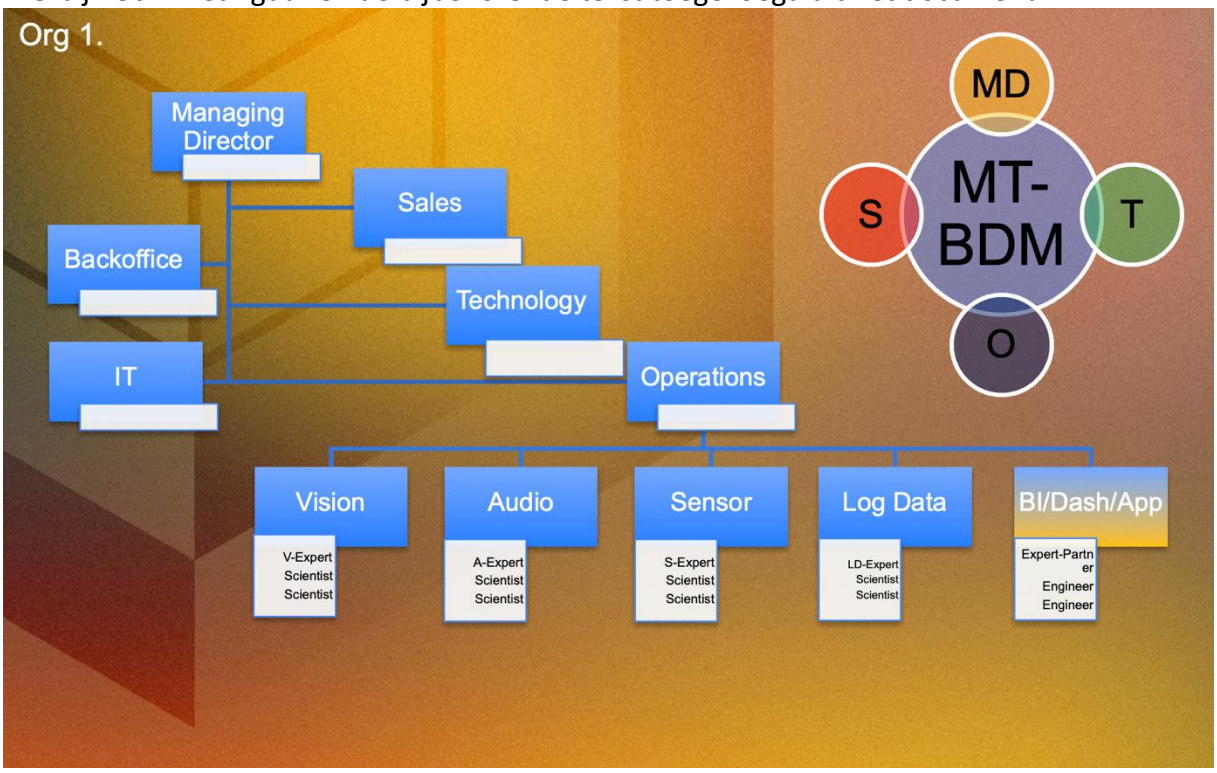


Figuur 15: timeline

Het primaire doel van ISO 27001 is het opzetten van een effectief ISMS dat in lijn is met de ISO 27001-norm. Het algehele doel omvat het vergroten van het bewustzijn en de competenties van medewerkers op het gebied van informatiebeveiliging, het versterken van de IT-infrastructuur tegen potentiële cyberbedreigingen en het waarborgen van compliance met internationale normen en regelgeving.

10.15. Organogram

Het onderstaande organogram is letterlijk uit de documentanalyse van Datacadabra gehaald. Hierbij heb ik het figuur en de bijbehorende tekst toegevoegd uit het document.



Directe aansturing van MD aan Backoffice, IT, Sales, Technology, Operations.

Sales: Accountmanagement, New Business, Commercie en dergelijke

Technology: Welke nieuwe technologieën toepasbaar voor de verschillende divisies, ontwikkeld schaalbare en modulaire oplossingen voor de AI-dienstverlening van DTCDBR. Houdt trends en innovaties nauwlettend in de gaten om zo het technisch niveau van DTCDBR concurrerend te houden en naar een hoger niveau te tillen.

Operations geeft directe sturing aan de divisies V, A, S, LD, BI waar in iedere divisie 1, mogelijk 2 experts/leads zijn van een divisie en in deze divisies zitten Scientisten. Kruisbestuiving mogelijk! BI/Dash tot op zekere hoogte vast onderdeel van DTCDBR. Voor echte applicatiebouw-Power BI e.d. partneren met derden.

Het MT wordt gevormd door de MD en de managers van S, T, O – Mogelijk aandeelhouders. MT-BDM bepalen gezamenlijk de ontwikkelingen van DTCDBR, de missie, visie, propositie, technologische ontwikkelingen, op welke trends inhaken e.d. voor zowel de kort-, middellange en lange termijn."

10.16. Risico's

Risico onummer	Risico titel	Risico beschrijving	Risico Oorzaak	Risico gevolg	Scope	Afdeling	Datum geconstateerd	Reden
1	Datalek	Een datalek is een incident waarbij gevoelige, vertrouwelijke, of beschermde gegevens onbedoeld worden blootgesteld, onthuld of gestolen. Dit kan gebeuren als gevolg van cyberaanvallen, onopzettelijke	Het datalek werd veroorzaakt door een succesvolle phishing-aanval op een medewerker die onbedoeld inloggegevens aan de aanvallers heeft verstrekt. De aanvallers verkregen daardoor toegang tot gevoelige klantgegevens.	Datalekken kunnen leiden tot schendingen van gegevensprivacywetgeving, boetes, juridische acties, reputatieschade en het verlies van het vertrouwen van klanten en partners.	De bescherming van gevoelige gegevens en informatiebeveiliging in de gehele organisatie	IT/ Informatie beveiliging	15-mrt-23	Door een medewerker is er geconstateerd dat een klant extra informatie in bezit had, wat niet had gehoeven

		fouten of menselijke fouten.						
2	Gegevensverlies	Gegevensverlies verwijst naar het onherstelbaar kwijtraken van belangrijke bedrijfsgegevens, zoals klantinformatie, financiële gegevens of intellectueel eigendom. Dit kan optred	Het gegevensverlies werd veroorzaakt door een menselijke fout waarbij een medewerker per ongeluk belangrijke gegevensbestanden van een gedeelde server v erwijderde zonder een back-up te maken.	Het verlies van kritieke gegevens kan leiden tot operationele verstoring, verlies van vertrouwen van klanten en leveranciers, juridische geschillen en financiële verliezen	Het beheer en de bescherming van belangrijke bedrijfsgegevens en informatieassets.	IT/ Gegevensbeheer	10-mei-23	De medewerker was bezig met het opschonen van oude bestanden op de gedeelde server en had niet opgemerkt dat enkele van deze besta

		en als gevolg van technische storingen, corruptie of gebrek aan back-ups						nden nog steeds in gebruik waren. De actie was onbedoeld en werd uitgevoerd zonder de vereiste dubbele controle.

3	Verlies van vertrouwen van klanten en leveranciers	Wanneer een organisatie te maken krijgt met incidenten zoals datalekken, operationele storingen of reputatieschade, kan het vertrouwen van zowel klanten als leveranciers ernstig worden geschaad.	Het verlies van vertrouwen van klanten en leveranciers werd veroorzaakt door een communicatiefout in een e-mailcampagne	Een afname van het vertrouwen kan leiden tot klantverloop, verlies van zakelijke partners, omzetdaling en langdurige reputatieschade.	Het behouden en herstellen van het vertrouwen van klanten en zakelijke relaties.	communicatie?	08-jun-23	Tijdens een marketingcampagne stuurde de organisatie per ongeluk een verkeerd geconfigureerde e-mail naar klanten en leveranciers, met verkeerde informatie over productaanbiedingen. Hierdoor ontstond

								verwarring en frustratie bij de ontvangers, wat resulteerde in een tijdelijk verlies van vertrouwen. De organisatie corrigeerde de fout snel en bood excuses aan

4	Nalevingskosten	Nalevingskosten verwijzen naar de uitgaven die een organisatie moet doen om te voldoen aan wettelijke voorschriften en regelgeving. Dit kan onder meer kosten voor nalevingsaudits, juridische kosten en boetes omvatten.		Niet-naleving van wet- en regelgeving kan leiden tot aanzienlijke financiële verplichtingen, boetes en juridische consequenties	Zorgen voor naleving van alle relevante wettelijke voorschriften en regelgeving die van toepassing zijn op de organisatie.	Juridische afdeling	20-jul-23	Door dat data cdabra op gesprekging voor het afsluiten van een contract, zijn ze erachter gekomen dat zij niet voldoen aan alle wet en regelgeving en daardoor tekenen van contract niet door kan gaan

5	Aansprakelijkheidskosten	Aansprakelijkheidskosten ontstaan wanneer een organisatie aansprakelijk wordt gesteld voor schade of letsel aan anderen. Dit kan variëren van productaansprakelijkheid tot aansprakelijkheid voor schadeclaims.	De organisatie werd geconfronteerd met aansprakelijkheidskosten als gevolg van een kleine softwarefout in een van haar producten.	Aansprakelijkheidskosten kunnen aanzienlijke financiële lasten met zich meebrengen, inclusief juridische verdedigingskosten en schadevergoedingen aan getroffen partijen	Het identificeren, beheersen en beperken van potentiële aansprakelijkheidskosten in verband met bedrijfsactiviteiten	Risk management	05-sep-23	Een consument ontdekte een kleine defect in een product van de organisatie, maar liep geen ernstige schade op. De consument diende echter een claim in voor gedeeltelijke vergoeding van de

								aankoopprijs van het product en eventuele bijkomende kosten voor reparatie. De organisatie accepteerde de aansprakelijkheid en ging akkoord met een redelijke schikking om het geschil op te lossen.

6	Reputatieschade	Reputatieschade treedt op wanneer er negatieve publiciteit, schandalen of incidenten de reputatie en geloofwaardigheid van een organisatie aantasten in de ogen van het publiek, klanten en partners	Hoewel de klacht niet wijdverspreid was en slechts één klant betrof, liep de organisatie het risico dat de negatieve recensie zich kon verspreiden en de perceptie van het publiek over de klantenservice van het bedrijf kon beïnvloeden. Dit kon mogelijk leiden tot een beperkte tijdelijke reputatieschade.	Reputatieschade kan leiden tot klantverlies, omzetdaling, moeilijkheden bij het aantrekken van nieuw talent en langdurige negatieve effecten op de merkwaarde.	Het beschermen, herstellen en versterken van de reputatie van de organisatie in de publieke perceptie.	Marketing/management	25-feb-23	Op 25 februari 2023 verscheen er een negatieve recensie van een klant op sociale media waarin een kleine ontevredenheid werd geuit over de klantenservice van de organisatie.

7	**Operationele storingen**	Operationele storingen omvatten gebeurtenissen zoals technische storingen, productiestops of andere problemen die de normale bedrijfsvoering verstoren.	De stroomstoring werd veroorzaakt door een plotselinge en onverwachte uitval in het lokale elektriciteitsnetwerk als gevolg van een technisch defect bij de elektriciteitsmaatschappij	Operationele storingen kunnen leiden tot omzetverlies, productieverlies, klantontevredenheid en moeilijkheden bij het herstellen van normale activiteiten	Het minimaliseren van risico's die kunnen leiden tot operationele storingen en het implementeren van plannen voor bedrijfscontinuïteit.	ontwikkelaars/operations	10-jun-23	Op 10 juni 2023 ondervond de organisatie een kortstondige stroomstoring vanwege een lokale stroomuitval, wat «resulteerde in een tijdelijke onderbreking van de kantooractiviteiten.

8	Verlies van intellectueel eigendom	Het verlies van intellectueel eigendom betekent dat waardevolle bedrijfsinformatie, innovaties of gepatenteerde processen in verkeerde handen vallen, waardoor concurrenten een voordeel krijgen	Het verlies van intellectueel eigendom werd veroorzaakt door een enkele voormalige werknemer die handelde uit ontevredenheid en bedrijfsdocumenten kopieerde. De bewuste medewerker ontdekte de inbreuk, maar er was geen blijvende schade aan waardevolle intellectuele eigendommen.	Verlies van intellectueel eigendom kan leiden tot concurrentieverlies, verlies van marktaandeel en verminderde concurrentiekracht	Het beschermen van bedrijfseigen informatie en intellectuele eigendomsrechten tegen ongeoorloofde toegang en gebruik	IT en eventueel R&D	14-sep-23	Op 14 september 2023 werd een medewerker bewustelos achtergelaten door een voormalige werknemer die enkele niet-geclassificeerde bedrijfsdocumenten had gekopieerd voordat hij vertrok.

Tabel 7: risico's inc oorzaken, gevolg en data

11. Reflectie inhoudelijk

Hieronder staan de reflecties per competentie weergegeven.

11.1. Analyseren

Beroepstaken

De beroepsactiviteiten in de scriptie richten zich op het diepgaand analyseren van Datacadabra's informatiebeveiligingsuitdagingen, waaronder SWOT- en risicoanalyses, stakeholderanalyse, en het gebruik van de 'Risk Impact Scale', om effectieve strategieën en maatregelen voor informatiebeveiliging te ontwikkelen.

Reflectie

In mijn onderzoek heb ik een grondige analytische benadering toegepast om de informatiebeveiligingsuitdagingen bij Datacadabra te onderzoeken. Door een mix van interviews, documentanalyses, SWOT-analyses en Root Cause Analysis (RCA) te gebruiken, kon ik de specifieke risico's die Datacadabra's informatiebeveiliging bedreigen, analyseren. Deze methoden stelden me in staat om niet alleen de oppervlakkige symptomen, maar ook de onderliggende oorzaken van de beveiligingsproblemen te identificeren. Mijn analyse leidde tot het verkrijgen van waardevolle inzichten, die cruciaal waren voor het formuleren van effectieve en doelgerichte aanbevelingen ter verbetering van Datacadabra's informatiebeveiliging. Tijdens mijn onderzoek vond ik het soms uitdagend om een documentanalyse uit te voeren, aangezien Datacadabra nauwelijks formele documentatie had over hun informatiebeveiligingspraktijken. Deze uitdaging benadrukte het belang van het aanscherpen van mijn analytische vaardigheden om toch betekenisvolle inzichten te verkrijgen.

11.2. Adviseren

Beroepstaken

Deze omvatten het adviseren over informatiebeveiligingsstrategieën, het aanbevelen van verbeteringen in de beveiligingsinfrastructuur, en het voorstellen van maatregelen om het bewustzijn en training van medewerkers te vergroten.

Reflectie

In mijn rol als adviseur voor Datacadabra's informatiebeveiliging, heb ik verschillende adviezen uitgewerkt, gericht op het verbeteren van de beveiligingsinfrastructuur en het verhogen van het bewustzijn en de training van medewerkers. Deze adviezen omvatten het aanbevelen van specifieke beveiligingstechnologieën, zoals multifactorauthenticatie en end-to-end-encryptie, en het ontwikkelen van uitgebreide training- en bewustwordingsprogramma's. Mijn analytische benadering in het identificeren van de belangrijkste beveiligingsrisico's en -uitdagingen heeft mij geholpen om doelgerichte en praktische adviezen te geven die niet alleen voldoen aan de huidige beveiligingsnormen, maar ook anticiperen op toekomstige uitdagingen. Hoewel het soms uitdagend was om de nodige informatie te verkrijgen - vooral omdat Datacadabra zelf niet altijd de nodige aandacht aan documentanalyse besteedde - heeft deze veelzijdige aanpak mij geholpen om een grondig inzicht te krijgen in de huidige beveiligingsrisico's van de organisatie. Deze diepgaande analyse was essentieel voor het identificeren van de belangrijkste gebieden die verbetering behoefden.

11.3. Ontwerpen

Beroepstaken

Het ontwikkelen van een gedetailleerde implementatiestrategie voor ISO 27001, het opstellen van effectieve beveiligingsprotocollen en -processen, en het integreren van geavanceerde technologieën zoals multifactorauthenticatie en end-to-end-encryptie.

Reflectie

In mijn onderzoek heb ik me gericht op de competentie 'Ontwerpen' door het ontwikkelen van een gedetailleerde implementatiestrategie voor ISO 27001 bij Datacadabra. Dit omvatte het opstellen van een roadmap, het uitwerken van BPMN-diagrammen van bedrijfsprocessen, en het aangeven van verbeterpunten of implementaties van informatiebeveiliging binnen verschillende processen bij Datacadabra. Mijn aanpak benadrukte het integreren van geavanceerde technologieën zoals multifactorauthenticatie en end-to-end-encryptie in de bedrijfsprocessen. Deze ontwerpactiviteiten waren van belang voor het vaststellen van effectieve beveiligingsprotocollen en -processen, en ze hielpen bij het verduidelijken van hoe informatiebeveiliging kon worden geïntegreerd binnen Datacadabra.

11.4. Algemene reflectie

Mijn ervaring met het werken bij Datacadabra was zeer positief en heeft mij in staat gesteld om me verder te ontwikkelen in het veld van informatiebeveiliging, een richting waarin ik na mijn afstuderen kan voortzetten. Echter, de begeleiding vanuit Saxion was teleurstellend, met frequente afwezigheid van docenten door privéomstandigheden, wat resulteerde in een gebrek aan begeleiding tijdens mijn afstudeerproject. Deze situatie was extra uitdagend vanwege mijn taalbarrière; hoewel ik Nederlands goed spreek, is het mijn vierde taal, wat de complexiteit van het project vergrootte. Ondanks deze hindernissen ben ik tevreden met de uitkomsten van mijn onderzoek. Ik ben ervan overtuigd dat met betere begeleiding vanuit Saxion de kwaliteit van mijn scriptie nog hoger had kunnen zijn.