Zo pak je de 10 grootste risico's bij softwareontwikkeling aan

RICHTLIJN MOET ZORGEN VOOR BETERE MAATWERKSOFTWARE

PROBLEMEN MET MAATWERKSOFTWARE ZIJN EEN BELANGRIJKE OORZAAK VOOR HET MISLOPEN VAN ICT-PROJECTEN. MAAR VAAK GAAT HET OM DEZELFDE, AL JAREN BEKENDE RISICO'S WAAR OOK AL JAREN BEKENDE MITIGERENDE MAATREGELEN VOOR ZIJN. DAAR IS NU EEN PRAKTIJKRICHTLIJN VOOR VAN NEN. LODEWIJK BERGMANS, LEEN BLOM, FRANK NIESSINK EN ARJEN REUDINK VERWACHTEN DAT HIERMEE DE SUCCESKANS VAN MAATWERKSOFTWAREONTWIKKELING RELATIEF EENVOUDIG OMHOOG KAN.

door Lodewijk Bergmans, Leen Blom, Frank Niessink en Arjen Reudink

beeld Shutterstock

ICT-PROJECTEN HEBBEN DE REPUTATIE DAT ZE UITLOPEN, NIET LEVEREN WAT UITEINDELIJK NODIG IS EN DE KOSTEN ERVAN HOGER ZIJN DAN BEGROOT. ICT-projecten waarin maatwerksoftware wordt ontwikkeld en/of onderhouden al helemaal; boven op de risico's die toch al gemoeid zijn met ICT-projecten in het algemeen, veroorzaken de omvang en complexiteit van maatwerksoftwareprojecten nog extra risico's. Deze projecten krijgen zowel te maken met risico's die generiek zijn voor ICT-projecten als met risico's die inherent zijn aan softwareontwikkeling. Dat terwijl veel risico's bij de ontwikkeling van software op maat bekend zijn en er ook voor veel risico's passende beheersmaatregelen beschikbaar zijn. Daarom heeft een aantal partijen de handen ineengeslagen en onder de vlag van NEN, de Stichting Koninklijk Nederlands Normalisatie Instituut, deze kennis gebundeld en beschikbaar gemaakt in de vorm van een Nederlandse Praktijkrichtlijn voor risicobeheersing bij ontwikkeling en onderhoud van maatwerksoftware: de NPR 5326.

NPR 5326 (Risicobeheersing bij ontwikkeling en onderhoud van maatwerksoftware) beschrijft tien risico's die kunnen optreden bij de ontwikkeling en het onderhoud van software en geeft zeventien risicobeheersmaatregelen om deze risico's te mitigeren. ICTU, Centric, SIG en SDB hebben bijgedragen aan NPR 5326. Hieronder geven zij aan hoe zij (delen van) de NPR toepassen in hun organisatie.

AUTEURS

LODEWIJK BERGMANS
is researcher bij Software Improvement Group (SIG), een onafhankelijke organisatie gespecialiseerd in het meten en verbeteren van de kwaliteit, veiligheid, kosten en risico's van softwaresystemen.

LEEN BLOM
is CTO bij Centric Public Sector Solutions. Centric levert IT-producten en -diensten in diverse markten, waaronder de lokale overheid.

CONTINUE KWALITEITS-BEWAKING MET EEN ONTWIKKELPIJPLIJN

Risico 01: de software wordt gewijzigd waardoor de kwaliteit verslechtert.
Risico 02: de omgeving verandert waardoor de kwaliteit verslechtert.
Dat het wijzigen van software risico's met zich meebrengt, zal niemand verbazen. Dat het niet wijzigen van software ook risico's met zich meebrengt is wat minder intuïtief, maar komt voort uit veranderingen in de omgeving waarin de software gebruikt wordt. Nieuw ontdekte beveiligingskwetsbaarheden in gebruikte bibliotheken, nieuwe versies van andere software waarmee de maatwerksoftware moet samenwerken, nieuwe regelgeving of wettelijke verplichtingen (zoals het besluit digitale toegankelijkheid, dat overheden verplicht digitale diensten toegankelijk te maken) en een andere manier van gebruiken van de toepassing, brengen eigenschappen van de software aan het licht die eerder geen probleem waren, maar dat nu wel worden.
De NPR adviseert een aantal maatregelen om dit risico te verminderen. Een daarvan is het inrichten van een geautomatiseerde ontwikkelpijplijn. Zo'n ontwikkelpijplijn bestaat uit stappen die een zogenaamde continuous-integrationserver (CI-server) regelmatig uitvoert. Dat zijn bijvoorbeeld het compileren van de broncode, het draaien van unit- en integratietesten, het installeren van de software in testomgevingen, het uitvoeren van functionele, performance- en beveiligingstesten en het uitvoeren van kwaliteitscontroles op de broncode.
Alle projecten die ICTU uitvoert waarbij maatwerksoftware wordt ontwikkeld en/of onderhouden, hebben een ontwikkelpijplijn. Figuur 1 laat zien hoe een CI-server een ontwikkelpijplijn toont aan de ontwikkelaars.

SCHATTEN EN KNIPPEN

Risico 03: De hoeveelheid werk is niet correct ingeschat waardoor de geplande functionaliteit niet op tijd af is.
Het op tijd leveren van functionaliteit zorgt ervoor dat de gehele keten van opdracht geven, opdracht aannemen en projectuitvoering planmatig en met de juiste mensen kan worden uitgevoerd. Overschrijdingen hebben effect op zowel het huidige project als op de opvolgende projecten, en op het noodzakelijke onderhoud. Het goed inschatten van de omvang is dus heel belangrijk. In de NPR zijn maatregelen aangegeven die hierbij helpen. Het opknippen in kleinere delen zorgt ervoor dat taken sneller kunnen worden gerealiseerd, waardoor bijsturen eenvoudiger en in een vroeg stadium mogelijk is. Opdrachtgever en opdrachtnemer hebben doorlopend contact, zodat het duidelijk blijft wat de businesswaarde is van elk increment.
Bij de vernieuwing van standaardsoftwarepakketten van Centric wordt de bepaling van de omvang van werkpakketten gedaan door de teams die deze werkpakketten ook uitvoeren. De ervaring is dat teams daardoor met risico's komen die door de projectmanager niet zo gemakkelijk kunnen worden onderkend, bijvoorbeeld dat vooraf verondersteld kennis niet altijd aanwezig is. Daarnaast wordt ook beter duidelijk wat de werkelijke beschikbaarheid is van individuele teamleden.
Vooraf bepalen we verschillende vernieuwingsscenario's die alle worden doorgerekend met de teams. Het bepalen van de haalbaarheid gebeurt door te kijken naar de omvang, maar vooral ook

	Declarative: Checkout SCM	Declarative: Tool Install	Setup	Build & Deploy	Tests	Quality	It & Sonar	Owasp	Runtime	Deploy	Art	Zapscan	Publish	Declarative: Post Actions
Average stage times: (Average full run time: ~53min 59s)	1s	2s	13s	2min 54s	48ms	458ms	16min 2s	3min 52s	511ms	2min 13s	41min 17s	41s	3s	1s
#[illegible] Feb 27 08:10	1s	158ms	19s	3min 18s	81ms	992ms	16min 21s	3min 36s	424ms	41s	49min 34s	35s	7s	1s
#[illegible] Feb 26 19:10	881ms	591ms	21s	2min 25s	32ms	467ms	15min 21s	3min 1s	188ms	10min 1s aborted	37ms aborted	29ms aborted	35ms aborted	1s
#[illegible] Feb 25 19:12	1s	11s	11s	2min 32s	36ms	649ms	16min 52s	4min 29s	373ms	33s	50min 59s	57s	643ms	1s
#[illegible] Feb 24 13:13	1s	298ms	20s	3min 27s	38ms	428ms	15min 24s	3min 54s	470ms	42s	48min 54s	1min 18s	613ms	1s
#[illegible] Feb 24 07:58	932ms	436ms	18s	0min 8s	9.1ms	375ms	15min 17s	4min 5s	411ms	41s	48min 16s	44s	8s	1s
#[illegible] Feb 18 07:58	1s	462ms	12s	3min 31s	44ms	458ms	16min 59s	4min 7s	496ms	31s	49min 58s	33s	6s	1s

De kolommen tonen de verschillende stappen die de CI-server uitvoert, bijvoorbeeld kwaliteitscontroles op de broncode (hier met behulp van SonarQube), het controleren van gebruikte bibliotheken op beveiligingskwetsbaarheden met behulp van de OWASP Dependency Checker, het draaien van een regressietest (ART = Automated Regression Test) en het controleren van de software op beveiligingsrisico's met behulp van OWASP Zapscan.

door mee te nemen hoe aanvaardbaar de risico's zijn. De uiteindelijk te kiezen richting moet worden gedragen door het complete projectteam; voor Centric een voorwaarde tot succes van het traject.

STAKEHOLDERS EN PRODUCT OWNER

Risico 06: Gebrekkige aansturing van het werk waardoor het product niet de juiste functionaliteit biedt.

Het succesvol opleveren van een gedragen en gewenst product wordt voor een groot deel beïnvloed door de opdrachtgever, zo merkten we bij SDB. Dit lijkt een simpele stelling, maar in de praktijk blijkt het vinden van een gemandateerde opdrachtgever (product owner) een lastig probleem en een moeilijk te mitigeren risico. Bij grotere organisaties heb je vrijwel altijd te maken met een gelaagde verantwoordelijkheidsstructuur, waar beslissingsbevoegdheid op zijn best (deels) gedelegeerd is. Dit betekent dat beslissingen over inhoud en prioriteit regelmatig niet voldoende tijdig zijn en daarmee het realiseren van de doelstellingen zoals beschreven in een projectplan ondergraven. Zonder voldoende begrip over de agile werkwijze kan oneigenlijk worden ingegrepen in het proces, met alle verwarring van dien.

De NPR beschrijft hoe je verschillende belanghebbenden kunt organiseren en activeren bij je project- of startbijeenkomst, hoe je hen gezamenlijk de eisen en acceptatiecriteria kunt laten vaststellen en waarom het regelmatig organiseren van demo's zorgt voor betrokkenheid, vertrouwen en uiteindelijk acceptatie van het opgeleverde product. Iemand die het product ziet groeien,

'NIET ELK ONTWIKKELTEAM HOEFT ALLE MODERNE TECHNIEKEN TOE TE PASSEN'

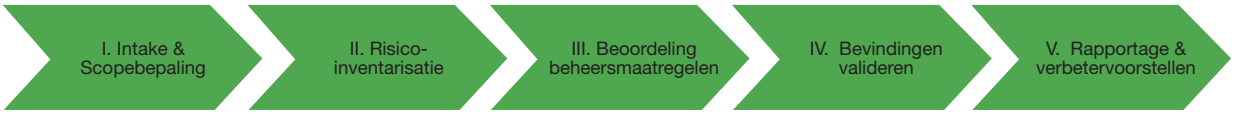
en daarbij invloed kan uitoefenen op vorm en functionaliteit, zal een ambassadeur worden, een pleitbezorger van het product.

Zodra deze belanghebbenden zijn geïdentificeerd, is het zaak om een gemandateerde product owner aan te stellen of te laten kiezen door deze stakeholders, waarbij alle betrokkenen een duidelijk en eenduidig beeld hebben over het mandaat van de product owner en de werkzaamheden die de product owner dient uit te voeren.

TOETSINGSINSTRUMENT

De NPR bevat een toetsingsinstrument: een aanpak om op een systematische en herhaalbare manier de toepassing van de maatregelen in de NPR te toetsen. Die is onder meer gebaseerd op enkele lessen die Software Improvement Group (SIG) in de loop der jaren heeft geleerd over het zinvol inventariseren van maatregelen die in een softwareontwikkelproces worden toegepast:

1. De maatregelen moeten effectief worden toegepast. Een bekend voorbeeld hiervan is wanneer een ontwikkelteam maar een deel van de scrumpractices toepast, wat de effectiviteit van scrum flink verzwakt.
2. Er moet voldoende vertrouwen en inzicht zijn over de daadwerkelijke toepassing van de getoetste best practices.
3. Het doel van een dergelijke inventarisatie moet zijn om te beoordelen of er



Figuur 2. Een overzicht van de stappen voor een systematische toetsing van de toepassing van NPR in een softwareontwikkelingsproject.

mogelijkheden zijn om de kwaliteit en efficiëntie van de softwareontwikkeling te verbeteren.
4. Niet elk ontwikkelteam hoeft alle moderne technieken toe te passen, maar veel organisaties willen zich spiegelen aan de mate waarin technieken elders in de praktijk worden gebruikt.
5. Een inventarisatie moet zo veel mogelijk objectief worden opgesteld; niet alleen vanuit een fairnessprincipe, maar ook zodat bijvoorbeeld opdrachtgevers kunnen controleren hoe een eindconclusie tot stand is gekomen.
Bovenstaande lessen zijn meegenomen in de aanpak, die bestaat uit een aantal stappen (zie figuur 2) om de inventarisatie zorgvuldig te doorlopen, waarbij is gekozen voor een lichtgewicht proces:

Ook het niet wijzigen van software brengt risico's met zich mee

Een toetsing begint met een (I) intake om het proces uit te leggen aan het team en om de benodigde documentatie voor de toetsing vast te stellen. Een belangrijke eigenschap van het toetsingsinstrument is de mogelijkheid om aan te geven wat de relevante risico's zijn (II), waarna alle beheersmaatregelen die relevant zijn voor de geselecteerde risico's worden beoordeeld (III). De resulterende bevindingen worden gevalideerd met het team (IV), en tot slot gepresenteerd, samen met aanbevelingen voor de verbetering van de werkwijze (V).

De screenshot in figuur 3 laat zien hoe in het toetsingsinstrument per risico (hier zijn alleen de risiconummers zichtbaar) kan worden aangegeven of het van toepassing is (TRUE of FALSE), hoeveel maatregelen uit de NPR bijdragen aan het verminderen van de risico's, en – nadat de maatregelen zijn beoordeeld – wat de uiteindelijke impact van die maatregelen is op elk risico.

Lijst van risico's	Risico van toepassing	Aantal maatregelen	Mitigatie door maatregelen
R01	TRUE	5	–
R02	TRUE	4	–
R03	TRUE	8	+
R04	TRUE	4	+
R05	FALSE	0	
R06	TRUE	3	+
R07	FALSE	0	
R08	FALSE	0	
R09	FALSE	0	
R10	TRUE	2	+

Figuur 3.

SUCCESKANS

De NPR 5326 'Risicobeheersing bij ontwikkeling en onderhoud van maatwerksoftware' beschrijft tien risico's die kunnen optreden bij de ontwikkeling en het onderhoud van software en geeft zeventien maatregelen om deze risico's te verminderen. Omdat de risicobeheersmaatregelen bestaan uit geaccepteerde werkwijzen, is de verwachting, en hoop, dat organisaties met behulp van de NPR relatief eenvoudig de succeskans van maatwerksoftwareontwikkeling en -onderhoud zullen verhogen. De NPR is vrij beschikbaar via www.nen.nl/npr5326.

AUTEURS

ARJEN REUDINK
is scrummaster bij het Software Development Bureau (SBD), een bedrijf dat zich sinds 1988 inzet voor kwalitatief hoogstaande en onderhoudbare software bij zijn opdrachtgevers.

FRANK NIESSINK
is kwaliteitsmanager bij ICTU, een onafhankelijke advies- en projectenorganisatie binnen de overheid die werkt aan een betere digitale overheid.