The target criterion VN2 “Place of encryption” states, where or rather on which system the encryption and decryption of e-mail takes place. We distinguish three possible criteria values: client, gateway and external.

Table 2. Target criteria

Targets / Target criteria	
High confidentiality of message exchange (VN)	
VN1	Content encryption procedure
VN2	Place of encryption
VN3	Encrypting e-mail attachments
VN4	Transport encryption procedure
VN5	Enhancements to transport encryption
High integrity assurance during message exchange (IN)	
IN1	Signature creation and verification possible
High identity assurance of the communication partners (IK)	
IK1	Creation of certificates possible
IK2	Signature creation and verification possible
Ensure high availability (VB)	
VB1	Dependence on the manufacturer/provider
Large scope of services (LU)	
LU1	Spam and malware filtering
LU2	Secure communication with non-PGP and -S/MIME users
LU3	Data Loss Prevention (DLP)
LU4	Sending large files
LU5	Subsequent encryption of incoming e-mail
Low installation effort (IA)	
IA1	Creation of key pairs by the end user
IA2	Certification of the public keys for each end user, if necessary
IA3	Publishing of the public keys to all communication partners by end users
IA4	Collection of public keys from all communication partners by end users
IA5	Installation and configuration of software on all client PCs, if necessary
IA6	Installation and configuration of central software, if necessary
Low acquisition costs (AK)	
AK1	One-time costs
Low operating costs (BK)	
BK1	Regular (monthly) costs
Ease of operation (EB)	
EB1	Additional user actions required when sending / receiving
EB2	Knowledge of encryption and signing required
Good support (SU)	
SU1	Help function on homepage, e. g. FAQ, documentation, interactive e-mail support
SU2	Hotline
SU3	On-site service
High trustworthiness of the manufacturer/provider (HV)	
HV1	Data protection, legal regulations in the country of origin
HV2	Awards
HV3	Known vulnerabilities, backdoors
HV4	Source code viewable
HV5	Experience in the fields of encryption, secure digital communication, etc.
HV6	References
High system/product maturity (SR)	
SR1	Period since the first product generation appeared
Good integrability (IB)	
IB1	Secure e-mail communication from mobile devices possible
IB2	Availability/compatibility with desktop operating systems
IB3	Compatibility with e-mail clients

The confidentiality of message exchange is even better, the closer the content encryption/ decryption process is located to the sender and receiver systems. The highest level of target achievement is possible if encryption or decryption takes place directly on the client systems of the communication partners and e-mails are thus transmitted in encrypted form on the entire transmission path (end-to-end). Encryption using in-house gateways at least ensures that the e-mails are encrypted from or to the company boundary. It is assumed that this is less confidential than end-to-end encryption. If the encryption/decryption is carried out by an external service provider, a further reduction in confidentiality can be assumed. The target criterion VN3 “Encryption of e-mail attachments” can be used to check whether only the e-mail messages themselves or their attachments are encrypted. Greater confidentiality of message exchange can be achieved if both e-mail messages and attachments are transmitted in encrypted form.

3.2. Determine target returns

In the second step, for each alternative (evaluated e-mail encryption solutions) the target returns are determined for each target criterion.

For this, we analysed the datasheets, product descriptions, whitepapers, manuals and similar documents. This approach ensures, that the target returns are compiled objective and are not attached by the user’s subjective cognition. In case that the target returns cannot be determined this way, we contacted or interviewed the manufacturer's support.

Table 3 shows a cutout of the complex matrix for the first target and its target criteria. The complete table with the determination of all target criteria for all six analysed solutions can be found at Appendix 1.

Table 3. Cutout of the Target Returns Matrix

Target: High confidentiality of message exchange (VN) **Target criteria**: Content encryption procedure (VN1) Place of encryption (VN2) Encrypting e-mail attachments (VN3) Transport encryption procedure (VN4) Enhancements to Transport Encryption (VN5)				
	Alternative Solutions			
	Mailvelope	**Z1 SecureMail Gateway**	**StartMail.com**	…
VN1	OpenPGP	OpenPGP, S/MIME	OpenPGP	
VN2	Client-PC	Gateway (intern)	StartMail Server (extern)	
VN3	No	Yes	No	
VN4	TLS 1.2	TLS 1.2	TLS 1.2	
VN5	PFS, DANE via add-ons	PFS	PFS	
…				

3.3. Determine target values

The relatively freely formulated alphanumeric target returns cannot be compared properly with each other. Therefore, they are transformed into non-dimensional quantities and represented in so-called target values. In our case, the target returns are transformed into target values according to a five-level nominal scale (1 – insufficient … 5 – very good). In Table 4 we show the same matrix cutout with its target values. The full target value matrix can also be found at Appendix 2.

Table 4. Cutout of the Target Value Matrix

	Alternative Solutions			
	Mailvelope	**Z1 SecureMail Gateway**	**StartMail.com**	…
VN1	3	5	3	
VN2	5	4	1	
VN3	1	5	1	
VN4	5	5	5	
VN5	5	4	4	
…				

3.4. Determine weighting of target criteria

In order to take into account, the individual application context of the encryption solution, which expresses itself through individual requirements, a weighting of the target criteria is necessary. For example, acquisition costs can have a different weighting depending on the amount of financial resources allocated. In our practice-based project, weights were used on the target level and not on the target criteria level. Furthermore, these weights were collected through a survey where security and IT specialists were interviewed with the help of questionnaires. The weights of the targets have been passed on to their criteria. Table 5 shows the target weights for our practice-based project.

Table 5. Average Weighted targets

Functional Targets							
VN	IN	IK	VB	LU			
3.8	3.6	3.8	3.2	2.4			
Non-Functional Targets							
IA	AK	BK	EB	SU	HV	SR	IB
2.6	3.0	3.4	2.8	2.8	3.2	2.6	3.6

(4 – important … 1 – not important; abbreviations see Table 1)

3.5. Perform value synthesis

In the final step of the utility value analysis the target values are multiplied with the weights and summed up to the so-called total benefit for each alternative. A detailed documentation of the calculation of the total benefits can be found in Appendix 3. According to the principle of utility value analysis, the alternative is considered to be the "best" with the greatest overall benefit. In Figure 1 the final results are shown for our set of alternative solutions.

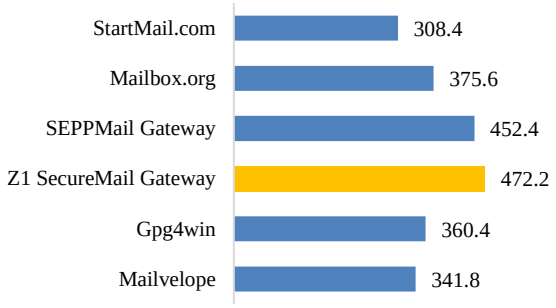

Figure 1. Total benefits of the alternative solutions

4. Conclusion

In this paper, we have applied the utility value analysis (UVA) as a decision support concept to the selection process of encryption solutions for e-mail communication. In our practice-oriented project, Z1 SecureMail Gateway from Zertificon is the solution with the greatest overall benefit. We were able to show that the selection process is made much more transparent by the UVA in particular because the individual requirements of users can be taken into account directly in the selection process by weighting the target criteria.

In order to regard the individual requirements in the selecting process even more it could be useful to perform the UVA twice. By the first UVA, the product

category (client, gateway, cloud-based) is selected. By the following second UVA, the concrete product within the category is selected. Such a cascaded approach furthermore has the advantage, that more category-specific criteria could be regarded within the second UVA.

5. References

[1] T. Campell, The first email message, https://www.cs.umd.edu/class/spring2002/cmsc434-0101/MUIseum/applications/firstemail.html (Accessed: 2017-09-11).

[2] The Radicati Group, Email Statistics Report 2017-2021, Feb 2017, https://www.radicati.com/wp/wp-content/uploads/2017/01/Email-Statistics-Report-2017-2021-Executive-Summary.pdf (Accessed: 2017-09-11).

[3] Thales, Global encryption trends 2017, Apr 2017, https://gets.thalesesecurity.com/pdf/ponemon-global-encryption-trends-study-infographic.pdf (Accessed: 2016-07-05).

[4] Pnomenon, The state of email encryption, 2017, https://www.laninfotech.com/email-security (Accessed: 2017-07-05).

[5] Osterman Research, Enterprise Encryption and Authentication Usage, 2016, https://www.echoworx.com/assets/Enterprise-Encryption-and-Authentication-Usage-A-Survey-Report.pdf (Accessed: 2017-09-05).

[6] B. Schneier, K. Seidell, and S. Vijayakumar, A Worldwide Survey of Encryption Products, 2016, https://www.schneier.com/academic/paperfiles/worldwide-survey-of-encryption-products.pdf (Accessed: 2017-09-26).

[7] B. Schneier, Secrets & Lies, dpunkt, Heidelberg, 2004.

[8] B. Schneier, E-mail Security. How to Keep Your Electronic Messages Private, John Wiley & Sons, New York, 1995.

[9] DsN - Deutschland sicher im Netz, Verschlüsselung von E-Mails – Leitfaden zur E-Mail-Sicherheit für Unternehmen, Berlin, 2015, https://www.sicher-im-netz.de/sites/default/files/download/leitfaden-e-mail-verschluesselung.pdf (Accessed: 2017-08-07).

[10] Technavio, Global E-mail Encryption Market 2017-2021, Dec 2016, https://www.technavio.com/report/global-it-security-global-e-mail-encryption-market-2017-2021 (Accessed: 2017-10-10).

[11] MarketsandMarkets, Email Encryption Market by Deployment Type, Industry Vertical, and Region - Global Forecast to 2020, Nov 2015, http://www.marketsandmarkets.com/Market-Reports/email-encryption-market-182623205.html (Accessed: 2017-05-15).

[12] National Institute of Standards and Technology (NIST), Guidelines on Electronic Mail Security, SP 800-45 Version 2, Feb 2007.

[13] C. Moecke, M. Volkamer, "Usable secure E-Mail communications – criteria and evaluation of existing approaches," in Information Management & Computer Security, vol. 21, no. 1, 2013, pp. 41-52.

[14] D. Fox, "E-Mail-Sicherheit: Kriterien, Standards und Lösungen," in Datenschutz und Datensicherheit, vol. 25, no. 8, 2001, pp. 452-458.

[15] C. Zangemeister, Nutzwertanalyse in der Systemtechnik, Books on Demand, Norderstedt, 2014.

[16] L. Heinrich, R. Riedl, D. Stelzer, Informationsmanagement: Grundlagen, Aufgaben, Methoden, Oldenbourg, München, 2014.

[17] H. Bleich, „Abhörsicher Mail-Services im Test," in Überwachung abwehren, c't wissen Sonderheft, 09/2015, pp. 66-91.

[18] T. Bär, "Tests: SEPPmail VM Secure E-Mail Gateway 500", in IT-Administrator, 02/2015, pp. 20-26.

Appendix 1: Target Returns Matrix

Targets / Target criteria		Alternative Solutions					
		Mailvelope	**Z1 SecureMail Gateway**	**StartMail.com**	**Gpg4win**	**SEPPMail Gateway**	**Mailbox.org**
High confidentiality of message exchange (VN)							
	VN1: Content encryption procedure	OpenPGP	OpenPGP, S/MIME	OpenPGP	OpenPGP, S/MIME	OpenPGP, S/MIME	OpenPGP
	VN2: Place of encryption	Client-PC	Gateway (intern)	StartMail Server (extern)	Client-PC	Gateway (intern)	Mailbox.org Server (extern)
	VN3: Encrypting e-mail attachments	No	Yes	No	Yes	Yes	Yes
	VN4: Transport encryption procedure	TLS 1.2	TLS 1.2	TLS 1.2	TLS 1.2	TLS 1.2	TLS 1.2
	VN5: Enhancements to transport encryption	PFS, DANE via add-ons (firefox/chrom)	PFS	PFS	PFS	PFS (in the pipeline DANE)	PFS, DANE
High integrity assurance during message exchange (IN)							
	IN1: Signature creation and verification possible	Yes	Yes (automatically or manually from end user)	Yes	Yes	Yes (automatically or manually from end user)	Yes
High identity assurance of the communication partners (IK)							
	IK1: Creation of certificates possible	No	Yes	No	Yes	Yes	No
	IK2: Signature creation and verification possible	Yes	Yes (automatically or manually from end user)	Yes	Yes	Yes (automatically or manually from end user)	Yes
Ensure high availability (VB)							
	VB1: Dependence on the manufacturer/provider	Software and add-on must be available for download	Gateway must be available (hardware or software, VM)	Service must be available	Software package must be available for download	Gateway must be available (hardware or software, VM)	Service must be available
Large scope of services (LU)							
	LU1: Spam and malware filtering	No	Yes	Yes	No	Yes	Yes
	LU2: Secure communication with non-PGP and -S/MIME users	No	Yes	Yes	No	Yes	Yes
	LU3: Data Loss Prevention (DLP)	No	Yes	No	No	No	No
	LU4: Sending large files	No	Yes	No	No	Yes	No
	LU5: Subsequent encryption of incoming e-mail	No	No	No	No	No	Yes
Low installation effort (IA)							
	IA1: Creation of key pairs by the end user	Yes	No	Yes	Yes	No	Yes
	IA2: Certification of the public keys for each end user, if necessary	No	Only when using S/MIME	No	Only when using S/MIME	Only when using S/MIME	No
	IA3: Publishing of the public keys to all communication partners by end users	Yes	Yes	Yes, but automatic signature creation is not possible	Yes	Yes	Yes
	IA4: Collection of public keys from all communication partners by end users	Yes	Yes, but only attached signatures are automatically read and saved	Yes, but only automatically if the recipient is also a user of StartMail	Yes	Yes, but only attached signatures are automatically read and saved	Yes, but only automatically if the recipient is also a user of mailbox.org
	IA5: Installation and configuration of software on all client PCs, if necessary	Yes	No	No	Yes	No	No
	IA6: Installation and configuration of central software, if necessary	No	Yes	No	No	Yes	No
Low acquisition costs (AK)							
	AK1: One-time costs	No	Yes, depending on number of employees and scope of functions	No	No	Yes, depending on number of employees and scope of functions	No
Low operating costs (BK)							
	BK1: Regular (monthly) costs	No	-	Yes	No	-	Yes
Ease of operation (EB)							
	EB1: Additional user actions required when sending / receiving	Yes	Depending on the settings at the gateway, user interaction can be completely avoided	Yes, optional it is possible that every outgoing e-mail is encrypted automatically	Yes, sometimes very cumbersome operation, e. g. sending, selecting certificates and encrypting attachments	Depending on the settings at the gateway, user interaction can be completely avoided	Yes, optional it is possible that every outgoing e-mail is encrypted automatically
	EB2: Knowledge of encryption and signing required	Yes	Not necessarily (if the gateway is configured accordingly)	Yes	Yes	Not necessarily (if the gateway is configured accordingly)	Yes
Good support (SU)							
	SU1: Help function on homepage, e. g. FAQ, documentation, interactive e-mail support	Yes (FAQ, user documentation)	Yes	Yes (FAQ, e-mail support)	Yes (multilingual, e-mail support, very detailed user documentation)	Yes	Yes (FAQ, web forum, e-mail support)
	SU2: Hotline	No	Yes	No	No	Yes	No
	SU3: On-site service	No	Yes, initial start-up by Zertificon possible	No	No	Yes, initial start-up by SEPPMail possible	No
High trustworthiness of the manufacturer/provider (HV)							
	HV1: Data protection, legal regulations in the country of origin	Germany	Germany	Netherlands	Sweden/ Germany	Switzerland	Germany
	HV2: Awards	No	Product of the year 2002 (Internet World magazine)	No	No	No	Test winner of Stiftung Warentest (Feb 2016)
	HV3: Known vulnerabilities, backdoors	No	No	No	No	No	No
	HV4: Source code viewable	Yes	No	No	Yes	No	Yes, partly (OX Guard)
	HV5: Experience in the fields of encryption, secure digital communication, etc.	approx. 4 years	approx. 15 years	approx. 9 years	approx. 10 years	approx. 15 years	approx. 25 years
	HV6: References	Use of certified DE-Mail providers	e.g. Allianz, IBM, Stiftung Warentest, Deutscher Sparkassen- und Giroverband	-	-	e.g. ING DiBa, EON, KPMG	-
High system/product maturity (SR)							
	SR1: Period since the first product generation appeared	approx. 4 years	approx. 10 years	approx. 2 years	approx. 10 years	approx. 14 years	approx. 12 years
Good integrability (IB)							
	IB1: Secure e-mail communication from mobile devices possible	Yes, but only via the apps of WEB.DE or GMX	No	No	No	No	No
	IB2: Availability/compatibility with desktop operating systems	Microsoft Windows 7-10, Mac10.6 or higher, Linux Debian, Ubuntu, Fedora, OpenSuse	Independent of desktop OS (as embedded in the SMTP stream)	Microsoft Windows, Mac, Linux	Only Microsoft Windows OS (XP…10)	Independent of desktop OS (as embedded in the SMTP stream)	Microsoft Windows, Mac, Linux
	IB3: Compatibility with e-mail clients	Only web mailer	All clients, no restrictions	All clients, no restrictions	Microsoft Outlook (Plug-in)	All clients, no restrictions	All clients, no restrictions

Appendix 2: Target Value Matrix

Targets / Target criteria	Alternative Solutions						Notes on transformation of target returns to target values
	Mailvelope	Z1 SecureMail Gateway	StartMail.com	Gpg4win	SEPPMail Gateway	Mailbox.org	
High confidentiality of message exchange (VN)							
VN1: Content encryption procedure	3	5	3	5	5	3	Best case S/MIME and PGP, then only one of the procedures; No content encryption would be the worst-case scenario.
VN2: Place of encryption	5	4	1	5	4	1	Better, the closer to the client PC.
VN3: Encrypting e-mail attachments	1	5	1	5	5	5	Best case: Yes
VN4: Transport encryption procedure	5	5	5	5	5	5	Best case: TLS 1.2
VN5: Enhancements to transport encryption	5	4	4	4	4	5	The more extensions, the better it is.
High integrity assurance during message exchange (IN)							
IN1: Signature creation and verification possible	5	5	5	5	5	5	Best case: Yes
High identity assurance of the communication partners (IK)							
IK1: Creation of certificates possible	1	5	1	5	5	1	Best case: Yes
IK2: Signature creation and verification possible	5	5	5	5	5	5	Best case: Yes
Ensure high availability (VB)							
VB1: Dependence on the manufacturer/provider	3	3	1	3	3	1	The worst performers are service providers.
Large scope of services (LU)							
LU1: Spam and malware filtering	1	5	5	1	5	5	Best case: Yes
LU2: Secure communication with non-PGP and -S/MIME users	1	5	5	1	5	5	Best case: Yes
LU3: Data Loss Prevention (DLP)	1	5	1	1	1	1	Best case: Yes
LU4: Sending large files	1	5	1	1	5	1	Best case: Yes
LU5: Subsequent encryption of incoming e-mail	1	1	1	1	1	5	Best case: Yes
Low installation effort (IA)							
IA1: Creation of key pairs by the end user	1	5	1	1	5	1	Best case: No
IA2: Certification of the public keys for each end user, if necessary	5	5	5	1	5	5	Best case: No
IA3: Publishing of the public keys to all communication partners by end users	1	3	1	1	3	3	Best case: No
IA4: Collection of public keys from all communication partners by end users	1	3	2	1	3	2	Best case: No
IA5: Installation and configuration of software on all client PCs, if necessary	1	5	1	1	5	1	Best case: No
IA6: Installation and configuration of central software, if necessary	5	1	5	5	1	5	Best case: No
Low acquisition costs (AK)							
AK1: One-time costs	5	1	5	5	1	5	Less is better.
Low operating costs (BK)							
BK1: Regular (monthly) costs	5	5	4	5	5	3	Less is better.
Ease of operation (EB)							
EB1: Additional user actions required when sending / receiving	2	4	3	2	4	3	Best case: No
EB2: Knowledge of encryption and signing required	3	5	3	2	5	3	Best case: No
Good support (SU)							
SU1: Help function on homepage, e. g. FAQ, documentation, interactive e-mail support	4	3	3	5	3	4	Best case: Yes
SU2: Hotline	1	5	1	1	5	1	Best case: Yes
SU3: On-site service	1	5	1	1	5	1	Best case: Yes
High trustworthiness of the manufacturer/provider (HV)							
HV1: Data protection, legal regulations in the country of origin	5	5	4	5	4	5	
HV2: Awards	1	4	1	1	1	5	Better, the more awards.
HV3: Known vulnerabilities, backdoors	5	5	5	5	5	5	Better, the less known security vulnerabilities.
HV4: Source code viewable	5	1	1	5	1	5	Best case: Yes
HV5: Experience in the fields of encryption, secure digital communication, etc.	2	5	4	4	5	4	More experience is better.
HV6: References	4	5	1	1	5	1	Many well-known customers are better.
High system/product maturity (SR)							
SR1: Period since the first product generation appeared	2	4	2	4	5	4	The longer, the better
Good integrability (IB)							
IB1: Secure e-mail communication from mobile devices possible	3	1	1	1	1	1	Best case: Yes
IB2: Availability/compatibility with desktop operating systems	4	5	4	3	5	4	Better compatibility is better.
IB3: Compatibility with e-mail clients	2	5	2	3	5	2	Better compatibility is better.

Appendix 3: Calculation of the Total Benefits (Value Synthesis)

Target criteria	Alternative Solutions					
	Mailvelope	Z1 SecureMail Gateway	StartMail.com	Gpg4win	SEPPMail Gateway	Mailbox.org
VN 1	3	5	3	5	5	3
VN 2	5	4	1	5	4	1
VN 3	1	5	1	5	5	5
VN 4	5	5	5	5	5	5
VN 5	5	4	4	4	4	5
Subtotal VN	19	23	14	24	23	19
Weight VN	3.8					
Partial Benefit VN[1]	72.2	87.4	53.2	91.2	87.4	72.2
IN 1	5	5	5	5	5	5
Subtotal IN	5	5	5	5	5	5
Weight IN	3.6					
Partial Benefit IN	18	18	18	18	18	18
IK 1	1	5	1	5	5	1
IK 2	5	5	5	5	5	5
Subtotal IK	6	10	6	10	10	6
Weight IK	3.8					
Partial Benefit IK	22.8	38	22.8	38	38	22.8
VB 1	3	3	1	3	3	1
Subtotal VB	3	3	1	3	3	1
Weight VB	3.2					
Partial Benefit VB	9.6	9.6	3.2	9.6	9.6	3.2
LU 1	1	5	5	1	5	5
LU 2	1	5	5	1	5	5
LU 3	1	5	1	1	1	1
LU 4	1	5	1	1	5	1
LU 5	1	1	1	1	1	5
Subtotal LU	5	21	13	5	17	17
Weight LU	2.4					
Partial Benefit LU	12	50.4	31.2	12	40.8	40.8
IA 1	1	5	1	1	5	1
IA 2	5	5	5	1	5	5
IA 3	1	3	1	1	3	3
IA 4	1	3	2	1	3	2
IA 5	1	5	1	1	5	1
IA 6	5	1	5	5	1	5
Subtotal IA	14	22	15	10	22	17
Weight IA	2.6					
Partial Benefit IA	36.4	57.2	39	26	57.2	44.2
AK 1	5	1	5	5	1	5
Subtotal AK	5	1	5	5	1	5
Weight AK	3.0					
Partial Benefit AK	15	3	15	15	3	15
BK 1	5	5	4	5	5	3
Subtotal BK	5	5	4	5	5	3
Weight BK	3.4					
Partial Benefit BK	17	17	13.6	17	17	10.2
EB 1	2	4	3	2	4	3
EB 2	3	5	3	2	5	3
Subtotal EB	5	9	6	4	9	6
Weight EB	2.8					
Partial Benefit EB	14	25.2	16.8	11.2	25.2	16.8
SU 1	4	3	3	5	3	4
SU 2	1	5	1	1	5	1
SU 3	1	5	1	1	5	1
Subtotal SU	6	13	5	7	13	6
Weight SU	2.8					
Partial Benefit SU	16.8	36.4	14	19.6	36.4	16.8
HVA 1	5	5	4	5	4	5
HVA 2	1	4	1	1	1	5
HVA 3	5	5	5	5	5	5
HVA 4	5	1	1	5	1	5
HVA 5	2	5	4	4	5	4
HVA 6	4	5	1	1	5	1
Subtotal HVA	22	25	16	21	21	25
Weight HVA	3.2					
Partial Benefit HVA	70.4	80	51.2	67.2	67.2	80
SR 1	2	4	2	4	5	4
Subtotal SR	2	4	2	4	5	4
Weight SR	2.6					
Partial Benefit SR	5.2	10.4	5.2	10.4	13	10.4
IB 1	3	1	1	1	1	1
IB 2	4	5	4	3	5	4
IB 3	2	5	2	3	5	2
Subtotal IB	9	11	7	7	11	7
Weight IB	3.6					
Partial Benefit IB	32.4	39.6	25.2	25.2	39.6	25.2
Total Benefit[2]	341.8	472.2	308.4	360.4	452.4	375.6

[1] The part benefit of a target is calculated by multiplying the weight with the sum of the target values ("subtotal").

[2] The total benefit results from the addition of the partial benefits. The alternative is considered to be the "best" with the greatest overall benefit.