Auswertung Berufsfeldanalyse 2024

Cyber Security Specialist mit eidg. Fachausweis

ICT Berufsbildung
Formation professionnelle
Formazione professionale

INHALT

ICT Berufsbildung
Formation professionnelle
Formazione professionale

Umfrage im Überblick

Umfrage im Überblick

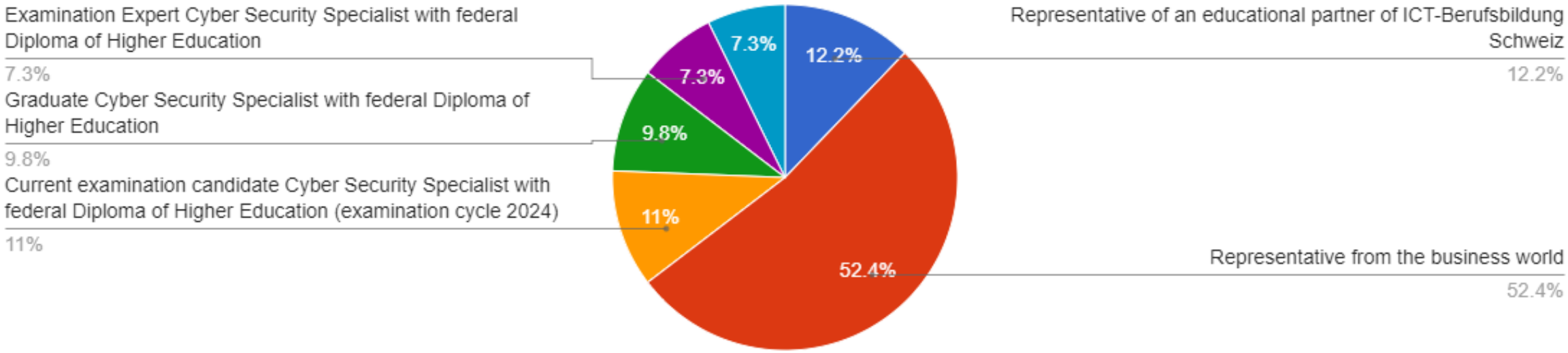
Berufsfeldanalyse Cyber Security Specialist mit eidg. Fachausweis		
Umfragedauer	9. Juli – 12. August 2024	
Umfrageformat	online via Findmind	
Sprache	Englisch	
Umfang	21 Fragen	
Streuung	ICT-Newsletter, LinkedIn, Kommissionen, Gremien und Partnerverbände, SCILS, Bildungspartner	
Anzahl Umfrageteilnehmende	total **66**	fertig ausgefüllt **53**
Prüfungsdokumente	Prüfungsordnung	Wegleitung
Webseite	Weiterbildung	Projektwebseite

ICT Berufsbildung
Formation professionnelle
Formazione professionale

Umfrageteilnehmende

Umfrageteilnehmende

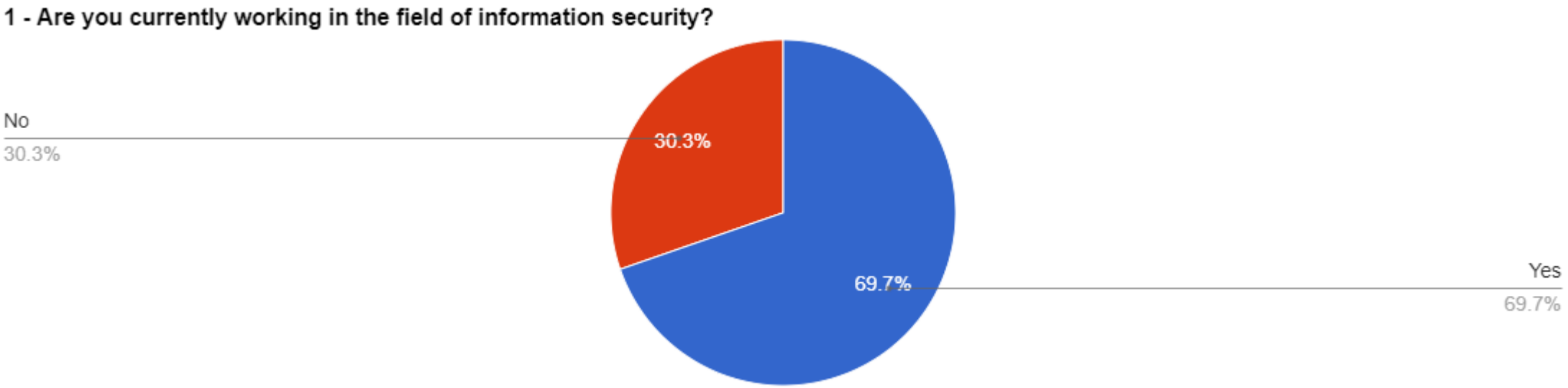
1 - From which perspective are you completing this survey?



Mehrfachantworten waren möglich

66

Aktuelle Tätigkeit im Security-Bereich

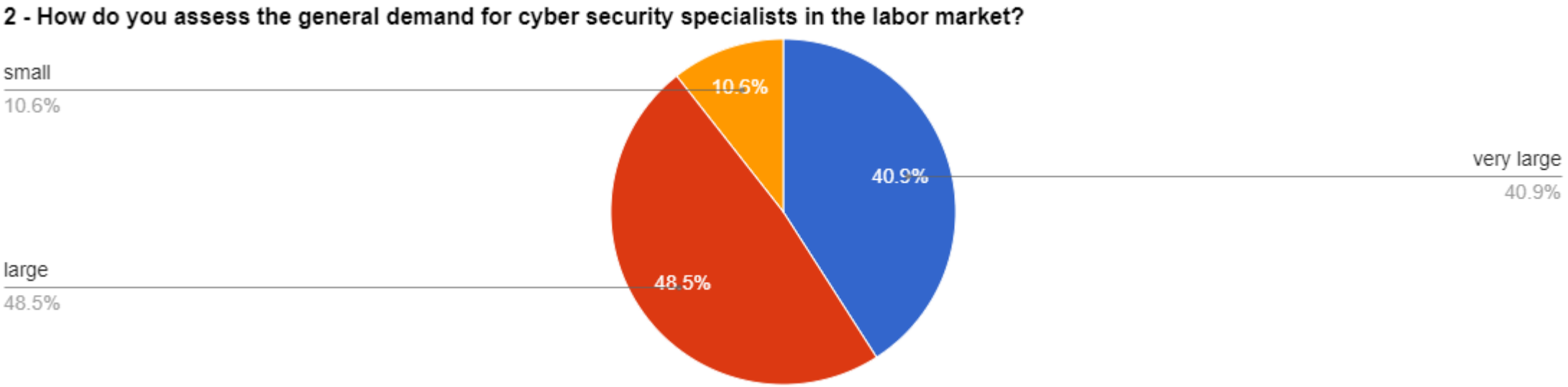


66

ICT Berufsbildung
Formation professionnelle
Formazione professionale

Handlungskompetenzen

Nachfrage im Arbeitsmarkt



Fast 90% der Befragten schätzt den Bedarf an Cyber Security Specialists im Arbeitsmarkt gross bis sehr gross ein.

66

Übersicht Handlungskompetenzen

↓ Handlungskompetenzbereich HKB		Handlungskompetenzen →						
A	**Systeme präventiv schützen**	A1: Entwicklung von Bedrohungen laufend beobachten	A2: Bedrohungen analysieren und Informationen aufbereiten	A3: Schwachstellen erkennen	A4: Schwachstellen schliessen	A5: Verfahren zur Täuschung einsetzen	A6: Stakeholder fachlich beraten	A7: Stakeholder trainieren
B	**Sicherheitsvorfälle erkennen**	B1: Systeme im Betrieb überwachen	B2: Daten analysieren und interpretieren	B3: Sicherheits-vorfälle triagieren	B4: Sicherheitsvor-fälle dokumentieren	B5: Behandlung eines Sicherheits-vorfalls überwachen		
C	**Sicherheitsvorfälle bewältigen**	C1: Sofortmass-nahmen umsetzen	C2: Beweismittel sichern	C3: Ursachen und Auswirkungen analysieren	C4: Schutzmass-nahmen definieren und umsetzen	C5: Wiederherstellung von Systemen unterstützen		
D	**Sicherheitslösungen planen und umsetzen**	D1: Systeme abgrenzen und Anforderungen spezifizieren	D2: Machbarkeit und Wirksamkeit prüfen	D3: Aufwand erheben und budgetieren	D4: Evaluation durchführen	D5: Teilprojekt abwickeln	D6: Team führen	

Wichtigkeit der Handlungskompetenzbereiche

	Ø	important 1	rather important 2	rather not important 3	not important 4
A) Preventive protection of systems	Ø: 1.09 Σ: 66	61 92.42%	4 6.06%	1 1.52%	
B) Detection of security incidents	Ø: 1.23 Σ: 66	51 77.27%	15 22.73%		
C) Handling of security incidents	Ø: 1.24 Σ: 66	51 77.27%	14 21.21%	1 1.52%	
D) Planning and implementation of security solutions	Ø: 1.52 Σ: 66	35 53.03%	28 42.42%	3 4.55%	

66

Wichtigkeit A) Systeme präventiv schützen

	Ø	important 1	rather important 2	rather not important 3	not important 4
A1: Continuously monitor threat developments	Ø: 1.42 Σ: 64	40 62.5%	21 32.81%	3 4.69%	
A2: Analyse threats and prepare information	Ø: 1.45 Σ: 64	39 60.94%	21 32.81%	4 6.25%	
A3: Identify vulnerabilities	Ø: 1.22 Σ: 64	50 78.13%	14 21.88%		
A4: Close vulnerabilities	Ø: 1.33 Σ: 64	47 73.44%	13 20.31%	4 6.25%	
A5: Use deceptive methods	Ø: 1.97 Σ: 64	15 23.44%	36 56.25%	13 20.31%	
A6: Provide technical advice to stakeholders	Ø: 1.73 Σ: 64	28 43.75%	26 40.63%	9 14.06%	1 1.56%
A7: Provide training to stakeholders	Ø: 1.91 Σ: 64	26 40.63%	20 31.25%	16 25%	2 3.13%

64

Wichtigkeit B) Sicherheitsvorfälle erkennen

	Ø	important 1	rather important 2	rather not important 3	not important 4
B1: Monitor systems during operations	Ø: 1.34 Σ: 61	42 68.85%	17 27.87%	2 3.28%	
B2: Analyse and interpret data	Ø: 1.39 Σ: 61	38 62.3%	22 36.07%	1 1.64%	
B3: Triage security incidents	Ø: 1.54 Σ: 61	35 57.38%	19 31.15%	7 11.48%	
B4: Document security incidents	Ø: 1.52 Σ: 61	33 54.1%	24 39.34%	4 6.56%	
B5: Supervise the handling of security incidents	Ø: 1.7 Σ: 61	26 42.62%	28 45.9%	6 9.84%	1 1.64%

61

Wichtigkeit C) Sicherheitsvorfälle bewältigen

	Ø	important 1	rather important 2	rather not important 3	not important 4
C1: Take urgent measures	Ø: 1.13 Σ: 61	54 88.52%	6 9.84%	1 1.64%	
C2: Secure evidence	Ø: 1.49 Σ: 61	36 59.02%	20 32.79%	5 8.2%	
C3: Analyse causes and effects	Ø: 1.33 Σ: 61	43 70.49%	16 26.23%	2 3.28%	
C4: Establish and take protective measures	Ø: 1.26 Σ: 61	45 73.77%	16 26.23%		
C5: Support system recovery	Ø: 1.77 Σ: 61	24 39.34%	27 44.26%	10 16.39%	

61

Wichtigkeit D) Sicherheitslösungen planen und umsetzen

	Ø	important 1	rather important 2	rather not important 3	not important 4
D1: Delineate system boundaries and specify requirements	Ø: 1.57 Σ: 58	29 50%	25 43.1%	4 6.9%	
D2: Check feasibility and effectiveness	Ø: 1.6 Σ: 58	28 48.28%	25 43.1%	5 8.62%	
D3: Estimate and budget workload	Ø: 2.1 Σ: 58	13 22.41%	27 46.55%	17 29.31%	1 1.72%
D4: Carry out evaluations	Ø: 2.19 Σ: 58	9 15.52%	30 51.72%	18 31.03%	1 1.72%
D5: Carry out subprojects	Ø: 2.26 Σ: 58	9 15.52%	26 44.83%	22 37.93%	1 1.72%
D6: Manage teams	Ø: 2.45 Σ: 58	12 20.69%	14 24.14%	26 44.83%	6 10.34%

58

Fehlende Handlungskompetenzen

- Awareness and culture
- Basic knowledge (network, firewall, client, server, proxy, WAF, reverse proxy, Active Directory, Entra, Azure etc.)
- basic understanding of regulatory & compliance requirements, data protection laws
- Categorization of security priorities based on Business needs/requirements
- Use of AI tools / Use of automation
- Cloud Security App Security Digital Forensics Data Loss Prevention
- Incident response and forensics
- Communication / Social interactions with stakeholders
- The whole area of continuous improvement
- handling complexity
- Decentralized security
- crisis management and processes
- It lacks the competence to understand the attacker

22

ICT Berufsbildung
Formation professionnelle
Formazione professionale

Prüfungsstruktur

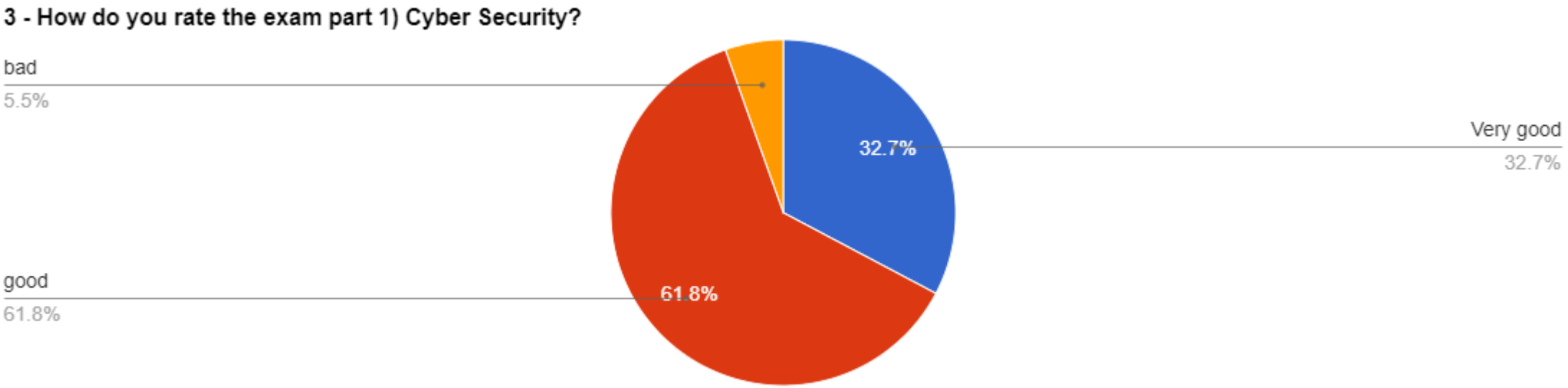
Prüfungsstruktur

Components of the examination

The examination comprises the following parts and lasts:

	Examination part	Type of examination	Duration	Weighting
1	Cyber Security	Practical case processing	5 h	60%
2	Projects & Business administration	Written case processing	2 h	20%
3	Leadership & Communication	Oral case processing and technical discussion	¾ h	20%
		Total	7 ¾ h	

Beurteilung Prüfungsteil 1: allgemein
Cyber Sicherheit (Praktische Fallbearbeitung)



Über 90% der Befragten beurteilt den Prüfungsteil 1 gut bis sehr gut.

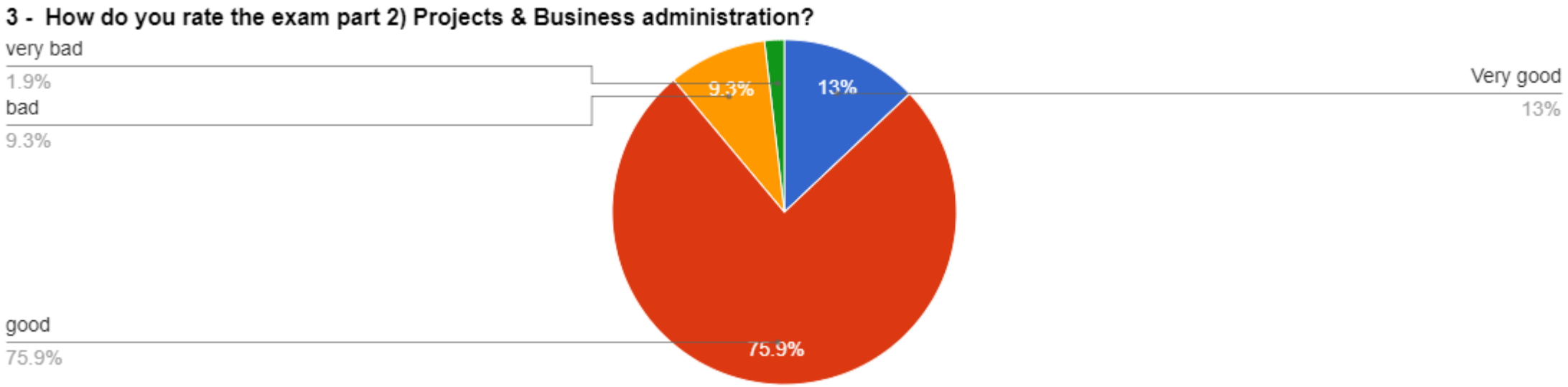
55

Beurteilung Prüfungsteil 1: Dauer & Gewichtung Cyber Sicherheit (Praktische Fallbearbeitung)

	Ø	too much 1	appropriate 2	not enough 3
Duration of 5 hours	Ø: 1.96 Σ: 55	6 10.91%	45 81.82%	4 7.27%
Weighting of 60%	Ø: 2.09 Σ: 55	6 10.91%	38 69.09%	11 20%

55

Beurteilung Prüfungsteil 2: allgemein
Projekte & Betriebswirtschaft (Schriftliche Fallbearbeitung)



Fast 90% der Befragten beurteilt den Prüfungsteil 2 gut bis sehr gut.

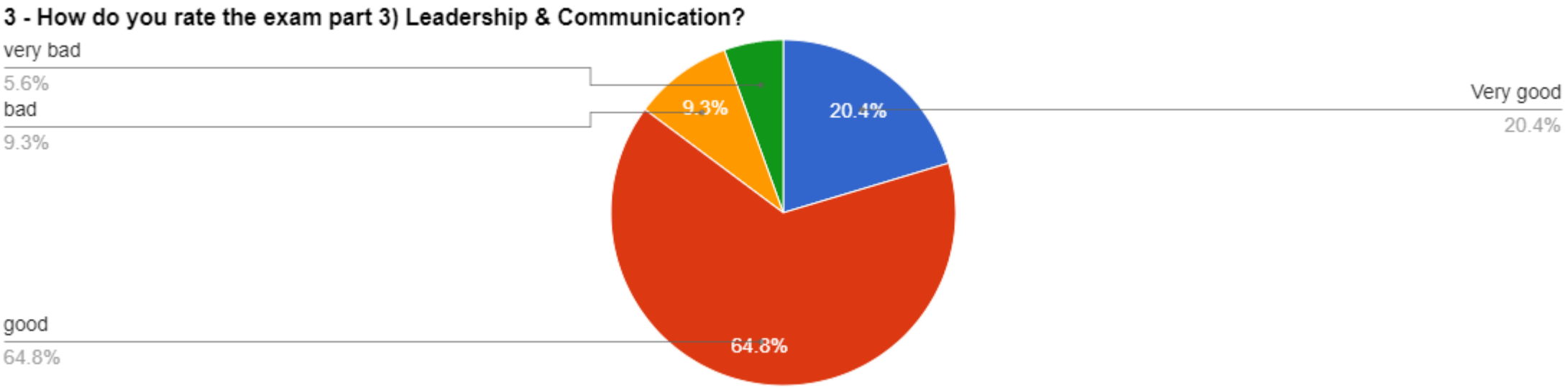
54

Beurteilung Prüfungsteil 2: Dauer & Gewichtung
Projekte & Betriebswirtschaft (Schriftliche Fallbearbeitung)

	Ø	too much 1	appropriate 2	not enough 3
Duration 2 hours	Ø: 2.04 Σ: 54	7 12.96%	38 70.37%	9 16.67%
Weighting 20%	Ø: 2.04 Σ: 54	7 12.96%	38 70.37%	9 16.67%

54

Beurteilung Prüfungsteil 3: allgemein
Führung & Kommunikation (mündliche Fallbearbeitung & Fachgespräch)



85% **der Befragten beurteilt den Prüfungsteil 3 gut bis sehr gut.**

54

Beurteilung Prüfungsteil 3: Dauer & Gewichtung
Führung & Kommunikation (mündliche Fallbearbeitung & Fachgespräch)

	Ø	too much 1	appropriate 2	not enough 3
Duration 0.75 hours	Ø: 2.19 Σ: 54	6 11.11%	32 59.26%	16 29.63%
Weighting 20%	Ø: 1.96 Σ: 54	10 18.52%	36 66.67%	8 14.81%

54

Kontakt

ICT-Berufsbildung Schweiz
Waisenhausplatz 14
3011 Bern

Tel. 058 360 55 50
info@ict-berufsbildung.ch
www.ict-berufsbildung.ch

Home › Verband › Zukunft & Entwicklung ›

Revision Fachausweis Cyber Security Specialist.

Überprüfung der eidgenössischen Berufsprüfung

Die Welt der ICT verändert sich schnell, insbesondere im Security-Bereich. Damit die ICT-Fachkräfte die auf dem Arbeitsmarkt gefragten Kompetenzen mitbringen, werden die Aktualität und Qualität der eidgenössischen Abschlüsse regelmässig kontrolliert.

Überprüfung
Als erstes steht die Überprüfung des Berufsbildes und der darin definierten Handlungskompetenzen für den eidgenössischen Fachausweis Cyber Security Specialist an.