



Sectoral Human Capital Study II (BBKL II)

Telecommunications and Cybersecurity

Survey results summary
– 1st edition

About the study



Project name

Sectoral Human Capital Study II Telecommunications and Cybersecurity



Main goals:

- » To increase the **knowledge about the current and future demand for skills** in the telecommunications and cybersecurity sector
- » To identify the **challenges for the sector** (3-year perspective)



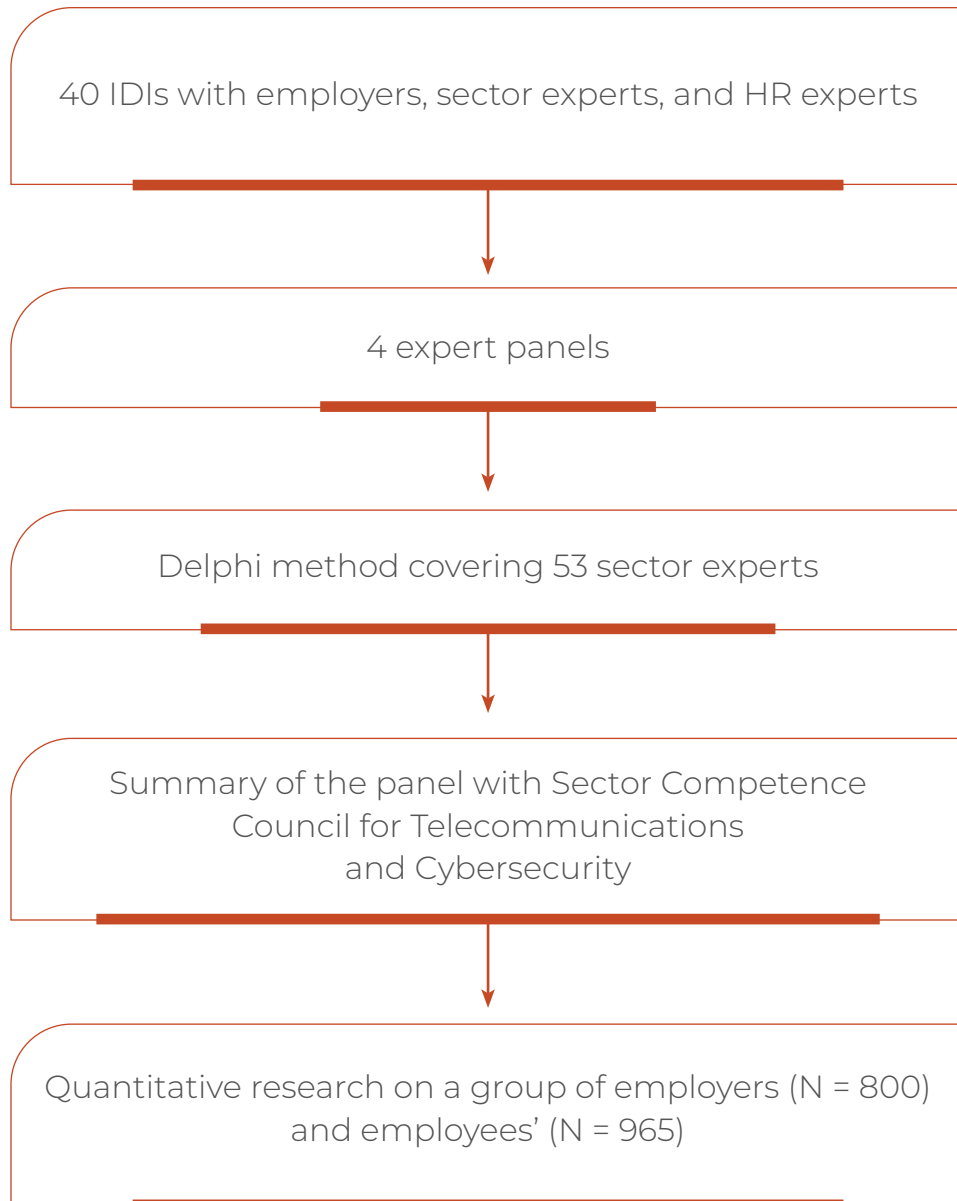
Research Dates, 1st edition:

18 December 2020 – 14 January 2022



Methodology

Methods used:



Qualitative research fieldwork:
20 April 2021 – 14 July 2021

Quantitative research fieldwork:
7 October 2021 – 27 October 2021

About the sector

Definition of the sector (based on the Polish Classification of Activity aka PKD):

- Wired telecommunications (PKD J.61.1) 
- Wireless telecommunications (PKD J.61.2) 
- Satellite telecommunications (PKD J.61.3) 
- Other types of telecommunications (PKD J.61.9) 
- Cybersecurity (PKD J.62.03.Z) 

Key employment data



15 438
companies*



42 687
employers in the
telecommunications sector**



Sales volume of products
and services in the
telecommunications sector:

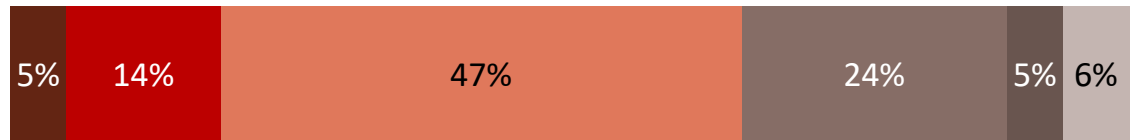
PLN 41.5 bn**

* Quarterly National Business Registry Number (REGON) and Statistics Poland (GUS) data as of 30/09/2021; only the PKD codes given above

** Information Society in Poland, GUS

The impact of the pandemic on the sector

- Very positive
- Positive
- Neither positive nor negative
- Negative
- Very negative
- Don't know / hard to say



Positive impact: **19%**

Negative impact: **29%**

By sector:

Telecommunications (T): **18%**

Cybersecurity (C): **27%**

By sector:

Telecommunications (T): **29%**

Cybersecurity (C): **23%**

Most common changes:

Positive:

- » Increased number of provided services (T: 56%, C: 78%)
- » Remote work (T: 54%, C: 58%)
- » Getting new partners for cooperation (T: 50%, C: 61%)

Negative:

- » Increased operating costs (T: 75%, C: 80%)
- » Procedures modified to meet COVID-19 safety requirements (T: 67%, C: 81%)
- » Staff shortages due to quarantine (T: 65%, C: 55%)

Source: SHCSII Telecommunications and Cybersecurity, 1st wave, quantitative survey of employers, n = 800.

Key business processes and assigned positions (telecommunications)

Business processes

Key positions

Software development

The process concerns the development of software and systems that enable the operation of passive infrastructure and electronic devices such as telephones, modems, set-top boxes, etc. Each of the listed devices and specific elements of the telecommunications infrastructure needs a special system (software) for proper operation. The system enables control and use of the device.

- » IT Architect
- » Developer
- » Quality Assurance

Designing telecommunications devices and infrastructure

The process consists in developing passive infrastructure projects, e.g., base transceiver stations (BTS), antennas, transmitters, and all kinds of electronic devices such as telephones and modems.

- » Engineer

Service coordination and maintenance of telecommunications infrastructure

The process includes activities related to the repair, modernization and ensuring uninterrupted operation (emission continuity) of base transceiver stations, antennas and other devices (as well as programs and services purchased by customers) enabling access to the telephone network, the Internet, TV, etc.

- » Project Manager

Selling

- » Sales Manager



Key business processes and assigned positions (cybersecurity)

Business processes

Key positions

Conducting security audits

Activities related to the assessment of whether infrastructure, systems, and applications meet specific requirements and safety standards.

- » Security Auditor
- » Penetration Tester

Analysis, asset protection and threat identification

Identifying all the goods that are in the company (devices, documents, digital assets, etc.) and assessing whether the particular resources are adequately protected.

- » Chief Information Security Officer (CISO)

Prevention for security

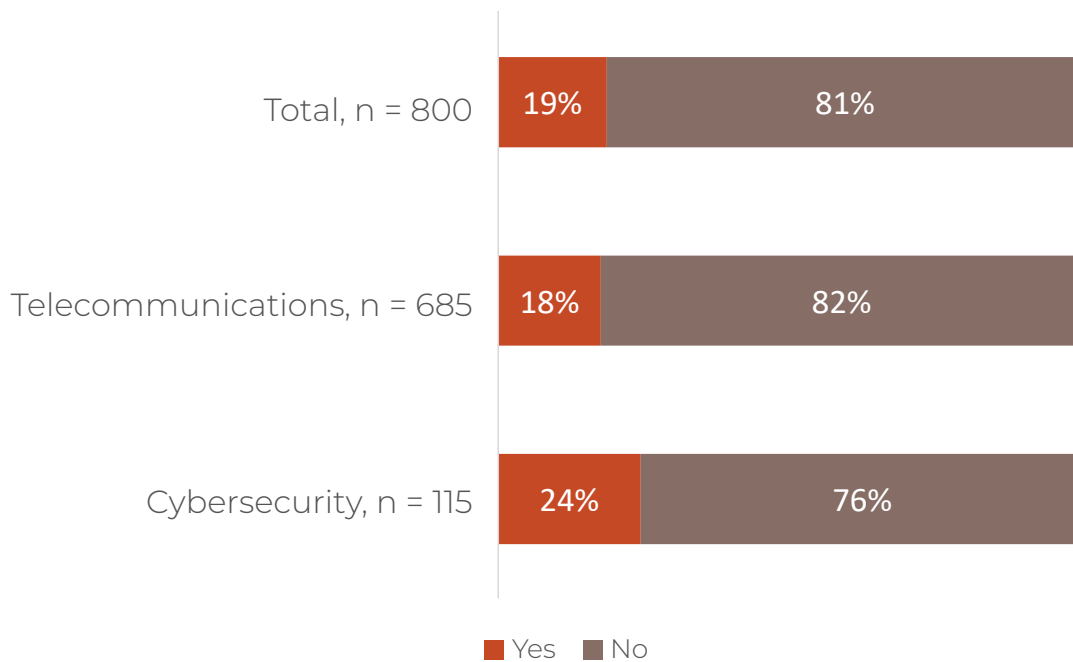
Monitoring systems and networks to detect potential threats; incident handling including activities related to blocking an incident, restoring infrastructure, and possible repairs, and drawing conclusions for the future.

- » Security Architect
- » Security Operations Centre (SOC) Coordinator
- » Security Expert

Selling

- » Sales Manager

Demand for labor



» **One in five** companies was looking for new specialists in the last 12 months.

» Key positions in greatest demand:

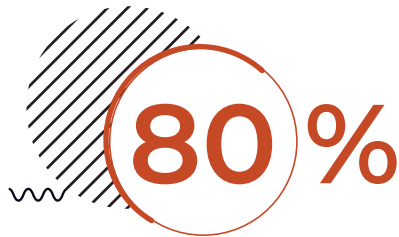
telecommunications:

- » Engineer (48%)
- » Developer (32%)
- » IT Architect (28%)

cybersecurity:

- » Security Auditor (49%)
- » Security Expert (38%)
- » Security Architect (32%)

Assessment of graduates' skills required to start work

A graphic showing the number 80% in a large, bold, orange font. The number is enclosed in a thin orange circle. To the left of the circle is a decorative pattern of diagonal lines and a wavy line. The background is white with a vertical orange bar on the left side of the page.

80%

of employers claim **graduates have the skills required by the sector**

However...

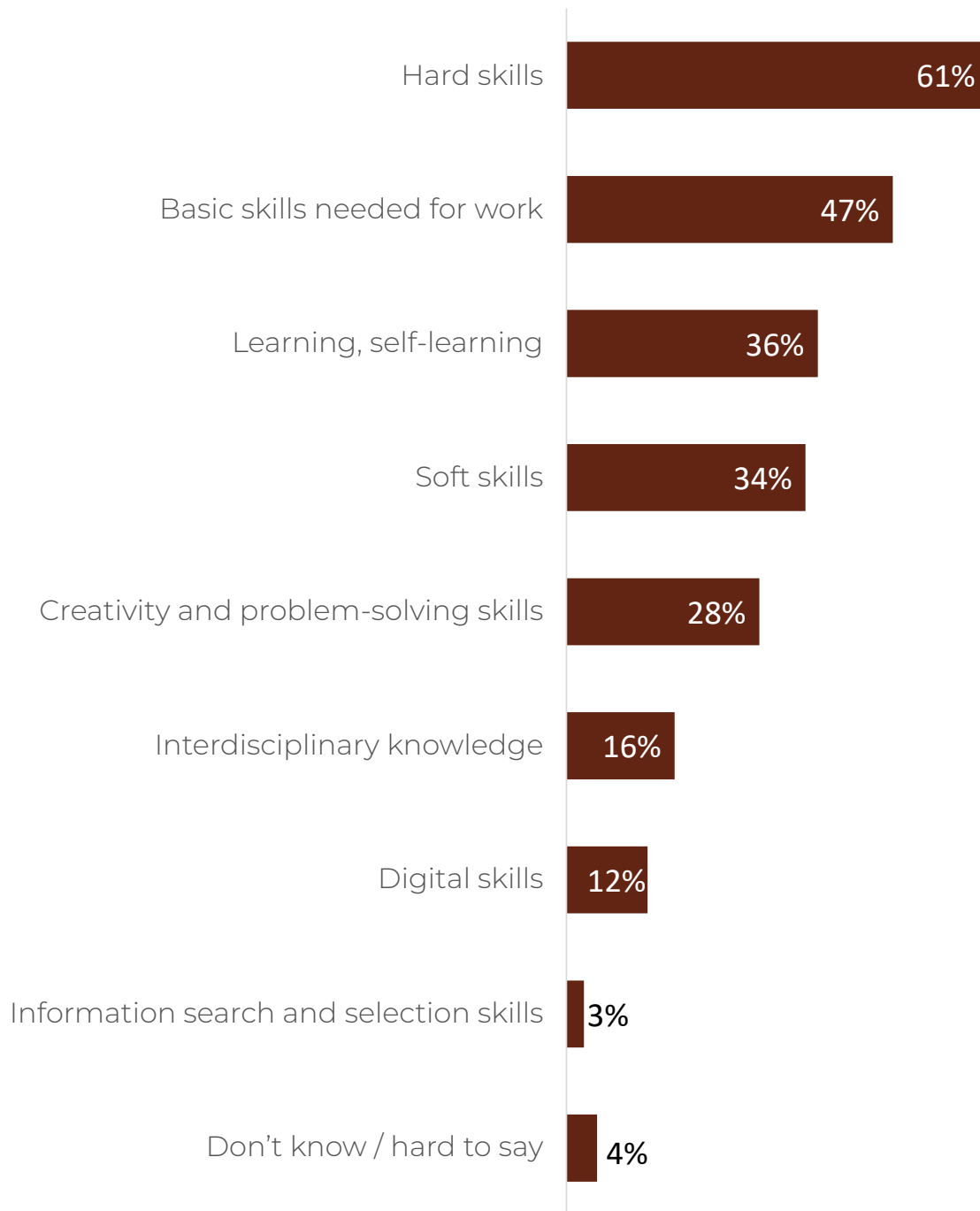
the assessment of new hires' skills is **less positive:**



- » **only every fourth employer** believes that graduates are fully prepared for work;
- » **two in five companies** say graduates should undergo some training before starting work;
- » **over 35%** of employees' **receive more or less complete training** before or after starting work;

Knowledge and skills that should be taught in schools/colleges

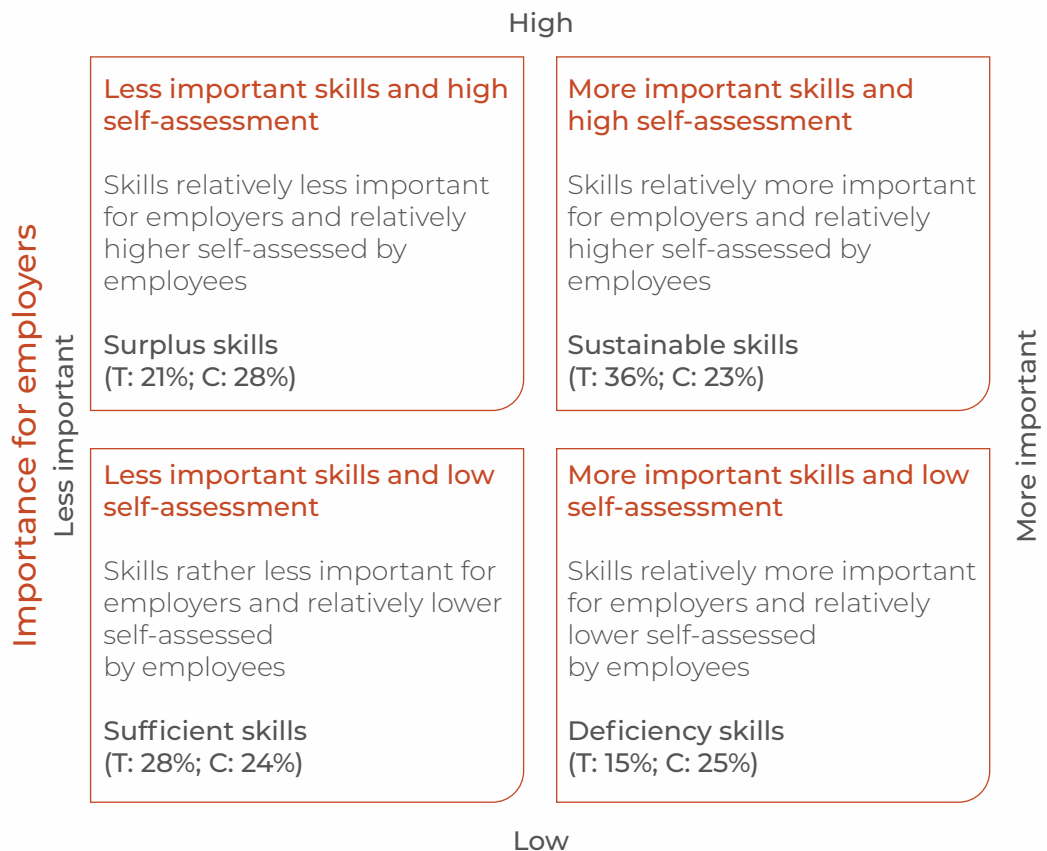
Hard skills are among the crucial ones.



Balance of competences (skills)

Skills mismatch: a comparison between a skill's importance assessment (in the context of a given position) conducted by employers, and employees' self-assessment of the mentioned skills.

Employees self-assessment of skills



Skills gap: a situation where at least 51% of companies assessing skills profiles identify skills that are relatively more important while it is difficult to recruit employees who have them.

Skills of the future: skills selected based on the expected change of importance (within the next 3 years) of the assessed skills.

Balance of competences (skills)

Skills relatively more important for employers and relatively lower self-assessed by employees (**deficiency skills**) that are currently hard-to-find (**skills gap**) and which importance is increasing (**skills of the future**) concern the following positions*:

Quality Assurance (Telecommunications)

- » Improving code quality and readability;
- » Finding operation errors of a system, program, service;

Security Expert (Cybersecurity)

- » Using security platforms (e.g. application and network firewalls);
- » Blocking threats (including potential security incidents);
- » Filing systems knowledge and principles of operation;
- » Operating systems and networks in terms of security;
- » Recovering data (e.g., data lost due to a security incident);
- » Knowledge of operating systems;
- » Recognizing attacks and disturbing incidents;

Security Architect (Cybersecurity)

- » Knowledge of digital security (systems, software);
- » Responsibility;
- » Managing systems;
- » Predicting attack scenarios (e.g., on a system, program, service);
- » Knowledge of foreign languages – especially English;

* Positions with the greatest number of skills are shown. Those with only few skills are omitted.



Balance of competences (skills)

Average importance of skills*:

- » Telecommunications
– from 4.26 to 4.80
- » Cybersecurity
– from 3.87 to 4.84

Average self-assessment of skills*:

- » Telecommunications
– from 4.07 to 4.55
- » Cybersecurity
– from 3.67 to 4.61

* Based on a five-point scale.

Skills of the future are those which importance is increasing (based on employers' predictions). The table below shows five skills of the future which entrepreneurs mentioned most often.

Telecommunications

Conducting and programming automated tests

Basic knowledge of programming languages and technologies (e.g. Python, C, C#, Java, JavaScript, Angular, React, Scala etc.)

Knowledge of cloud technologies

Knowledge of IT technologies (including most recent ones)

Improving code quality and readability

Cybersecurity

Planning attack scenarios

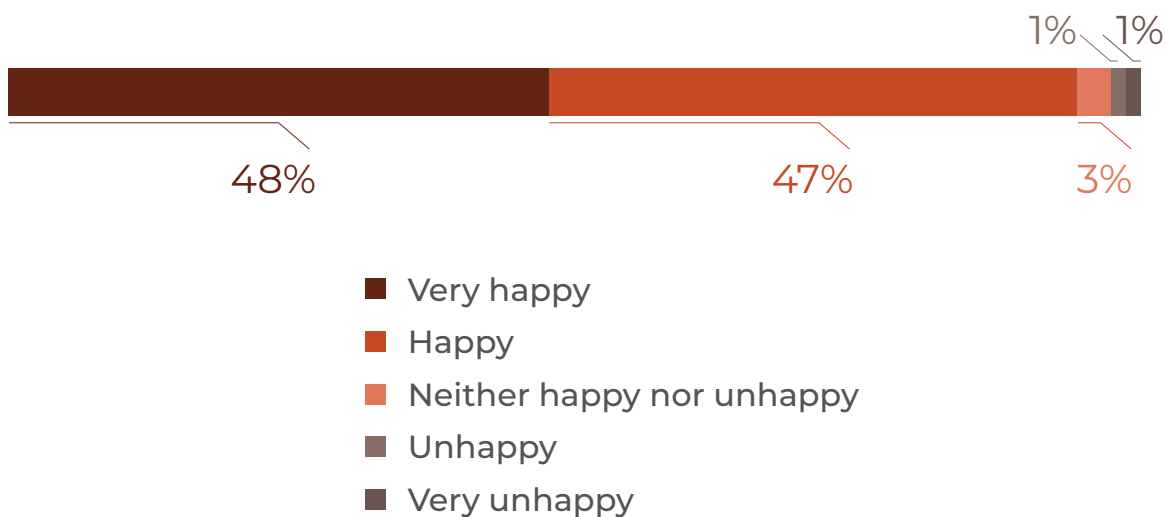
Knowledge of legal standards concerning pen-tests and pen-tester liability

Blocking threats (including potential security incidents)

High level of interpersonal communication

Collecting information and verifying its quality

Employees' work satisfaction



95%

of employees in key positions
are satisfied with their work

Top rated aspects of work



» relations with superiors (97%)



» relations with co-workers (96%)



» working conditions (96%)



» possibility to demonstrate initiative
and independence (96%)



Challenges

Three key challenges

- » Ensuring employees' personal development to enable them to keep their jobs – Total: 51%, T: 51%, C: 53%.
- » Meeting the standards and requirements for emerging new technologies – Total: 50%, T: 50%, C: 49%.
- » Informing clients about threats when using technologies and services offered by the company – Total: 46%, T: 45%, C: 49%.

Challenges with greatest absolute difference between sectors

- » Finding new IT specialists to design systems, programs, applications etc. (9 p.p. difference in favor of C).
- » Verifying new employees' skills and their employment history with regard to personal data protection (9 p.p. difference in favor of C).
- » Improving user experience when using the technologies and services offered by the company (6 p.p. difference in favor of C).

Sector: T – Telecommunications, C - Cybersecurity

Source: SHCSII Telecommunications and Cybersecurity, 1st wave, quantitative survey of employers and employees.

Percentages are the share of companies that provided the listed answers.

For the full report

„Sectoral Human Capital Study II
– telecommunications and cybersecurity.
1st edition”

visit our website

 [https://www.parp.gov.pl/component/site/site/
bilans-kapitaluludzkiego#wynikibadanbranzowych](https://www.parp.gov.pl/component/site/site/bilans-kapitaluludzkiego#wynikibadanbranzowych)